MANUAL DE PROTECCIÓN DE DATOS

IBIZA NURSE SERVICE S.L

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: 27 de abril 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

IBIZA NURSE SERVICE S.L 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, **IBIZA NURSE SERVICE S.L** queda obligada y es responsable de cumplir con la normativa estatal y europea vigente de protección de datos.

Es especialmente importante subrayar que **IBIZA NURSE SERVICE S.L** 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 Sociedad.
- 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 breve posible las solicitudes de ejercicio de dichos derechos. Para ello, se puede hacer uso de los modelos recogidos en los **Anexos XI y XII**.
- Nombrar al Delegado de Protección de Datos (DPO) o a un Responsable de Protección de Datos, 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 XIII**.
- Utilizar las cláusulas de protección de datos recogidas en el **Anexo XIV** para informar y, en caso de ser necesario, solicitar el consentimiento de los interesados (empleados, candidatos, clientes, propietarios, colaboradores, proveedores, visitantes, usuarios web, etc.). Se recomienda que, si es posible, cada uno de estos interesados firme la cláusula correspondiente, de forma que la Sociedad 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 Sociedad puede utilizar los contratos recogidos en el **Anexo XV** con Proveedores que presten servicios con o sin acceso a datos personales y con Clientes a los que la Sociedad 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 XVI**.
- Completar periódicamente el Formulario de Verificación del **Anexo XVII** 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 **IBIZA NURSE SERVICE S.L**. En el **Anexo XVIII** 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 su organización sufre cambios, nuevas líneas de negocio, o recoge una nueva tipología de datos, contacte con su comercial ya que es probable que deban darse nuevos pasos sobre la adaptación de su organización a la normativa.

2. Introducción

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 **IBIZA NURSE SERVICE S.L** 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 **ARANZADI** en **IBIZA NURSE SERVICE S.L.** La Sociedad 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 **IBIZA NURSE SERVICE S.L** 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:
    - el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;
    - 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
    - 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**:
    - 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;
    - 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 presente Reglamento;
- **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 presente Reglamento, o sobre la conformidad con el presente Reglamento 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 presente Reglamento;
- **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**:
    - 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
    - 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 **IBIZA NURSE SERVICE S.L** 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 **IBIZA NURSE SERVICE S.L** 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 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 **IBIZA NURSE SERVICE S.L**, con domicilio social en C/ Pais Vasco Nº5 201, 07800; Ibiza (Islas Baleares).

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 **IBIZA NURSE SERVICE S.L.**

La política, procedimientos y medidas recogidas en el presente Manual de Protección de Datos podrán ser extendidas a cualesquiera otras instalaciones que **IBIZA NURSE SERVICE S.L** 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.

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 Sociedad, programas informáticos, archivos que contengan datos personales y programas que traten los mismos.
- Documentación de la Sociedad 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 **IBIZA NURSE SERVICE S.L**, 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 Sociedad 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 Sociedad, 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 Sociedad, 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 **IBIZA NURSE SERVICE S.L**, 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. **IBIZA NURSE SERVICE S.L**, como Responsable del Tratamiento, solamente podrán 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 **IBIZA NURSE SERVICE S.L** 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 **IBIZA NURSE SERVICE S.L** como Responsable del Tratamiento, y no serán tratados, posteriormente, de manera incompatible 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 **IBIZA NURSE SERVICE S.L,** 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 **IBIZA NURSE SERVICE S.L** 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, **IBIZA NURSE SERVICE S.L** 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, **IBIZA NURSE SERVICE S.L** 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

- **IBIZA NURSE SERVICE S.L** 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 **IBIZA NURSE SERVICE S.L.**

Principio de responsabilidad proactiva: IBIZA NURSE SERVICE S.L, 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, **IBIZA NURSE SERVICE S.L** 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: IBIZA NURSE SERVICE S.L 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 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

IBIZA NURSE SERVICE S.L, 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 **IBIZA NURSE SERVICE S.L** por su condición de Responsable del Tratamiento:

- Realizar por sí mismo, o a través de un representante o del Delegado de Protección de Datos, o por medio de persona autorizada al efecto, cualesquiera de las gestiones de notificación ante la Agencia Española de Protección de Datos (AEPD).
- Redactar, establecer y comprobar 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; 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, que, entre otras funciones, supervise el cumplimiento del RGPD.
- 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 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

IBIZA NURSE SERVICE S.L ha acordado la designación del siguiente **Delegado de Protección de Datos (DPO)** para todos los tratamientos de datos realizados por la Sociedad:

Nombre y Apellidos:

La Sociedad, 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 y de otras disposiciones de protección de datos estatales y europeas.
- Supervisar el cumplimiento del RGPD, 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 auditorias 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.
- 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.
- 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

IBIZA NURSE SERVICE S.L 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
CLIENTES/PACIENTES/PROVEEDORES/GESTIÓN DE RRHH/SELECCIÓN DE PERSONAL	Mª VICTORIA CEGARRA GUTIERREZ

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 **IBIZA NURSE SERVICE S.L**, 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 XIII** del presente Manual de Protección de Datos.
- Comunicar al DPO 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 DPO 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 **IBIZA NURSE SERVICE S.L.**

- Consultar con el DPO las cláusulas a utilizar en los contratos de prestación de servicios con Encargados del Tratamiento.
- Solicitar la autorización del DPO 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 **IBIZA NURSE SERVICE S.L** garantice a los interesados el ejercicio efectivo sus derechos.
- Colaborar con el Responsable del Tratamiento y con el DPO en la formación y concienciación del personal de **IBIZA NURSE SERVICE S.L** 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 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 XVI** 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 DPO 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

IBIZA NURSE SERVICE S.L 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 Sociedad.

Nombre y Apellidos: **Mª Victoria Cegarra Gutierrez**

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 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 **IBIZA NURSE SERVICE S.L**, 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 con la mayor brevedad posible,
  - comunicar al DPO 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 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 XVI** 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 **IBIZA NURSE SERVICE S.L,** 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 **IBIZA NURSE SERVICE S.L** 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 **IBIZA NURSE SERVICE S.L** 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 **IBIZA NURSE SERVICE S.L** 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 **IBIZA NURSE SERVICE S.L** 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 el **Anexo XIV** 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.

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 **IBIZA NURSE SERVICE S.L** 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 XVI** 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 **IBIZA NURSE SERVICE S.L** 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 **IBIZA NURSE SERVICE S.L.** 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.
- Queda prohibido utilizar los recursos telemáticos de **IBIZA NURSE SERVICE S.L** (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 phishing

Uso de aplicaciones

- Únicamente podrán utilizarse aquellas aplicaciones creadas por el personal de **IBIZA NURSE SERVICE S.L** 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.

Otras medidas de seguridad

Queda prohibido:

- Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de **IBIZA NURSE SERVICE S.L** 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 la Sociedad. **IBIZA NURSE SERVICE S.L** 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.

IBIZA NURSE SERVICE S.L 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 **IBIZA NURSE SERVICE S.L**, 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

IBIZA NURSE SERVICE S.L, 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 Delegado de Protección de Datos (DPO), 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)
- 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 **IBIZA NURSE SERVICE S.L** 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

Los sistemas de información que tratan datos personales se concentran en los siguientes recursos:

☑ **Nube/cloud**
☐ **Servidor Central (si lo hubiese)**
- ☐ Sistema Operativo:
- ☐ Dispone de SAI *(Sistema Alimentación Ininterrumpida)*
- ☐ Copia de Seguridad
  - ☐ Nombre Aplicación Copia de Seguridad:
  - ☐ Soporte Copias de Seguridad:
    - ☐ Cinta ☐ Disco Duro Ext.(por duplicado) ☐ Memoria Ext. ☐ CD/DVD ☐ A distancia ☐ Otros
    - ☐ Si a Distancia indique el nombre del proveedor, si es Otro, indique el soporte.
  - ☐ Lugar de Almacenamiento de Copias de Seguridad:
    - ☐ Mismo lugar que el servidor
    - ☐ Lugar distinto. Indicar dirección o proveedor de servicio:
  - ☐ Tiempo *(periodicidad):*
    - ☐ Diaria
    - ☐ Semanal (todos los niveles)
- ☐ Cifrado de Datos
  - ☐ Nombre Aplicación Cifrado de Datos en Discos Internos
  - ☐ El cifrado de datos se realiza por la aplicación de gestión de datos *(ej. Contraseñas)*
  - ☐ Soporte Copias de Seguridad:
    - ☐ Cinta ☐ Disco Duro Ext. ☐ Memoria Ext. ☐ CD/DVD ☐ A distancia ☐ Otros
    - ☐ Si a Distancia indique el nombre del proveedor, si es Otro, indique el soporte.

☐ **PCS (ordenadores de sobremesa)**
- ☐ Sistema Operativo instalado en la mayoría de PCS:
- ☐ Acceso mediante usuarios y contraseña (modificada anualmente)
- ☐ Conectados en Red a Servidor Central
- ☐ Copia de seguridad realizada desde el Servidor Central
- ☐ Copia de seguridad realizada desde el propio PC
  - ☐ Tiempo *(periodicidad):*
    - ☐ Diaria
    - ☐ Semanal *(todos los niveles)*
  - ☐ Aplicación para Copia de Seguridad *(Sólo si no es volcado directo):*
  - ☐ Volcado directo de archivos a soporte
  - ☐ Soporte Utilizado:
    - ☐ Disco Duro Ext. ☐ Memoria Ext. ☐ CD/DVD ☐ Otros ☐ A distancia ☐ Otros
    - ☐ Si a Distancia indique el nombre del proveedor, si es Otro, indique el soporte.

☑ **Equipos portátiles**
- ☑ Sistema Operativo instalado en la mayoría de portátiles: Windows 10 Pro
- ☐ Conectados en Red a Servidor Central
- ☐ Copia de seguridad realizada desde el Servidor Central
- ☑ Copia de seguridad realizada desde el propio portátil
  - ☑ Tiempo *(periodicidad):*
    - ☑ Diaria en la nube
    - ☑ Quincenal (a través de disco duro externo)
  - ☐ Aplicación para Copia de Seguridad *(Sólo si no es volcado directo):*
  - ☐ Volcado directo de archivos a soporte
  - ☑ Soporte Utilizado:
    - ☑ Disco Duro Ext. ☐ Memoria Ext. ☐ CD/DVD ☐ Otros ☑ A distancia ☐ Otros
    - ☑ Si a Distancia indique el nombre del proveedor:

Antivirus:

☐ **APLICACIONES con datos de carácter personal**

Nombre	Fichero/s	Copias de seguridad	Periodicidad

5.3. Encargados del Tratamiento

IBIZA NURSE SERVICE S.L, 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 y 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 **IBIZA NURSE SERVICE S.L**, así como durante la vigencia de la relación contractual, **IBIZA NURSE SERVICE S.L** 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 **IBIZA NURSE SERVICE S.L**.

Igualmente, **IBIZA NURSE SERVICE S.L** puede actuar como prestador de servicios para diversas sociedades. En los contratos a firmar con estas sociedades, **IBIZA NURSE SERVICE S.L** 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 **Anexo XV** 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, conformes al RGPD, 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 **IBIZA NURSE SERVICE S.L**
- El listado de Responsables del Tratamiento a los que **IBIZA NURSE SERVICE S.L** 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.

IBIZA NURSE SERVICE S.L 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, 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.

IBIZA NURSE SERVICE S.L 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 modelo aprobadas por los Responsables y Encargados del Tratamiento y la Autoridad de Control competente (Transferencias mediante garantías adecuadas).

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

IBIZA NURSE SERVICE S.L 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)

IBIZA NURSE SERVICE S.L tiene derecho a crear y mantener 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, IBIZA NURSE SERVICE S.L garantizará 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**: En caso de crearse este Canal de Denuncias, **IBIZA NURSE SERVICE S.L** deberá informar 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

IBIZA NURSE SERVICE S.L 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, **IBIZA NURSE SERVICE S.L** 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, **IBIZA NURSE SERVICE S.L** 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 **IBIZA NURSE SERVICE S.L**, 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.

5.7.1. Dispositivos digitales

Deber de información: **IBIZA NURSE SERVICE S.L** 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.

5.7.2. Desconexión digital

Deber de información: **IBIZA NURSE SERVICE S.L** 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.

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, **IBIZA NURSE SERVICE S.L** 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 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, **IBIZA NURSE SERVICE S.L** 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, **IBIZA NURSE SERVICE S.L,** 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.

6.1. Medidas de Seguridad a aplicar a tratamientos automatizados

A título indicativo, en este apartado se recogen las medidas de seguridad, relacionadas con tratamientos automatizados, que **IBIZA NURSE SERVICE S.L,** como Responsable o Encargado del Tratamiento, puede decidir 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**

- **Actualización**: Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible.

- **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 posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.
- **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.

- **Control de acceso físico y lógico**

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 Sociedad les haya encomendado.
- **Identificación y autenticación**: 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 ni se dejarán anotadas en lugar común y 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 Sociedad.
- 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.

- **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 ANEXO II. 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.

- **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 IV** 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. El **Anexo VI** 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 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 Sociedad, 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**.

- **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.

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

- **Notificación**: Cualquier persona que preste servicios para **IBIZA NURSE SERVICE S.L** 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** o con una aplicación de gestión de incidencias. En cualquiera

de los dos sistemas se deben 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 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, con 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 **IBIZA NURSE SERVICE S.L** 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.

- **Copias de seguridad**

La posibilidad de que en una incidencia puedan perderse datos personales que constan en los sistemas informáticos de **IBIZA NURSE SERVICE S.L**, 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.

- **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.

- **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.

- **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**.

- **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 Sociedad; 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 Sociedad podrá poner en marcha, de forma inmediata, su actividad.

6.2. Medidas de Seguridad a aplicar a tratamiento no automatizados

A título indicativo, en este apartado se recogen las medidas de seguridad, relacionadas con tratamientos no automatizados, que **IBIZA NURSE SERVICE S.L,** como Responsable o Encargado del Tratamiento, puede decidir 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.

- **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 Sociedad 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 las medidas de seguridad físicas implementadas para evitar el acceso indiscriminado son las siguientes: **alarma con videovigilancia/ puerta de acceso con llave**.

- **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. El **Anexo IV** del presente Manual de Protección de Datos recoge la plantilla para el registro de incidencias que afecten a datos personales.

Todo aquello acontecido que se considere una incidencia debe quedar debidamente reflejado en un Registro habilitado al efecto.

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

- **Notificación**: Cualquier persona que preste servicios para **IBIZA NURSE SERVICE S.L** 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, con 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.

- **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, **IBIZA NURSE SERVICE S.L**,:

- 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

- **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.

- **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

6.4.1. Introducción

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***.

Es necesario recalcar que este concepto de brecha de seguridad sólo es aplicable a las incidencias de seguridad que afecten a **datos personales**.

Siguiendo la **Guía para la gestión y notificación de brechas de seguridad de la Agencia Española de Protección de Datos (AEPD)**, el presente procedimiento contempla las siguientes **fases** para la correcta gestión de brechas de seguridad:

<table>
<tr><th colspan="6">Procedimiento de gestión y notificación de brechas de seguridad</th></tr>
<tr><th colspan="2">Incidentes de seguridad</th><th colspan="4">d Brechas de seguridad</th></tr>
<tr><td rowspan="3">1. Preparación</td><td rowspan="3">2. Detección / Identificación</td><td>d</td><td colspan="2">Plan de actuación</td><td rowspan="3">6. Seguimiento y cierre</td></tr>
<tr><td rowspan="2">3. Análisis / Clasificación</td><td>4. Proceso de respuesta</td></tr>
<tr><td>5. Proceso de notificación</td></tr>
</table>

6.4.2. Preparación

Si la empresa está preparada para afrontar la gestión de una incidencia de seguridad podrá responder de forma rápida, ordenada y eficaz al evento, minimizando las consecuencias sobre la propia empresa y terceras partes implicadas.

Para ello, será necesario que la empresa **documente** debidamente el proceso de gestión de la brecha de seguridad producida, a través de:

- **Manual de Protección de Datos**: recoge las políticas y procedimientos de seguridad de la empresa, del que el presente procedimiento forma parte. En este Manual de Protección de Datos y sus Anexos se recogen también los soportes y aplicaciones, así como las medidas técnicas y organizativas implantadas por la empresa para proteger los datos personales y garantizar su seguridad (confidencialidad, integridad y disponibilidad).
- **Procedimientos de gestión de incidencias** y su correspondiente **Registro de Incidencias** (*recogidos en el Manual de Protección de Datos de la empresa*). Este Registro de Incidencias debe completarse cada vez que se produzca una incidencia de seguridad que pueda afectar a datos personales.
- **Asignación de los recursos humanos y medios materiales** necesarios para la correcta gestión y solución de las incidencias de seguridad: notificación, registro y gestión de las incidencias.

  Para, como mínimo, aquellas incidencias de seguridad que se sospeche puedan causar una brecha de seguridad, indicar:

  - Datos de los **recursos humanos** asignados:
    - El **responsable del tratamiento**, que es quien decide acerca del tratamiento y quien asume la responsabilidad de los tratamientos de datos personales que se llevan a cabo en la empresa.

Responsable del Tratamiento	*(indicar)*

- En caso de haber sido nombrado (de forma obligatoria o voluntaria), el **delegado de protección de datos (DPD),** que es quien se debe encargar de supervisar la licitud de los tratamientos, informando y asesorando al responsable del tratamiento.

Delegado de protección de datos	*(indicar)*

- El **responsable de seguridad técnico** de la empresa, que es la persona encargada de supervisar los controles y medidas necesarias para proteger los datos y controlar su eficacia.

Responsable de seguridad técnico	*(indicar)*

- El o los **responsables funcionales** de la o de las actividades de tratamiento afectadas por la incidencia de seguridad, que es, junto con el o los **usuarios** de los datos personales, quienes podrán proporcionar información sobre la ocurrencia de la incidencia.

Responsable/s Funcional/es	*(indicar)*
Usuario/s de los datos	*(indicar)*

- El o los **encargados del tratamiento** que puedan apoyar al responsable del tratamiento en la correcta gestión y notificación de las incidencias de seguridad.

Encargado/s del tratamiento	*(indicar)*

- El **responsable de notificar** la posible brecha de seguridad a la AEPD y a los interesados.

Responsable de notificar la brecha	*(indicar)*

- Los **<u>medios materiales</u>** necesarios para la gestión de la incidencia y su correcta resolución:

Aplicaciones	*(indicar)*
Medidas	*(indicar)*
Otros	*(indicar)*

- **<u>Análisis de riesgos</u>** (*realizado a través del Formulario de Verificación para evaluar la necesidad de realizar una Evaluación de Impacto – EIPD*) de la o de las actividades de tratamiento afectadas por la incidencia de seguridad.

- **EIPD** (*en caso de ser necesaria)* de la o de las actividades de tratamiento afectadas por la incidencia de seguridad.
- **Plan de contingencia** de la empresa, que deberá ser acorde al riesgo del tratamiento de los datos e incorporar medidas técnicas y organizativas necesarias para restablecer la situación.

6.4.3. Detección / Identificación

Durante esta fase se deben **concretar**:

- las situaciones que se consideran incidentes de seguridad y
- las fuentes, herramientas o mecanismos de detección o sistemas de alerta.

Para detectar incidentes de seguridad, la empresa recurre a:

- **Fuentes internas**: *(dejar o marcar únicamente aquellas fuentes utilizadas por la empresa para detectar incidentes)*
  - **Notificación de incidencias por parte de los usuarios de los datos**, como, por ejemplo:
    - presencia de archivos con caracteres inusuales,
    - recepción de correos electrónicos con archivos adjuntos sospechosos,
    - comportamiento extraño de dispositivos,
    - imposibilidad de acceder a ciertos servicios,
    - extravío/robo de dispositivos de almacenamiento o equipos con información
    - avisos de software antivirus
    - otros: _____
  - **Incidentes detectados o gestionados por personal técnico de la empresa**, como, por ejemplo:
    - avisos de software antivirus
    - analizadores de logs
    - consumidores excesivos de memoria o disco en servidores y equipos
    - anomalías de tráfico de red o picos de tráfico en horas inusuales
    - alertas de sistemas de detección/prevención de intrusión (IDS/IPS)
    - alertas de sistemas de correlación de eventos
    - análisis de registros de conexiones realizadas a través de proxys corporativos o conexiones bloqueadas en los cortafuegos
    - análisis de registro de servidores y aplicaciones con intentos de acceso no autorizados
    - análisis de registros en herramientas DLP (Data Loss Prevention)
    - escáner de vulnerabilidades del sistema

- avisos de seguridad de fuentes externas
- amenazas explícitas de ataques a los sistemas de información de la empresa
  - otros: _____
- *(indicar otras fuentes internas)*

- **Fuentes externas**: *(dejar o marcar únicamente aquellas fuentes utilizadas por la empresa para detectar incidentes)*
  - **Avisos/alertas de seguridad proporcionados por**:
    - **Incibe** (Instituto Nacional de Cyberseguridad): https://www.incibe.es/suscripciones
    - **CCN** (Centro Criptográfico Nacional): https://www.ccn-cert.cni.es/seguridad-al-dia.html
    - **OSI** (Oficina de Seguridad del Internauta): https://www.osi.es/es/boletines/suscribirse
    - **Fuerzas y Cuerpos de Seguridad del Estado / Cuerpo Nacional de Policía:** https://www.policia.es/prensa/historico/prensa_1.html
    - **Facua – Consumidores en acción:** https://www.facua.org/
    - **Medios de comunicación,** como:
      - https://retina.elpais.com/
      - Otros: _____
    - **Organismos públicos**, como:
      - _____
  - **Proveedores** de servicios informáticos, de servicios de internet, fabricantes de soluciones de seguridad, consultorías informáticas, etc.:
    - ...
    - ...
    - ...
  - *(si la empresa está suscrita a algún otro boletín de noticias de seguridad o visita frecuentemente páginas web o recibe revistas sobre seguridad, indicar en este punto)*
- **Encargados del tratamiento** que puedan comunicar una incidencia de seguridad a la empresa.
- **Clientes** que se pueden ver afectados por una incidencia de seguridad y se la comuniquen a la empresa.
- *(indicar otras fuentes externas)*

Las **situaciones identificadas** que la empresa considera como incidencias de seguridad o que pueden dar lugar a un incidente de seguridad son: *(dejar o marcar únicamente aquellas situaciones identificadas por la empresa)*

- Incumplimiento o vulneración por parte de los usuarios de los datos de las políticas y medidas adoptadas por la empresa (mesas limpias, bloqueo de pantallas, accesos con usuario y contraseña, detección de intrusos, videovigilancia, control y registros de acceso, etc.).
- Contratación de encargados del tratamiento negligentes
- Pérdida de confidencialidad de datos sujetos al secreto profesional
- Usurpación de la identidad
- Acceso a cuentas privilegiadas
- Pérdida de control sobre los datos personales o restricción de sus derechos
- Pérdida de un dispositivo con datos personales (portátil, pen drive, Smartphone, etc.)
- Robo y filtración de datos
- Publicación accidental de datos personales
- Reversión no autorizada de la seudonimización
- Documentos desechados sin adoptar medidas de seguridad adecuadas
- Insuficiente o errónea implantación de las medidas de seguridad
- Otros: _____

La empresa debe anotar en su **Registro de Incidencias** aquellos incidentes de seguridad detectados e identificados como incidencias de seguridad que afecten a datos personales. Este Registro contiene los siguientes campos:

- Nº de incidencia
- Fecha y hora de la incidencia
- Tipo de incidencia
- Descripción de la incidencia
- Persona que notifica la incidencia
- Persona a quien se notifica la incidencia
- Gravedad de la incidencia
- Estado de la incidencia
- Efectos producidos
- Medidas adoptadas para su resolución
- *(añadir, si es el caso, otros campos existentes en el Registro de incidencias utilizado por la empresa)*

Incidencia de seguridad detectada

Indicar a continuación una descripción de la incidencia detectada y registrada que ser clasificada posteriormente como brecha de seguridad:

Incidente de seguridad	*(indicar una breve descripción del incidente)*
Controles/medidas existentes en el momento del incidente	*(indicar)*

6.4.4. Plan de actuación – Análisis / Clasificación

En esta fase es importante discernir si la **incidencia de seguridad** que se está gestionando y se ha registrado debidamente en el Registro de Incidencias es simplemente un **incidente de seguridad** o si se trata realmente de una **brecha de seguridad**. Es importante tener en cuenta que todas las brechas de seguridad son incidentes de seguridad, pero no todos los incidentes de seguridad son necesariamente brechas de seguridad.

Clasificación de la incidencia de seguridad:

En caso de sospecharse que un incidente de seguridad es también una brecha de seguridad, para poder clarificar dicha sospecha, **la incidencia registrada deberá clasificarse por**:

- **Tipo de amenaza (origen de la incidencia)**: *(dejar o marcar el tipo correspondiente)*
  - 0-day - vulnerabilidad no conocida que permite a un atacante el acceso a datos personales hasta que la vulnerabilidad es resuelta por el fabricante o desarrollador.
  - APT – ataque dirigido con el objetivo de recabar información que permita continuar con ataques más sofisticados (mail enviado a empleados con malware y su instalación en un equipo proporcionando una puerta de entrada al sistema).
  - Denegación del servicio (DoS/DDoS) – ataque cuyo objetivo es inundar de tráfico un sistema hasta que éste no sea capaz de dar servicio a los usuarios legítimos del mismo.
  - Acceso a cuentas privilegiadas – ataque que se consigue a través de una cuenta de un usuario con privilegios avanzados (previamente ha tenido que conseguir el nombre de usuario y contraseña de este usuario), lo que le permite libertad de acciones en el sistema.
  - Código malicioso – ataque realizado a través de una pieza de software con el objetivo de infiltrarse o dañar un equipo de red con finalidades diversas (un usuario puede instalarlo de forma involuntaria).

- Compromiso de la información – cualquier ataque o incidente relacionada con el acceso no autorizado y la fuga, modificación o borrado de información no pública.
- Robo y/o filtración de datos – pérdida o robo de dispositivos de almacenamiento de información.
- Desfiguración (defacement) – ataque dirigido cuyo objetivo es la modificación de una web corporativa con la intención, por ejemplo, de colgar mensajes reivindicativos con intenciones diversas.
- Explotación de vulnerabilidades de aplicaciones – ataque cuyo objetivo es explotar una vulnerabilidad existente en un sistema o producto consiguiendo comprometer una aplicación utilizada por la empresa.
- Ingeniería social – ataque basado en el engaño, llevado a cabo generalmente a través de redes sociales, que consiste en dirigir la conducta de una persona u obtener información sensible (por ejemplo, que un usuario pulse un enlace haciéndole pensar que es lo correcto).
- Otro: *(anotar una breve descripción del incidente en función de la información de la que se disponga)*

- **Contexto u origen de la amenaza**: *(dejar o marcar el contexto u origen correspondiente)*
  - Interna
  - Externa
- **Categoría de seguridad de los sistemas y datos afectados**: *(indicar)*
  - _____
- **Vector de ataque o método** (ruta o medio por el que se ha materializado el incidente): *(indicar)*
  - _____

Valoración del incidente de seguridad y su alcance

Para valorar si el incidente de seguridad es o no una brecha de seguridad, así como su alcance, la empresa debe determinar su **peligrosidad**: *(dejar o marcar la valoración correspondiente)*

- **Categoría o nivel de criticidad** respecto a la seguridad de los sistemas afectados:
  - Crítico (afecta a datos valiosos, gran volumen y en poco tiempo)
  - Muy alto (cuando dispone de capacidad para afectar a información valiosa, en cantidad apreciable)
  - Alto (cuando dispone de capacidad para afectar a información valiosa)
  - Medio (cuando dispone de capacidad para afectar a un volumen apreciable de información)
  - Bajo (escasa o nula capacidad para afectar a un volumen apreciable de información)

- **Naturaleza, sensibilidad y categorías de los datos personales afectados**:
  - Datos sensibles: de salud, biométricos, datos relativos a la vida sexual, etc.
  - Datos financieros: transacciones, posiciones, ingresos, cuentas, facturas
  - Datos de comportamiento: localización, tráfico, hábitos y preferencias
  - Datos de escaso riesgo: datos de contacto, de educación, familiares, profesionales, biográficos
- **Datos legibles/ilegibles:**
  - Datos no protegidos mediante algún sistema de cifrado o seudonimizado
  - Datos protegidos mediante algún sistema de cifrado o seudonimizado
- **Volumen de datos personales:**
  - Cantidad (en registros, ficheros, documentos...): (indicar)
  - Periodo de tiempo (por ejemplo: una semana, un mes, un año...): (indicar)
- **Facilidad de identificación de los interesados:**
  - Facilidad alta para deducir la identidad de los interesados a partir de los datos involucrados en la brecha
  - Facilidad media para deducir la identidad de los interesados a partir de los datos involucrados en la brecha
  - Facilidad baja para deducir la identidad de los interesados a partir de los datos involucrados en la brecha
- **Severidad de las consecuencias del incidente para los interesados** (estimación de la magnitud del impacto potencial del incidente en los interesados):
  - Muy alta: las personas pueden enfrentar consecuencias significativas, o incluso irreversibles, que no pueden superar (exclusión o marginación social, dificultades financieras tales como deudas considerables o incapacidad para trabajar, dolencias psicológicas o físicas a largo plazo, muerte, etc.)
  - Alta: las personas pueden enfrentar consecuencias importantes, que deberían poder superar, aunque con serias dificultades (malversación de fondos, listas negras de los bancos, daños a la propiedad, pérdida de empleo, citación judicial, empeoramiento de la salud, etc.)
  - Media: las personas pueden encontrar inconvenientes importantes que podrán superar a pesar de algunas dificultades (costos adicionales, denegación de acceso a servicios comerciales, miedo, falta de comprensión, estrés, dolencias físicas menores, etc.)
  - Baja: las personas no se verán afectadas o pueden encontrar algunos inconvenientes que superarán sin ningún problema (tiempo de reingreso de información, molestias, irritaciones, etc)
- **Características especiales de los interesados:**

  - Afecta a interesados con características especiales o necesidades especiales (como, por ejemplo, menores o pacientes)
  - No afecta a interesados con características especiales o necesidades especiales (como, por ejemplo, menores o pacientes)
- **Número de interesados afectados:**
  - Más de 100.000 interesados
  - Más de 10.000 interesados
  - Más de 1.000 interesados
  - Más de 100 interesados
  - Menos de 100 interesados
- **Características especiales de la empresa:**
  - (describir la actividad/sector u otras características de la empresa)
- **Perfil de los usuarios:**
  - (indicar su posición dentro de la empresa y sus privilegios de acceso a los datos personales afectados por la brecha de seguridad)
- **Número y tipología de los sistemas afectados:**
  - (indicar número de sistemas afectados)
  - (indicar la tipología de los sistemas afectados)
- **Impacto de la brecha en la empresa** (desde el punto de vista de la protección de la información, la categoría o criticidad de los servicios afectados, la conformidad legal y/o la imagen pública):
  - Alto (perjuicio muy grave)
  - Medio (perjuicio grave)
  - Bajo (perjuicio limitado)
- **Requerimientos legales y regulatorios**:
  - Notificación de la brecha a la AEPD y cualquier otra obligación de notificación
  - Comunicación a Fuerzas y Cuerpos de Seguridad del Estado en caso de delito.

Para determinar si un incidente de seguridad es o no una brecha de seguridad deberán tenerse en cuenta los resultados de:

- el análisis de riesgos o EIPD (si se ha realizado) realizado con anterioridad al tratamiento de los datos personales
- la clasificación del incidente
- la valoración del incidente/brecha de seguridad y su alcance

Por lo tanto, teniendo en cuenta el análisis del incidente de seguridad registrado, la empresa debe determinado si este incidente de seguridad es o no una **brecha de seguridad**:

Incidente de seguridad	*(indicar una breve descripción del incidente)*
Brecha de seguridad	*(indicar sí o no)*

Una vez se ha determinado que el incidente de seguridad analizado es una **brecha de seguridad**, la empresa la debe **clasificar** en una o varias de las siguientes categorías:

- **Brecha de confidencialidad**: se produce cuando terceros no autorizados acceden a la información. La severidad de la pérdida de confidencialidad varía según el alcance de la divulgación, es decir, el número potencial y el tipo de partes que pueden haber accedido ilegalmente a la información.
- **Brecha de integridad**: se produce cuando se altera la información original y la sustitución de datos puede ser perjudicial para el individuo. La situación más grave ocurre cuando existen serias posibilidades de que los datos alterados se hayan utilizado de una manera que pueda dañar al individuo.
- **Brecha de disponibilidad**: su consecuencia es que no se puede acceder a los datos originales cuando es necesario. Puede ser temporal (los datos son recuperables, pero tomará un periodo de tiempo y esto puede ser perjudicial para el individuo), o permanente (los datos no pueden recuperarse).

Por lo tanto, teniendo en cuenta los tipos de brechas de seguridad, la empresa ha determinado que la brecha de seguridad producida en la empresa es:

Brecha de seguridad	*(indicar si es una brecha de confidencialidad, integridad y/o disponibilidad)*
Peligrosidad de la brecha	*(indicar la peligrosidad de la brecha: muy alta, alta, media, baja, muy baja)*

Investigación, comunicación y coordinación de los medios internos/externos implicados

En este punto es importante saber cómo se va a tratar la incidencia/brecha de seguridad, quien se va a encargar de cada tarea y cómo se escalan a los equipos internos o externos adecuados *(el procedimiento de gestión de incidencias está descrito en el Manual de Protección de Datos):*

- **Notificación**: cualquier persona/usuario que preste servicios para la empresa 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/brecha de seguridad 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** registrará la incidencia/brecha de seguridad en el Registro de Incidencias de la empresa. El **responsable de seguridad técnico** es responsable de poner en marcha unas primeras medidas de contención.
- **Gestión**: El **responsable de seguridad técnico** comunicará la incidencia/brecha de seguridad 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, con la mayor brevedad posible, los técnicos den respuesta a la incidencia/brecha de seguridad detectada y supervisará personalmente la actividad de estos y la subsanación de la anomalía. El **responsable de seguridad técnico** comunicará la incidencia/brecha de seguridad a la **empresa**, al **delegado de protección de datos** y al **responsable de su notificación a la AEPD y a los afectados**, principalmente si la incidencia/brecha de seguridad puede afectar a los derechos y libertades de los interesados. Finalizada la incidencia/brecha de seguridad, 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

6.4.5. Plan de actuación – Proceso de respuesta

Figuras implicadas

Una vez que la empresa ha determinado que el incidente de seguridad es una brecha de seguridad se requiere la participación de las siguientes figuras:

- **Responsable del tratamiento** - encargado de aplicar las medidas técnicas y organizativas para demostrar que el tratamiento es conforme al RGPD, así como de notificar la brecha de seguridad a la AEPD sin dilación indebida y, en su caso, a los interesados
- **Expertos en materia de seguridad** – asesorar al responsable del tratamiento
  - puede ser personal de la propia empresa: **responsable de seguridad técnico** / departamento de informática de la empresa
  - o subcontratados: empresa o personal externo contratado para asesorar a la empresa en materia de seguridad
- **Encargado del tratamiento**: *(dejar o marcar la opción correspondiente)*

  - Notificar al responsable del tratamiento, sin dilación indebida, la brecha de seguridad, con indicación de toda aquella información mínima y necesaria para su comunicación
  - Gestionar la brecha de seguridad en nombre del responsable del tratamiento (teniendo presente que la delegación de funciones no implica la delegación de responsabilidad)
- **Delegado de protección de datos (DPD)** - en caso de ser asignado, el DPO es el encargado de liderar el plan de actuación en todos sus aspectos
- **Responsable funcional y usuarios de los datos** – dependiendo del incidente/brecha de seguridad, es posible que estas figuras sean quienes puedan proporcionar información sobre el problema.
- **AEPD** - encargada de verificar que se cumple con el RGPD y, en este caso concreto, en lo relativo a la gestión de la brecha de seguridad

Fase de contención del incidente/brecha de seguridad

Durante el proceso de respuesta, y como se ha descrito en el procedimiento de gestión de incidencias, la empresa, en una primera fase, intenta **contener el incidente/brecha de seguridad** adoptando medidas de seguridad de contención, como, por ejemplo:

- impidendo el acceso al origen de la divulgación (dominios, puertos, servidores, conexiones, equipos informáticos, conexiones remotas, etc.),
- cerrando un sistema,
- desconectando un ordenador infectado de la red corporativa,
- deshabilitar a un equipo ciertas funciones,
- retirando inmediatamente una información difundida erróneamente a través de internet,
- suspendiendo las credencias lógicas y físicas con acceso a información privilegiada,
- cambiando las contraseñas de seguridad de usuarios privilegiados o haciendo que los usuarios de manera segura,
- haciendo una copia de seguridad del sistema (clonado), una copia bit a bit del disco duro que contiene el sistema y analizado la copia utilizando herramientas forenses,
- aislando el sistema utilizado para revelar los datos con el fin de realizar un análisis forense más tarde,
- si los datos han sido enviados a servidores públicos, solicitando al propietario (o webmaster) que elimine los datos divulgados,
- si no es posible eliminar los datos divulgados, proporcionando un análisis completo al departamento correspondiente (legal, compliance, recursos humanos, etc.) o a quien ejerza dichas funciones en la empresa

- vigilando la difusión de lso documentos/datos filtrados en los diferentes sitios web y redes sociales, así como los comentarios y reacciones de los usuarios de internet.
- etc.

Dependiendo de la medida a adoptar, ésta podría ser tomada por el propio usuario de forma rápida, incluso antes de confirmar si se trata de un incidente de seguridad.

En este punto, indicar las medidas adoptadas por la empresa para contener el incidente/brecha de seguridad:

Medidas adoptadas por el profesional para contener el incidente/brecha	Orden de prioridad	Responsables asignados	Tiempos estimados	Efectos esperados

Estas medidas de contención proporcionan tiempo a la empresa para poder desarrollar una estrategia a medida, una solución adecuada.

Fase de erradicación

En esta fase, la empresa intenta **solventar determinados efectos** del incidente/brecha de seguridad adaptando medidas de seguridad, como, por ejemplo:

- eliminar un malware,
- desactivar cuentas de usuarios vulneradas,
- definir el proceso de desinfección, basado en firmas, herramientas, nuevas versiones/revisiones de software, etc. y probarlo,
- asegurar que el proceso de desinfección funciona correctamente, sin dañar servicios,
- comprobar la integridad de los datos almacenados en el sistema, mediante un sistema de hashes, por ejemplo, que permita garantizar que los ficheros no han sido modificados,
- revisar la correcta planificación y actuación de los motores y firmas de antivirus,
- análisis de antivirus de todo el sistema, los discos duros y la memoria,
- restaurar conexiones y privilegios paulatinamente,

- etc.

En este punto, indicar las medidas adoptadas por la empresa para contener el incidente/brecha de seguridad:

Medidas adoptadas por el profesional para erradicar la situación generada	Orden de prioridad	Responsables asignados	Tiempos estimados	Efectos esperados

El objetivo de esta fase es evitar o eliminar la posibilidad de que el incidente/brecha de seguridad vuelva a producirse. En este sentido, se debe revisar el listado de posibles escenarios de riesgos (PER) para comprobar si el riesgo estaba identificado en el mismo y, en caso necesario, reevaluar en su caso las medidas de salvaguarda que se hubieran impuesto con la finalidad de garantizar su efectividad. Esta fase también sirve para identificar y mitigar todas las vulnerabilidades que hubiesen sido explotadas.

Fase de recuperación

Esta fase tiene como objetivo el **restablecimiento del servicio** en su totalidad, confirmando su funcionamiento normal y evitando en la medida de lo posible que sucedan nuevos incidentes basados en la misma causa.

Esto puede implicar tanto la adopción de medidas activas como la implantación de controles periódicos y eficaces que permitan el seguimiento pormenorizado de los procesos de mayor riesgo.

Se deben identificar las distintas soluciones dirigidas a evitar nuevos incidentes/brechas de seguridad basados en la misma causa, así como reducir el riesgo de los mismos.

Soluciones: Medidas activas y controles periódicos	Orden de prioridad	Responsables asignados	Tiempos estimados	Efectos esperados

Durante todo el ciclo de vida del procedimiento de gestión de la brecha de seguridad, y en especial en el proceso de respuesta, se deben recolectar y custodiar las **evidencias** que permitan disponer de información presentable ante terceros. Así mismo, todo el proceso de respuesta queda debidamente **documentado**, incluyendo las conclusiones de los técnicos y responsables del equipo para extraer lecciones aprendidas y ser incluidas en un **informe final** *(ver contenido de este informe en el punto "Seguimiento y cierre").*

6.4.6. Plan de actuación – Proceso de notificación

Notificación a la AEPD

Tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de seguridad, debe notificarla a la AEPD sin dilación y a más tardar en las 72 horas siguientes, **a menos que sea improbable que la brecha constituya un riesgo para los derechos y libertades de las personas físicas (los titulares de los datos).** En caso necesario, si el responsable del tratamiento se acoge a esta excepción deberá demostrarlo.

Esta notificación deberá realizarse a través del **formulario** facilitado por la AEPD en su página web: https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/procedimientoBrechaSeguridad.jsf

Si la notificación no se realiza en el plazo de 72 horas, deberá justificar los motivos de la dilación.

Si en el momento de la notificación, no fuese posible facilitar toda la información, se facilitará posteriormente, de manera gradual. La primera notificación se realizará en las primeras 72h y al menos se realizará una comunicación final o de cierre cuando se disponga de toda la información relativa al incidente. Cuando se realice la primera notificación se informará si proporcionará más información a posteriori.

Cuando una brecha de seguridad pueda afectar a los datos de personas en más de un Estado miembro, se realizará una evaluación sobre cuál es la autoridad principal a la que se deberá realizar la notificación y, en caso de duda, se notificará, como mínimo, a la autoridad de control local donde la brecha ha tenido lugar.

En el siguiente enlace se podrán encontrar la identificación y datos de contacto de todas las diferentes Autoridades de Control: http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

Notificación a los interesados

Si la brecha de seguridad entraña un **alto riesgo** para los derechos y libertades de los titulares de los datos, el responsable del tratamiento también deberá comunicar la brecha a estos **interesados**, sin dilación indebida y con un lenguaje claro y sencillo, de forma concisa y transparente, **salvo que:**

- el responsable del tratamiento haya adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se hayan aplicado a los datos personales afectados por la brecha la seguridad, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;
- el responsable del tratamiento haya tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado;
- suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

Existen diversos **factores** a tener en consideración para decidir si se ha de realizar la comunicación a las personas afectadas:

- Cuáles son las obligaciones legales y contractuales.
- Riesgos que comporta la pérdida de los datos: daños físicos, daños reputacionales, etc.
- Si existe un riesgo razonable de suplantación de identidad o fraude (en función del tipo de información que se ha visto afectada y teniendo en cuenta si la información estaba seudonimizada o cifrada).
- Hasta qué punto la persona afectada puede evitar o mitigar posibles daños posteriores.

Se describirá en un lenguaje claro y sencillo, de forma concisa y transparente la naturaleza de la violación de la seguridad de los datos personales y **contendrá, como mínimo, la siguiente información**:

- El nombre y los datos de contacto del delegado de protección de datos (DPD) o de otro punto de contacto en la empresa del que se pudiere obtener información.
- Descripción general del incidente/brecha de seguridad y momento en que se ha producido.
- Descripción de las posibles consecuencias de la brecha de seguridad.
- Descripción de los datos e información personal de los afectados.
- Resumen de las medidas implantadas hasta el momento para controlar los posibles daños.
- Otras informaciones útiles a los afectados para proteger sus datos o prevenir posibles daños.

La notificación preferentemente se realizará de forma directa al afectado, ya sea por teléfono, correo electrónico, SMS, a través de correo postal, o a través de cualquier otro medio dirigido al afectado que la empresa considere adecuado.

La notificación indirecta, a través de avisos públicos en sitios web como blogs corporativos, o comunicados de prensa, se utilizará cuando para la notificación directa los costos sean excesivos o cuando no sea posible contactar con las personas afectadas (por ejemplo, porque se desconocen, o los datos de contacto no están actualizados).

Notificación a las Fuerzas y Cuerpos de Seguridad.

Si es necesario, la brecha será comunicada también a las **Fuerzas y Cuerpos de Seguridad**.

6.4.7. Seguimiento y cierre

En esta fase se llevarán a cabo **tareas** de seguimiento y cierre como, por ejemplo:

- Valoración de contratación de un **análisis forense digital experto** – con el objetivo de analizar los hechos y recopilar evidencias precisas.
- Valoración de adopción de **medidas procesales** – iniciar un procedimiento judicial fines de imputación de hechos y reparación del daño. No obstante, se tendrá en cuenta el daño que pueda derivarse del proceso judicial, ya que éste podría incrementar el perjuicio en lugar de reducirlo.
- Realización de un **informe final** sobre la brecha de seguridad – el delegado de protección de datos (DPD) o, en caso de no haberse designado un DPD, la persona asignada por la empresa:
  - comprobará que las medidas correctoras adoptadas son adecuadas para la resolución de la brecha y para la minimización del riesgo en caso de que produzca otra de similares características
  - comprobará que ha concluido el proceso de notificación a la AEPD y, en su caso, a los interesados

- elaborará un informe final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final. Este informe incluirá toda la información y documentación relativa a la brecha:
  - Dirección de la empresa
  - Alcance e impacto del incidente/brecha de seguridad
  - Controles preventivos existentes
  - Acciones de respuesta tomadas sobre las diferentes alternativas consideradas para la resolución del incidente/brecha de seguridad.
  - Acciones tomadas para la prevención de futuros incidentes/brechas de seguridad.
  - Impacto en la resolución del incidente/brecha de seguridad de las acciones de respuesta tomadas.
  - Acciones definidas para el seguimiento.

- **Cierre** de la brecha de seguridad – una vez las acciones derivadas de los procesos del plan de actuación han concluido y se han alcanzado los objetivos, se procederá al cierre de la brecha de seguridad.

6.4.8. Ejemplos prácticos de brechas de seguridad

Ejemplo	Notificación a la autoridad de control	Notificación a los interesados
Ciberataque a una web segura administrada por una empresa en la que se roban datos personales de los usuarios Los clientes son de un solo Estado de la UE.	**Sí -** Informar a la autoridad supervisora competente si hay consecuencias potenciales para las personas	**Sí -** Informar a las personas dependiendo de la naturaleza de los datos personales afectados y si la gravedad de las posibles consecuencias es alta para las personas
Un centro de recepción de llamadas de un responsable de tratamiento se ve afectado por un corte de energía y los clientes no pueden llamar ni acceder a sus datos	**No**	**No**
Un responsable sufre un ataque de ransomware de encriptación que produce el cifrado de todos los datos	**Sí -** informar a la autoridad supervisora competente si hay posibles consecuencias	**Sí -** informar a las personas, según la naturaleza de los datos personales afectados y

de la compañía. No hay copias de seguridad realizadas y los datos no se pueden restaurar.	para las personas, ya que esto es una pérdida de información y disponibilidad.	el posible efecto de la falta de disponibilidad de los datos, así como otras consecuencias probables
Una empresa de comercio electrónico (compras a través de internet) sufre un ciberataque y se publican on-line los nombres de usuario, las contraseñas y el historial de compras de esos usuarios	**Sí -** informar a la autoridad supervisora principal si involucra procesamiento transfronterizo	**SI**, ya que podría conducir a un alto riesgo
En un hospital los registros médicos no están disponibles durante un período de 30 horas debido a un ciberataque.	**Sí -**el hospital está obligado a notificar que puede haber un alto riesgo para el paciente y su privacidad.	**Sí -** informar a las personas afectadas.
En un Colegio o centro educativo de menores se envían datos personales de estudiantes a una dirección de correo errónea y con una lista de distribución de 150 destinatarios	**Sí**	**Sí -** informe a las personas según el alcance y el tipo de datos personales involucrados y la gravedad de las posibles consecuencias.

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

Tal y como establece el RGPD y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales relativo a la Protección de las Personas físicas,, **IBIZA NURSE SERVICE S.L** está obligada a llevar a cabo una EIPD si realiza uno de los siguientes tratamientos de datos:

- Una evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
- Un tratamiento a gran escala de las categorías especiales de datos o de los datos personales relativos a condenas e infracciones penales;
- Una observación sistemática a gran escala de una zona de acceso público.

Además, **IBIZA NURSE SERVICE S.L** deberá revisar periódicamente si alguno de los tratamientos de datos que realiza está incluido en las Listas publicadas por la Agencia Española de Protección de Datos (AEPD).

Independientemente de los supuestos obligados por el RGPD o por la AEPD, cada Responsable Funcional deberá realizar una primera aproximación al análisis de riesgos en base a la información contenida en el Registro de Actividades de Tratamiento (**Anexo I**) y a la información que conozca por su propia experiencia en el desarrollo de sus funciones para la Sociedad.

Para ello, deberá completar el formulario de verificación que se adjunta como **Anexo XVII**. Este formulario deberá ser revisado periódicamente por el Responsable Funcional correspondiente (cada 6 meses o en caso de que se produzcan modificaciones en el tratamiento de los datos, como recogida de nuevas categorías de datos, utilización de nuevas aplicaciones, diferentes destinatarios, etc.).

El Responsable Funcional deberá poner en conocimiento del DPO los resultados, indicando si ha habido alguna modificación en los mismos respecto al último formulario de verificación.

Si del resultado del formulario de verificación se deduce que es probable que algún tratamiento de datos conlleva un **alto riesgo** para los derechos y libertades de los individuos, la Sociedad deberá realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD).

Para la realización de la EIPD **IBIZA NURSE SERVICE S.L** se basará en una metodología sistemática, documentada y repetible, con el fin de que poder valorar cómo evoluciona el nivel de riesgo en función de las decisiones que se vayan adoptando y de la propia evolución del tratamiento de los datos.

Se comenzará identificando las **Actividades de Tratamiento afectadas** por los tratamientos de datos que pueden conllevar un alto riesgo para los derechos y libertades de los individuos.

Para cada Actividad de Tratamiento afectada, se realizará una **descripción sistemática de las operaciones de tratamiento previstas y de sus fines**:

- **entrada** de los datos (origen de los datos, base legítima del tratamiento, finalidad/es),
- **clasificación** de los datos (dependiendo de su utilidad: identificar a la persona, conocer aspectos de su personalidad, evaluarla…),
- **activos** (aplicaciones, documentos y otros soportes, dispositivos o tecnologías utilizadas para el tratamiento de los datos, y dónde están almacenados),
- **agentes** (personas, áreas o empresas involucradas en el tratamiento de datos, y qué función realizan para llevar a cabo dicho tratamiento);
- **procesos clave** (operaciones imprescindibles para alcanzar la finalidad del tratamiento de los datos: alta de los interesados (empleado, proveedor, cliente…), consulta, seguimiento, pago, etc.)

En este punto, **IBIZA NURSE SERVICE S.L** deberá **valorar y justificar la necesidad y proporcionalidad** de la Actividad del Tratamiento con respecto a su finalidad, es decir, si los datos tratados, los activos utilizados, los agentes con acceso a los datos y los procesos clave (operaciones de tratamiento) son o no prescindibles para alcanzar dicha finalidad.

En el siguiente paso, se relacionará cada proceso clave de cada Actividad de Tratamiento afectada con los datos, activos y agentes utilizados, de forma que se pueda obtener una visión exacta de cada **flujo de información**: quién accede y en qué momento a datos personales concretos.
Una vez se obtenga esta información, se procederá a **gestionar el riesgo**. Para ello, se **identificarán** los posibles escenarios de riesgo (PER) a los que puedan estar expuestos los datos personales, se **analizarán** las medidas ya adoptadas para mitigar dichos riesgos y se **valorará** la probabilidad de que se produzcan y la gravedad, si se producen, para los derechos y libertades de los interesados.

En caso de resultar necesario, se deberá **tratar el riesgo** a través de medidas correctivas que definitivamente eliminen o reduzcan dicho riesgo a un nivel aceptable.

7. Derechos de protección de datos

7.1. Derecho de información

Según el principio de transparencia, principio vinculado al derecho de información, **IBIZA NURSE SERVICE S.L**, 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.

IBIZA NURSE SERVICE S.L 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 de 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, **IBIZA NURSE SERVICE S.L** 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 XIV**, 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.

IBIZA NURSE SERVICE S.L 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.

IBIZA NURSE SERVICE S.L 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.

Nombre y Apellidos: **Mª Victoria Cegarra Gutierrez**

IBIZA NURSE SERVICE S.L, 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 **IBIZA NURSE SERVICE S.L** 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.

IBIZA NURSE SERVICE S.L 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, **IBIZA NURSE SERVICE S.L** 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 Sociedad 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 XI** del presente Manual de Protección de Datos.
- Si la solicitud no reúne los requisitos recogidos en el primer punto, la Sociedad debe solicitar su subsanación.
- La Sociedad 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 XII** 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 XII** 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 **IBIZA NURSE SERVICE S.L** 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 Sociedad 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 XI** 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 Sociedad debe solicitar su subsanación.
- La Sociedad 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 XII** 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 XII** 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 Sociedad deberá comunicarles la rectificación para que ellas también la efectúen.

7.4. Derecho de supresión y derecho al olvido

Los interesados pueden solicitar a **IBIZA NURSE SERVICE S.L** 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.

- Para ejercitar el derecho de supresión, el titular de los datos deberá dirigir a la Sociedad 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 XI** 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 Sociedad debe solicitar su subsanación.
- La Sociedad 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 XII** 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 XII** 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 Sociedad 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 **IBIZA NURSE SERVICE S.L** 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 Sociedad 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 XI** 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 Sociedad debe solicitar su subsanación.
- La Sociedad 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 XII** 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 XII** 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 Sociedad 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 **IBIZA NURSE SERVICE S.L,** 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 Sociedad 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 XI** 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 Sociedad debe solicitar su subsanación.
- La Sociedad 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 XII** 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 XII** 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 **IBIZA NURSE SERVICE S.L**, 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 Sociedad 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 XI** 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 Sociedad debe solicitar su subsanación.
- La Sociedad 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 XII** 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 XI** 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, **IBIZA NURSE SERVICE S.L** debe informarle sobre los sistemas de exclusión publicitaria existentes.

1. Anexos

ANEXO I: Registro de Actividades de Tratamiento

ANEXO II: Relación de usuarios

ANEXO III: Listado de prestadores de servicios

ANEXO IV: Registro de incidencias

ANEXO V: Inventario de soportes

ANEXO VI: Registro de entrada y salida de soportes

ANEXO VII: Registro de acceso a datos sensibles

ANEXO VIII: Registro de controles periódicos

ANEXO IX: Delegación de autorizaciones

ANEXO X: Recibo del MPD por los empleados o usuarios

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

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

ANEXO XIII: Nombramientos: Responsables

ANEXO XIV: Cláusulas Informativas

ANEXO XV: Contratos de prestación de servicios

ANEXO XVI: Gestión y Notificación de Brechas de Seguridad

ANEXO XVII: Formulario de Verificación

ANEXO XVIII: Plazos orientativos de conservación de los datos

Anexo XIX: Página Web – Cláusula Informativa y Política de cookies

ANEXO XX: Sello de Calidad y Certificado RGPD

ANEXO I. Registro de Actividades de Tratamiento

Actividad de Tratamiento:	**CLIENTES**
Responsable de Tratamiento:	IBIZA NURSE SERVICE S.L
Delegado de Protección de Datos:	
Responsable Funcional:	Mª Victoria Cegarra Gutierrez
Finalidades:	Gestión contable, fiscal y administrativa de los datos de los clientes.
Base legítima del Tratamiento:	Contrato
Sistema de tratamiento:	Mixto
Plazo de conservación de los datos:	Otros: _____Ley: _____
Categorías de Datos:	
Datos de carácter identificativo:	D.N.I./N.I.F. , Nombre y apellidos , Dirección postal,E-mail,Teléfono, Firma
Otros datos tipificados:	Económicos, financieros y de seguros
Respuesta ejercicio de derechos de protección de datos	
Contacto ejercicio de derechos:	**info@ibizanurseservice.com**
Procedimiento Ejercicio de Derechos:	Apartado 7
Origen y procedencia de los datos:	
Origen de los datos:	El propio interesado o su representante legal ; Entidad privada
Categorías de interesados:	Clientes , Personas de contacto , Representante legal
Mecanismo de recogida de los datos:	Presupuesto, Contrato
Cesión o comunicación de datos:	
Categorías de destinatarios:	Organismos de la Seguridad Social , Administración Tributaria , Bancos, Cajas de Ahorro y Cajas Rurales , Administración Pública con competencia en la materia, Otros destinatarios de cesiones:Consejeria de Sanidad
Transferencia internacional de datos:	No TID
Seguridad	
Activos (servidores, equipos, aplicaciones…)	Apartado 5.2. de este Manual de Protección de Datos
Soportes no automatizados	Anexo IV de este Manual de Protección de Datos
Medidas técnicas y organizativas de seguridad	Apartado 6 de este Manual de Protección de Datos

Actividad de Tratamiento:	**PACIENTES**
Responsable de Tratamiento:	IBIZA NURSE SERVICE S.L
Delegado de Protección de Datos:	
Responsable Funcional:	Mª Victoria Cegarra Gutierrez
Finalidades:	Gestión de los datos de los pacientes para la prestación de asistencia sanitaria. Gestión de la historia clínica.
Base legítima del Tratamiento:	Interés Legítimo
Sistema de tratamiento:	Mixto
Plazo de conservación de los datos:	Otros: _____Ley: _____
Categorías de Datos:	
Categorías especiales de datos:	Salud
Datos de carácter identificativo:	Nombre y apellidos
Otros datos tipificados:	Características personales
Respuesta ejercicio de derechos de protección de datos	
Contacto ejercicio de derechos:	**info@ibizanurseservice.com**
Procedimiento Ejercicio de Derechos:	Apartado 7
Origen y procedencia de los datos:	
Origen de los datos:	El propio interesado o su representante legal
Categorías de interesados:	Pacientes
Mecanismo de recogida de los datos:	Formulario
Cesión o comunicación de datos:	
Categorías de destinatarios:	Fuerzas y cuerpos de seguridad , Otros destinatarios de cesiones:servicios de salud
Transferencia internacional de datos:	No TID
Seguridad	
Activos (servidores, equipos, aplicaciones…)	Apartado 5.2. de este Manual de Protección de Datos
Soportes no automatizados	Anexo IV de este Manual de Protección de Datos
Medidas técnicas y organizativas de seguridad	Apartado 6 de este Manual de Protección de Datos

Actividad de Tratamiento:	**PROVEEDORES**
Responsable de Tratamiento:	IBIZA NURSE SERVICE S.L
Delegado de Protección de Datos:	
Responsable Funcional:	Mª Victoria Cegarra Gutierrez
Finalidades:	Gestión contable, fiscal y administrativa de los datos de los proveedores
Base legítima del Tratamiento:	Contrato
Sistema de tratamiento:	Mixto
Plazo de conservación de los datos:	Facturas: 10 años.Código Penal, Normativa contable, Código de Comercio, Normativa IVA, LIS
Categorías de Datos:	
Datos de carácter identificativo:	D.N.I./N.I.F. , Nombre y apellidos , Dirección postal,E-mail,Teléfono, Firma
Otros datos tipificados:	Características personales ; Económicos, financieros y de seguros
Respuesta ejercicio de derechos de protección de datos	
Contacto ejercicio de derechos:	**info@ibizanurseservice.com**
Procedimiento Ejercicio de Derechos:	Apartado 7
Origen y procedencia de los datos:	
Origen de los datos:	El propio interesado o su representante legal
Categorías de interesados:	Proveedores , Representante legal
Mecanismo de recogida de los datos:	Ofertas, tarjetas de visita, contratos
Cesión o comunicación de datos:	
Categorías de destinatarios:	Administración Tributaria , Bancos, Cajas de Ahorro y Cajas Rurales , Administración Pública con competencia en la materia
Transferencia internacional de datos:	No TID
Seguridad	
Activos (servidores, equipos, aplicaciones…)	Apartado 5.2. de este Manual de Protección de Datos
Soportes no automatizados	Anexo IV de este Manual de Protección de Datos
Medidas técnicas y organizativas de seguridad	Apartado 6 de este Manual de Protección de Datos

Actividad de Tratamiento:	**GESTIÓN DE RRHH**
Responsable de Tratamiento:	IBIZA NURSE SERVICE S.L
Delegado de Protección de Datos:	
Responsable Funcional:	Mª Victoria Cegarra Gutierrez
Finalidades:	Gestión de los recursos humanos de la empresa
Base legítima del Tratamiento:	Contrato
Sistema de tratamiento:	Mixto
Plazo de conservación de los datos:	Nóminas, TC1, TC2, etc.: 10 años: Código Penal, Normativa contable, Normativa laboral, Código de Comercio, Normativa IVA, LIS
Categorías de Datos:	
Otros tipos de datos:	Curriculum Vitae
Datos de carácter identificativo:	D.N.I./N.I.F., Nº S.S./Mutualidad, Nombre y apellidos, Tarjeta sanitaria, Dirección postal,E-mail,Teléfono, Firma, Imagen
Otros datos tipificados:	Características personales ; Académicos y profesionales; Detalles del empleo ; Económicos, financieros y de seguros
Respuesta ejercicio de derechos de protección de datos	
Contacto ejercicio de derechos:	**info@ibizanurseservice.com**
Procedimiento Ejercicio de Derechos:	Apartado 7
Origen y procedencia de los datos:	
Origen de los datos:	El propio interesado o su representante legal
Categorías de interesados:	Empleados
Mecanismo de recogida de los datos:	Contrato
Cesión o comunicación de datos:	
Categorías de destinatarios:	Organismos de la Seguridad Social, Fundae , Administración Tributaria, Empresas de prevención de riesgos , Entidades bancarias, Entidades Aseguradoras , Administración Pública con competencia en la materia
Transferencia internacional de datos:	No TID
Seguridad	
Activos (servidores, equipos, aplicaciones…)	Apartado 5.2. de este Manual de Protección de Datos
Soportes no automatizados	Anexo IV de este Manual de Protección de Datos
Medidas técnicas y organizativas de seguridad	Apartado 6 de este Manual de Protección de Datos

Actividad de Tratamiento:	**SELECCIÓN DE PERSONAL**
Responsable de Tratamiento:	IBIZA NURSE SERVICE S.L
Delegado de Protección de Datos:	
Responsable Funcional:	Mª Victoria Cegarra Gutierrez
Finalidades:	Gestión de los Curriculum Vitae remitidos por los candidatos que desean participar en los procesos de selección de la entidad.
Base legítima del Tratamiento:	Contrato
Plazo de conservación de los datos:	1 año Ley: _____
Categorías de Datos:	
Otros tipos de datos:	Curriculum Vitae
Datos de carácter identificativo:	D.N.I./N.I.F. , Nombre y apellidos , Dirección postal,E-mail,Teléfono, Firma, Imagen
Otros datos tipificados:	Características personales
Respuesta ejercicio de derechos de protección de datos	
Contacto ejercicio de derechos:	**info@ibizanurseservice.com**
Procedimiento Ejercicio de Derechos:	Apartado 7
Origen y procedencia de los datos:	
Origen de los datos:	El propio interesado o su representante legal
Categorías de interesados:	Solicitantes de empleo
Mecanismo de recogida de los datos:	Curriculum vitae, PLATAFORMAS DE EMPLEO
Cesión o comunicación de datos:	
Categorías de destinatarios:	Otros destinatarios de cesiones:No se realizan comunicaciones de datos a terceros
Transferencia internacional de datos:	No TID
Seguridad	
Activos (servidores, equipos, aplicaciones…)	Apartado 5.2. de este Manual de Protección de Datos
Soportes no automatizados	Anexo IV de este Manual de Protección de Datos
Medidas técnicas y organizativas de seguridad	Apartado 6 de este Manual de Protección de Datos

ANEXO II. Relación de usuarios

La relación de usuarios con acceso al Sistema Operativo y a las aplicaciones que recogen datos personales se encuentra recogida en Directorio Activo y el correspondiente gestor de usuarios de las distintas aplicaciones. A continuación se detalla la relación de usuarios que tienen acceso a datos personales en **soporte**.

Nombre y apellidos	Puesto de trabajo	Fecha de alta en el sistema	Fecha de baja en el sistema	Actividad de tratamiento con permiso de acceso	Nivel de acceso (Acceso o Modificación)

ANEXO III. Listado de prestadores de servicios

- **Encargados del Tratamiento que prestan servicios a IBIZA NURSE SERVICE S.L (Responsable del Tratamiento) con acceso a datos personales.**

ENCARGADO DE TRATAMIENTO
Nombre o razón social: NIN DE CARDONA SL **Dirección**: Plaza Castellini nº3 4º Derecha; 30201 Cartagena (Murcia) **CIF**: B30808372 **Actividad del Encargado**: la prestación de servicios de asesoramiento asesoria contable, fiscal y laboral **Servicio prestado**: Gestión contable, fiscal, administrativa y laboral **Descripción del servicio prestado**: Gestión de impuestos, facturas, gestiones frente a la administración pública, elaboración de contratos, gestión de nóminas, seguros sociales y otros usos relacionados con temas laborales **Categorías de interesados**: Trabajadores, Candidatos, Clientes, Proveedores, Otros **Categorías de datos**: Datos identificativos, Datos de características personales, Datos de circunstancias sociales, Datos académicos y profesionales, Datos de detalles de empleo, Datos económicos, financieros y de seguros, Otros Fecha del contrato de prestación de servicios: Duración del contrato: Vigencia del contrato principal. Destino de los datos: Devolver al responsable del tratamiento

ENCARGADO DE TRATAMIENTO
Nombre o razón social: **Dirección**: **CIF**: **Actividad del Encargado** **Servicio prestado**: **Descripción del servicio prestado**: **Categorías de interesados**: **Categorías de datos**: Fecha del contrato de prestación de servicios: Duración del contrato: Vigencia del contrato principal. Destino de los datos: Devolver al responsable del tratamiento

- **Sociedades (Responsables del Tratamiento) a las que IBIZA NURSE SERVICE S.L, como Encargado del Tratamiento, presta un servicios con acceso a datos.**

RESPONSABLE DE TRATAMIENTO
Nombre o razón social: **Dirección:** **CIF:** **Actividad del Responsable:** **Servicio Prestado:** **Descripción del servicio prestado**: **Categorías de interesados:** **Categorías de datos:** Duración del contrato: Vigencia del contrato principal. Destino de los datos: Devolver al responsable del tratamiento E-mail de contacto:

- **Prestadores de servicios sin acceso a datos personales, pero con libre acceso a las instalaciones de IBIZA NURSE SERVICE S.L.**

PRESTADOR DEL SERVICIO
Nombre o razón social: **Dirección**: **CIF**: **Servicio Prestado**: Fecha del contrato de prestación de servicios: Duración del contrato: Vigencia del contrato principal.

ANEXO IV. Registro de incidencias

La Sociedad cuenta con la aplicación donde se refleja cada incidencia que se produce en los sistemas. En dicha aplicación se hacen constar todos los datos relativos a dichas incidencias.

A continuación se recogen las plantillas a utilizar en caso de producirse incidencias que afecten a datos personales en **soportes**.

REGISTRO DE INCIDENCIAS						
Nº Incidencia	**Fecha y hora incidencia**	**Descripción**	**Persona que notifica**	**Persona a quien se notifica**	**Efectos producidos**	**Medidas correctoras**

REGISTRO DE RECUPERACION DE DATOS						
Nº Incidencia	**Fecha y hora notificación**	**Persona que notifica**	**Procedimiento recuperación de datos**	**Persona que realiza la recuperación**	**Datos recuperados o grabados manualmente**	**Autorización Responsable Funcional**

ANEXO V. Inventario de soportes

La Sociedad custodia el inventario de soportes automatizado en **en el despacho del responsable de seguridad técnico.**

A continuación se recoge la plantilla para el inventario de **soportes**.

INVENTARIO DE SOPORTES							
Descripción	**Tipo de soportes**	**Etiqueta**	**Fecha de alta**	**Actividad de Tratamiento**	**Datos sensibles SÍ/NO**	**Ubicación**	**Fecha de baja**

ANEXO VI. Registro de entrada y salida de soportes

REGISTRO DE ENTRADA DE SOPORTES						
Fecha y hora de entrada	**Nº de soportes o documentos**	**Tipo de soporte o documento**	**Tipo de información que contiene**	**Emisor**	**Forma de envío**	**Persona responsable de la recepción**

REGISTRO DE SALIDA DE SOPORTES						
Fecha y hora de salida	**Nº de soportes o documentos**	**Tipo de soporte o documento**	**Tipo de información que contiene**	**Destinatario**	**Forma de envío**	**Persona responsable de la entrega**

ANEXO VII. Registro de acceso a datos sensibles

A continuación se incluye el Registro de Acceso 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.

REGISTRO DE ACCESO A DATOS SENSIBLES			
Identificación del usuario	**Actividad de tratamiento**	**Fecha y hora**	**Documentación a la que se tiene acceso**

ANEXO VIII. Registro de controles periódicos

Cada uno de los Responsables Funcionales, respecto a su Actividad de Tratamiento, y con el asesoramiento del Delegado de Protección de Datos (DPO), revisarán **periódicamente** el cumplimiento de los siguientes controles:

REGISTRO DE CONTROLES PERIÓDICOS – SOPORTES NO AUTOMATIZADOS			
Responsable de la revisión	**Control**	**Periodo**	**Medida correctora**
Responsables Funcionales	Revisar los posibles cambios producidos en los sistemas de información que afecten a soportes no automatizados	Anual	
Responsables Funcionales	Verificar que únicamente se están tratando los datos necesarios para cumplir la finalidad para la que fueron recogidos y que se han eliminado una vez han pasado los plazos de conservación	Anual	
Responsables Funcionales	Revisar si está actualizado el listado de prestadores de servicios con acceso a datos personales	Anual	
Responsables Funcionales	Comprobar la actualización de la relación de usuarios autorizados a acceder a datos almacenados en soportes no automatizados (locales, mobiliario...)	Anual	
Responsables Funcionales	Comprobar la actualización de la relación de usuarios autorizados a trabajar fuera de las instalaciones y con acceso a datos almacenados en soportes no automatizados	Anual	
Responsables Funcionales	Verificar que todos los usuarios han firmado el Recibo del Manual de Protección de Datos	Anual	
Responsables Funcionales	Verificar que el inventario de soportes no automatizados está actualizado	Anual	
Responsables Funcionales	Comprobar que los soportes no automatizados están etiquetados	Anual	
Responsables Funcionales	Revisar la correcta destrucción de soportes no automatizados	Anual	
Responsables Funcionales	Comprobar que los usuarios conocen sus funciones y obligaciones en cuanto a la seguridad de datos personales en soporte no automatizado	Semestral	
Responsables Funcionales	Analizar las incidencias registradas que afecten a soportes no automatizados	Semestral	
Responsables Funcionales	Comprobar que el soporte papel se almacena en mobiliario con mecanismos que obstaculicen su	Semestral	

REGISTRO DE CONTROLES PERIÓDICOS – SOPORTES NO AUTOMATIZADOS			
Responsable de la revisión	**Control**	**Periodo**	**Medida correctora**
	apertura		
Responsables Funcionales	Revisar si se producen entradas y salidas de soportes no automatizados con datos personales y, en caso afirmativo, si se lleva un Registro	Semestral	
Responsables Funcionales	Revisar que solo las personas autorizadas acceden a los locales con datos personales en soporte no automatizado	Semestral	
Responsables Funcionales	Verificar que los soportes no automatizados con datos sensibles se almacenan en áreas protegidas con puertas con sistemas de cierre	Semestral	
Responsables Funcionales	Comprobar que se han adoptado las medidas de seguridad necesarias para impedir el acceso o manipulación de los soportes no automatizados con datos sensibles durante su traslado fuera de las instalaciones de la Sociedad	Semestral	
Responsables Funcionales	Comprobar que se realizan correctamente los registros de acceso a datos sensibles en soporte no automatizado realizados por múltiples usuarios	Mensual	
Responsables Funcionales	Revisar que se realizan los Informes mensuales de los registros de acceso a datos sensibles en soporte no automatizado	Mensual	

El Responsable de Seguridad Técnico, con el asesoramiento del Delegado de Protección de Datos (DPO), revisará **periódicamente** el cumplimiento de los siguientes controles:

REGISTRO DE CONTROLES PERIÓDICOS – SOPORTES AUTOMATIZADOS			
Responsable de la revisión	**Control**	**Periodo**	**Medida correctora**
Responsable de Seguridad Técnico	Comprobar que las personas con acceso autorizado necesitan realmente acceder a los datos personales	Anual	
Responsable de Seguridad Técnico	Comprobar que las personas autorizadas están identificadas individualmente	Anual	
Responsable de Seguridad	Revisar que las contraseñas son individuales y se cambian	Anual	

REGISTRO DE CONTROLES PERIÓDICOS – SOPORTES AUTOMATIZADOS			
Responsable de la revisión	**Control**	**Periodo**	**Medida correctora**
Técnico	periódicamente (por lo menos una vez al año)		
Responsable de Seguridad Técnico	Verificar que se limita el intento reiterado de accesos	Anual	
Responsable de Seguridad Técnico	Verificar que existe un inventario de soportes automatizado y está actualizado	Anual	
Responsable de Seguridad Técnico	Comprobar que los soportes automatizados están etiquetados o identificados	Anual	
Responsable de Seguridad Técnico	Revisar la correcta destrucción de soportes automatizados con arreglo al procedimiento establecido	Anual	
Responsable de Seguridad Técnico	Verificar la existencia de copias de seguridad, por lo menos semanales	Semestral	
Responsable de Seguridad Técnico	Revisar que se realizan correctamente las recuperaciones de datos	Semestral	
Responsable de Seguridad Técnico	Comprobar que los usuarios conocen sus funciones y obligaciones en cuanto a la seguridad de datos de personales en soporte automatizado	Semestral	
Responsable de Seguridad Técnico	Analizar si las incidencias que afecten a datos personales han sido registradas (incluyendo las recuperaciones de datos) y se han tomado las medidas correctoras adecuadas	Semestral	
Responsable de Seguridad Técnico	Revisar si se registra las entradas y salidas de soportes automatizados (por ej. las copias de seguridad)	Anual	
Responsable de Seguridad Técnico	Revisar que solo las personas autorizadas tienen acceso a los soportes automatizados con datos personales	Anual	
Responsable de Seguridad Técnico	Revisar que solo las personas autorizadas tienen acceso a los CPDs (data center)	Anual	
Responsable de Seguridad Técnico	Comprobar si la distribución de soportes (cintas de seguridad, portátiles, smartphones…) de datos sensibles se realiza cifrándolos previamente	Semestral	
Responsable de Seguridad Técnico	Revisar que la transmisión de datos sensibles a través de redes de comunicaciones (internet, correos electrónicos…) se realiza cifrándolos previamente	Semestral	

REGISTRO DE CONTROLES PERIÓDICOS – SOPORTES AUTOMATIZADOS			
Responsable de la revisión	**Control**	**Periodo**	**Medida correctora**
Responsable de Seguridad Técnico	Verificar que las copias de respaldo y los procedimientos de recuperación están ubicadas en un lugar diferente de aquel en el que se encuentran los sistemas de información	Semestral	
Responsable de Seguridad Técnico	Comprobar que existen y se realizan correctamente los registros de acceso a datos sensibles en soporte automatizado	Mensual	
Responsable de Seguridad Técnico	Comprobar que los registros de acceso a datos sensibles en soporte automatizado son revisados mensualmente y se realizan los correspondientes informes mensuales	Mensual	

ANEXO IX. Delegación de autorizaciones

A continuación se recoge la plantilla de Delegación de autorizaciones, que hace referencia a las funciones que el Delegado de Protección de Datos (DPO), cada uno de los Responsables Funciones respecto a su Actividad de Tratamiento, el Responsable de Seguridad Técnica o el Gestor de Solicitudes de Ejercicio de Derechos delegan a diferentes usuarios.

DELEGACIÓN DE AUTORIZACIONES			
Responsable de la autorización	**Función delegada**	**Usuario/s autorizado/s**	**Fecha límite autorización**
Responsable de Seguridad Técnico	Conceder, alterar o anular el acceso autorizado a la Red y a las aplicaciones		
Responsables Funcionales	Conceder, alterar o anular el acceso autorizado a las propias instalaciones de la Sociedad		
Responsable de Seguridad Técnico	Conceder, alterar o anular el acceso autorizado a las instalaciones (CPDs, servidores, equipos…)		
Responsables Funcionales	Conceder, alterar o anular el acceso autorizado a las instalaciones (garita, locales, mobiliario...)		
Responsable de Seguridad Técnico	Llevanza y actualización del Registro de Incidencias (soporte automatizado)		
Responsables Funcionales	Llevanza y actualización del Registro de Incidencias (soporte no automatizado)		
Responsables Funcionales	Autorizar la salida de soportes con datos personales (tanto físicos como documentos adjuntos a un e-mail)		
Responsables Funcionales	Persona responsable de la recepción o entrega de soportes		
Responsable de Seguridad Técnico	Realización de las copias de seguridad		
Responsable de Seguridad Técnico	Ejecución de procedimientos de recuperación de datos		
Responsables Funcionales	Autorizar el trabajo con datos personales fuera de las instalaciones		
Delegado de Protección de	Realizar las modificaciones necesarias en el presente Manual de Protección de Datos		

DELEGACIÓN DE AUTORIZACIONES			
Responsable de la autorización	**Función delegada**	**Usuario/s autorizado/s**	**Fecha límite autorización**
Datos (DPO)			
Responsable de Seguridad Técnico	Ejecutar los controles periódicos de verificación establecidos en el Manual de Protección de Datos que afecten a soportes automatizados		
Responsables Funcionales	Ejecutar los controles periódicos de verificación establecidos en el Manual de Protección de Datos que afecten a soportes no automatizados		
Responsables Funcionales	Mantener actualizado el Registro de Actividades de Tratamiento		
Gestor de Solicitudes de Ejercicio de Derechos	Contestar en plazo y forma las solicitudes de ejercicios de derechos de protección de datos.		
Delegado de Protección de Datos (DPO)	Redactar las cláusulas informativas correspondientes para permitir hacer efectivos los derechos de los individuos.		
Delegado de Protección de Datos (DPO)	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.		
Responsables Funcionales	Colaborar con el Delegado de Protección de Datos (DPO) en la divulgación de las funciones del personal y en la difusión de la normativa al respecto.		
Responsables Funcionales	Utilizar cláusulas para solicitar el consentimiento y/o informar a los interesados del tratamiento de sus datos, de sus derechos en protección de datos y demás exigencias de la normativa de protección de datos.		
Responsables Funcionales	Consultar y solicitar la autorización del Delegado de Protección de Datos (DPO) antes de ceder cualquier dato a un tercero.		
Responsables Funcionales	Consultar con el Delegado de Protección de Datos (DPO) el clausulado necesario a incluir en los contratos con encargados del tratamiento.		
Responsable de Seguridad Técnico	Autorizar la recuperación de datos en el caso de incidencias de seguridad que lo requieran		
Responsables Funcionales	Establecer los criterios de archivo y custodia de los soportes o documentos relativos a soportes no automatizados; estos criterios deben garantizar la correcta conservación de los mismos, su localización y consulta, así como posibilitar el ejercicio de derechos.		
Responsables Funcionales	Adoptar las medidas necesarias para que, en el caso de soportes no automatizados, si no existen medidas		

DELEGACIÓN DE AUTORIZACIONES			
Responsable de la autorización	**Función delegada**	**Usuario/s autorizado/s**	**Fecha límite autorización**
	que obstaculicen la apertura de armarios o dispositivos de almacenamiento, se impida el acceso a personas no autorizadas		
Responsables Funcionales	Colaborar con el Delegado de Protección de Datos (DPO) en la divulgación al personal de las normas de seguridad que afecten al desarrollo de sus funciones y las consecuencias de su incumplimiento		

ANEXO X. Recibo del Manual de Protección de Datos por los empleados o usuarios

El presente modelo de recibo del Manual de Protección de Datos debe ser firmado por cada trabajador/usuario de la Sociedad que acceda a datos personales, como prueba de la recepción por el mismo del presente Manual de Protección de Datos.

RECIBO DEL MANUAL DE PROTECCIÓN DE DATOS		
*Como usuario autorizado para acceder a datos personales, cuyo Responsable del Tratamiento es **IBIZA NURSE SERVICE S.L,** manifiesto que tengo pleno conocimiento del Manual de Protección de Datos, y de las funciones y obligaciones que, en materia de protección de datos, me conciernen como usuario, entre las que se encuentra el **deber de secreto profesional** respecto a los datos personales a los que tenga acceso, incluso una vez finalizadas mis relaciones con **IBIZA NURSE SERVICE S.L.***		
USUARIO (Nombre y Apellidos)	**NIF**	**FECHA Y FIRMA**

ANEXO XI. Modelos de ejercicio de derechos por el interesado

COMUNICACIÓN DEL EJERCICIO DE DERECHOS DE ACCESO, RECTIFICACIÓN, SUPRESIÓN, LIMITACIÓN DEL TRATAMIENTO, PORTABILIDAD Y OPOSICIÓN						
Fecha de solicitud	**Nombre y apellidos del solicitante**	**DNI**	**Derecho ejercitado**	**Observaciones**	**Nombre y apellidos del receptor**	**Fecha de respuesta**

EJERCICIO DEL DERECHO DE ACCESO

D./Dª....., (en adelante el interesado) con D.N.I....., del que se acompaña fotocopia, manifiesta su deseo de ejercer su derecho de acceso a los datos personales objeto de tratamiento por parte del responsable del tratamiento **IBIZA NURSE SERVICE S.L**, con domicilio fiscal en C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares).
En caso de ejercer los derechos en nombre de un tercero debido a la minoría de edad del interesado o bien por discapacidad declarada (sobre la que debe adjuntar copia), indicar el nombre del tercero interesado menor de edad o discapacitado y DNI: _____.

El interesado solicita las siguientes acciones por parte de **IBIZA NURSE SERVICE S.L**:

- Que se le facilite gratuitamente el acceso a sus datos, sin dilación indebida y a más tardar en el plazo de un mes a contar desde la recepción del presente escrito.

- Que si la solicitud del derecho de acceso fuese estimada, se ponga en conocimiento del interesado los datos que son objeto de tratamiento por parte del responsable del tratamiento de algún modo en el que quede probada su recepción efectiva por parte del interesado o su representante legal.

- Que esta información comprenda de modo conciso, transparente, inteligible y de fácil acceso, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos, los datos que sobre mi persona están siendo tratados por el responsable del tratamiento, y los resultantes de cualquier elaboración, proceso o tratamiento (incluida la elaboración de perfiles), así como el origen de los datos, el plazo de conservación de los mismos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

Domicilio del solicitante a efectos de recibir notificaciones respecto al presente ejercicio de derechos:

En ....., a.....de.....de 20…

Firma del Solicitante: _____

EJERCICIO DEL DERECHO DE RECTIFICACION

D./Dª....., (en adelante el interesado) con D.N.I....., del que se acompaña fotocopia, manifiesta su deseo de ejercer su derecho de rectificación de los datos personales objeto de tratamiento por parte del responsable del tratamiento **IBIZA NURSE SERVICE S.L**, con domicilio fiscal en C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares).

En caso de ejercer los derechos en nombre de un tercero debido a la minoría de edad del interesado o bien por discapacidad declarada (sobre la que debe adjuntar copia), indicar el nombre del tercero interesado menor de edad o discapacitado y DNI: _____.

El interesado solicita las siguientes acciones por parte del responsable del tratamiento:

- Que se proceda gratuitamente a la efectiva corrección, sin dilación indebida y a más tardar en el plazo de un mes desde la recepción de esta solicitud, de los siguientes datos:

Dato Incorrecto	Dato Correcto

- Que si la solicitud del derecho de rectificación fuese estimada, se ponga en conocimiento del interesado los datos que han sido corregidos de algún modo en el que quede probada su recepción efectiva por parte del interesado o su representante legal.

- Que, en el caso de que el responsable del tratamiento considere que la rectificación no procede, me sea comunicada dicha resolución igualmente, de forma motivada y dentro del plazo de un mes indicado.

Domicilio del solicitante a efectos de recibir notificaciones respecto al presente ejercicio de derechos:

En ....., a.....de.....de 20…

Firma del Solicitante: _____

EJERCICIO DEL DERECHO DE SUPRESIÓN

D./Dª....., (en adelante el interesado) con D.N.I....., del que se acompaña fotocopia, manifiesta su deseo de ejercer su derecho de cancelación de todos o parte de los datos personales objeto de tratamiento por parte del responsable del tratamiento **IBIZA NURSE SERVICE S.L**, con domicilio fiscal en C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares).

En caso de ejercer los derechos en nombre de un tercero debido a la minoría de edad del interesado o bien por discapacidad declarada (sobre la que debe adjuntar copia), indicar el nombre del tercero interesado menor de edad o discapacitado y DNI: _____.

El interesado solicita las siguientes acciones por parte del responsable del tratamiento:

- Que se proceda gratuitamente a la efectiva supresión, sin dilación indebida y a más tardar en el plazo de un mes desde la recepción de esta solicitud, de los siguientes datos: *(Marcar con una X lo que proceda)*
  - ☐ Supresión total de todos los datos.
  - ☐ Supresión exclusivamente de los siguientes datos:

Datos a suprimir

- Que si ha hecho públicos mis datos personales, informe a los responsables que estén tratándolos de la presente solicitud, así como de la supresión de cualquier enlace a dichos datos (**derecho al olvido**) o de cualquier copia o réplica de los mismos.
- Que si la solicitud del derecho de supresión fuese estimada, se proceda, si ha lugar, al bloqueo de los datos solicitados y me sea comunicado de algún modo en el que quede probada su recepción por mi parte o por mi representante legal, y que, pasado el plazo de prescripción de las posibles responsabilidades o acciones consecuencia del tratamiento de datos, se proceda a su efectiva supresión.
- Que, en el caso de que el responsable del tratamiento considere que la supresión no procede, me sea comunicada dicha resolución igualmente, de forma motivada y dentro del plazo de un mes indicado.

Domicilio del solicitante a efectos de recibir notificaciones respecto al presente ejercicio de derechos:

En .....,
Firma del Solicitante: _____

EJERCICIO DEL DERECHO DE LIMITACIÓN DEL TRATAMIENTO

D./Dª....., (en adelante el interesado) con D.N.I....., del que se acompaña fotocopia, manifiesta su deseo de ejercer su derecho de limitación del tratamiento de todos o parte de los datos personales objeto de tratamiento por parte del responsable del tratamiento **IBIZA NURSE SERVICE S.L**, con domicilio fiscal en C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares).

En caso de ejercer los derechos en nombre de un tercero debido a la minoría de edad del interesado o bien por discapacidad declarada (sobre la que debe adjuntar copia), indicar el nombre del tercero interesado menor de edad o discapacitado y DNI: _____.

El interesado solicita las siguientes acciones por parte del responsable del tratamiento:

- Que se proceda gratuitamente a la efectiva limitación de tratamiento, sin dilación indebida y a más tardar en el plazo de un mes desde la recepción de esta solicitud, de los siguientes datos: *(Marcar con una X lo que proceda)*

  ☐ Limitar el tratamiento de todos los datos sobre mi persona.
  ☐ Limitar el tratamiento exclusivamente de los siguientes datos:

Datos sobre los que recae el ejercicio	Justificación

En caso de que la Justificación esté acreditada por algún medio documental, se requiere que el interesado la adjunte a la presente solicitud.

- Que si la solicitud del derecho de limitación del tratamiento fuese estimada, dicha resolución se ponga en conocimiento del interesado de algún modo en el que quede probada su recepción efectiva por parte del interesado o su representante legal.
- Que, en el caso de que el responsable del tratamiento considere que la limitación del tratamiento no procede, me sea comunicada dicha resolución igualmente, de forma motivada y dentro del plazo de 1 mes indicado.

Domicilio del solicitante a efectos de recibir notificaciones respecto al presente ejercicio de derechos:

En ....., a.....de.....de 20…
Firma del Solicitante: _____

EJERCICIO DEL DERECHO A LA PORTABILIDAD DE LOS DATOS

D./Dª....., (en adelante el interesado) con D.N.I....., del que se acompaña fotocopia, manifiesta su deseo de ejercer su derecho a la portabilidad de todos o parte de los datos personales objeto de tratamiento por parte del responsable del tratamiento **IBIZA NURSE SERVICE S.L**, con domicilio fiscal en C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares).

En caso de ejercer los derechos en nombre de un tercero debido a la minoría de edad del interesado o bien por discapacidad declarada (sobre la que debe adjuntar copia), indicar el nombre del tercero interesado menor de edad o discapacitado y DNI: _____.
El interesado solicita al responsable del tratamiento que proceda gratuitamente, sin dilación indebida y a más tardar en el plazo de un mes desde la recepción de esta solicitud, a las siguientes acciones *(Marcar con una X lo que proceda)*:

- ☐ Recibir los datos personales que le haya facilitado previamente, así como los derivados directamente del uso del servicio prestado, en un formato estructurado, de uso común y lectura mecánica.
- ☐ Transmitir directamente dichos datos a otro responsable del tratamiento.
- ☐ Recibir o transmitir a otro responsable del tratamiento exclusivamente los siguientes datos *(Marcar con una X lo que proceda)*:

Datos sobre los que recae el ejercicio	Recibir	Transmitir

- Si la solicitud del derecho a la portabilidad de los datos fuese estimada, dicha resolución se ponga en conocimiento del interesado de algún modo en el que quede probada su recepción efectiva por parte del interesado o su representante legal.
- En el caso de que el responsable del tratamiento considere que la portabilidad de los datos no procede, me sea comunicada dicha resolución igualmente, de forma motivada y dentro del plazo de 1 mes indicado.

Domicilio del solicitante a efectos de recibir notificaciones respecto al presente ejercicio de derechos:

En ....., a.....de.....de 20…

Firma del Solicitante: _____

EJERCICIO DEL DERECHO DE OPOSICION

D./Dª....., (en adelante el interesado) con D.N.I....., del que se acompaña fotocopia, manifiesta su deseo de ejercer su derecho de oposición de todos o parte de los datos personales objeto de tratamiento por parte del responsable del tratamiento **IBIZA NURSE SERVICE S.L**, con domicilio fiscal en C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares).

En caso de ejercer los derechos en nombre de un tercero debido a la minoría de edad del interesado o bien por discapacidad declarada (sobre la que debe adjuntar copia), indicar el nombre del tercero interesado menor de edad o discapacitado y DNI: _____.
El interesado solicita las siguientes acciones por parte del responsable del tratamiento:
Que se proceda gratuitamente a la efectiva exclusión del tratamiento sin dilación indebida y a más tardar en el plazo de un mes desde la recepción de esta solicitud, de los siguientes datos: *(Marcar con una X lo que proceda)*

☐ Oposición al tratamiento de todos los datos sobre mi persona.
☐ Oposición exclusivamente de los siguientes datos:

Datos sobre los que recae el ejercicio	Justificación

En caso de que la Justificación esté acreditada por algún medio documental, se requiere que el interesado la adjunte a la presente solicitud.

- Que si la solicitud del derecho de oposición fuese estimada, dicha resolución se ponga en conocimiento del interesado de algún modo en el que quede probada su recepción efectiva por parte del interesado o su representante legal.
- Que, en el caso de que el responsable del tratamiento considere que la oposición no procede, me sea comunicada dicha resolución igualmente, de forma motivada y dentro del plazo de un mes indicado.

Domicilio del solicitante a efectos de recibir notificaciones respecto al presente ejercicio de derechos:

En ....., a.....de.....de 20…
Firma del Solicitante: _____

ANEXO XII. Modelos de contestación o denegación al ejercicio de derechos por el interesado

CARTA CONTESTACIÓN ANTE EL EJERCICIO DEL DERECHO DE ACCESO

Con fecha.....,

D./Dª....., (en adelante el interesado) con D.N.I....., solicitó el acceso a los datos personales de los que es titular y que se encuentran en nuestro sistema de información.

ó

D./Dª....., con D.N.I....., en nombre y representación de D./Dª....., solicitó el acceso de los datos personales que se encuentran en nuestro sistema de información.

IBIZA NURSE SERVICE S.L, como Responsable del Tratamiento, en cumplimiento de lo dispuesto en el artículo 13 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales relativo a la Protección de las Personas físicas, 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, **accede a lo solicitado**, comprometiéndose a enviar la documentación que a continuación se relaciona **en el plazo máximo de un mes a contar desde la fecha de recepción de la solicitud del ejercicio del derecho de acceso**:

- Fines del tratamiento
- Categorías de datos personales
- Destinatarios (incluyendo transferencias internacionales de datos)
- Plazo previsto de conservación de los datos
- Origen de los datos (si éstos no han sido obtenidos del propio interesado)
- La existencia o no de decisiones automatizadas, incluida la elaboración de perfiles

Ud. puede ejercer otros derechos en protección de datos, como la rectificación, la supresión, la limitación del tratamiento, la portabilidad o la oposición a dicho tratamiento de sus datos. En cualquier situación, Ud. tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD).

Esta información se facilitará en forma legible mediante escrito, copia o fotocopia remitida por correo, o por cualquier otro procedimiento adecuado en función de la configuración de los datos.

En Ibiza a .....de.....de 20..

IBIZA NURSE SERVICE S.L

CARTA DENEGACIÓN ANTE EL EJERCICIO DEL DERECHO DE ACCESO

Con fecha.....,

D./Dª....., (en adelante el interesado) con D.N.I....., solicitó el acceso a los datos personales de los que es titular y que se encuentran en nuestro sistema de información.

ó

D./Dª....., con D.N.I....., en nombre y representación de D./Dª....., solicitó el acceso de los datos personales que se encuentran en nuestro sistema de información.

IBIZA NURSE SERVICE S.L, como Responsable del Tratamiento, en cumplimiento de lo dispuesto en el artículo 13 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales relativo a la Protección de las Personas físicas y en los artículos 12 y 15 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, **no accede a lo solicitado,** debido a:

☐ La existencia de obligaciones legales que impiden la revelación de los datos por parte del Responsable del Tratamiento.
☐ El derecho de acceso ha sido ejercitado en los últimos **seis meses** en relación con los mismos datos, no habiendo acreditado el interesado una causa legítima para poder volver a ejercitarlo.
☐ No existencia de datos personales del interesado en los sistemas de información del profesional.
☐ Otros motivos (indicar).....

Ud. puede ejercer otros derechos en protección de datos, como la rectificación, la supresión, la limitación del tratamiento, la portabilidad o la oposición a dicho tratamiento de sus datos.

En cualquier situación, Ud. tiene derecho a presentar una reclamación o a recabar la tutela de la Agencia Española de Protección de Datos, o de las Entidades competentes en su caso, en los términos establecidos en la normativa vigente en materia de protección de datos, y conforme a disposiciones reglamentarias reflejadas en el 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.

En Ibiza a .....de.....de 20..

IBIZA NURSE SERVICE S.L

CARTA CONTESTACIÓN ANTE EL EJERCICIO DEL DERECHO DE RECTIFICACIÓN

Con fecha .....,

D./Dª....., con DNI....., solicitó la rectificación de los siguientes datos personales obrantes en nuestro sistema de información:

- _____
- _____

ó

D./Dª....., con D.N.I....., en nombre y representación de D./Dª....., solicitó la rectificación de los siguientes datos personales obrantes en nuestro sistema de información:

- _____
- _____

IBIZA NURSE SERVICE S.L, como Responsable del Tratamiento, en cumplimiento de lo dispuesto en el artículo 14 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales relativo a la Protección de las Personas físicas y los artículos 12 y 16 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, **accede a lo solicitado**, procediendo a la rectificación de dichos datos, obrantes en su sistema de información, **en el plazo máximo de un mes a contar desde la fecha de recepción de la solicitud del ejercicio del derecho de rectificación**, quedando rectificados en nuestro sistema de información, tal y como a continuación se detalla:

- _____
- _____

No obstante, **IBIZA NURSE SERVICE S.L** está obligado a bloquear los datos rectificados, conservándolos únicamente a disposición de Tribunales, del Ministerio Fiscal u otras Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles derivadas del tratamiento y por el plazo de prescripción de las mismas. Los datos bloqueados no serán tratados para ninguna otra finalidad distinta de la indicada en este párrafo.

Ud. puede ejercer otros derechos en protección de datos, como el acceso, la supresión, la limitación del tratamiento, la portabilidad o la oposición a dicho tratamiento de sus datos. En cualquier situación, Ud. tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD).

En Ibiza a .....de.....de 20..

IBIZA NURSE SERVICE S.L

CARTA DENEGACIÓN ANTE EL EJERCICIO DEL DERECHO DE RECTIFICACIÓN

Con fecha .....,

D./Dª....., con DNI....., solicitó la rectificación de los siguientes datos personales obrantes en nuestro sistema de información:

- _____
- _____

ó

D./Dª....., con D.N.I....., en nombre y representación de D./Dª....., solicitó la rectificación de los siguientes datos personales obrantes en nuestro sistema de información:

- _____
- _____

IBIZA NURSE SERVICE S.L, como Responsable del Tratamiento, y en cumplimiento del artículo 14 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales relativo a la Protección de las Personas físicas y de lo dispuesto en los artículos 12 y 16 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, **no accede a lo solicitado**, debido a:

☐ Por causar un perjuicio a intereses legítimos del interesado o de terceros
☐ Existencia de un obligación legal de conservación de dichos datos.
☐ No existencia de datos personales del interesado en los sistemas de información del profesional.
☐ El derecho de rectificación ha sido ejercitado en los últimos **seis meses** en relación con los mismos datos, no habiendo acreditado el interesado una causa legítima para poder volver a ejercitarlo.
☐ Otros motivos (indicar).....

Ud. puede ejercer otros derechos en protección de datos, como el acceso, la supresión, la limitación del tratamiento, la portabilidad o la oposición a dicho tratamiento de sus datos.

En cualquier situación, Ud. tiene derecho a presentar una reclamación o a recabar la tutela de la Agencia Española de Protección de Datos, o de las Entidades competentes en su caso, en los términos establecidos en la normativa vigente en materia de protección de datos, y conforme a disposiciones reglamentarias reflejadas en el 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.

En Ibiza a .....de.....de 20..

IBIZA NURSE SERVICE S.L

CARTA CONTESTACIÓN ANTE EL EJERCICIO DEL DERECHO DE SUPRESIÓN

Con fecha .....,

D./Dª....., con DNI....., solicitó la supresión de los siguientes datos personales obrantes en nuestro sistema de información:

- _____
- _____

ó

D./Dª....., con D.N.I....., en nombre y representación de D./Dª....., solicitó la supresión de los siguientes datos personales obrantes en nuestro sistema de información:

- _____
- _____

IBIZA NURSE SERVICE S.L, como Responsable del Tratamiento, en cumplimiento de lo dispuesto en el artículo 15 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales relativo a la Protección de las Personas físicas y en los artículos 12 y 17 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, **accede a lo solicitado**, procediendo a la supresión de dichos datos, obrantes en su sistema de información, **en el plazo máximo de un mes a contar desde la fecha de recepción de la solicitud del ejercicio del derecho de supresión**.

No obstante, **IBIZA NURSE SERVICE S.L** está obligado a bloquear los datos, conservándolos únicamente a disposición de Tribunales, del Ministerio Fiscal u otras Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles derivadas del tratamiento y por el plazo de prescripción de las mismas. Los datos bloqueados no serán tratados para ninguna otra finalidad distinta de la indicada en este párrafo. Una vez transcurrido dicho plazo, se procederá a su supresión.

Ud. puede ejercer otros derechos en protección de datos, como el acceso, la rectificación, la limitación del tratamiento, la portabilidad o la oposición a dicho tratamiento de sus datos. En cualquier situación, Ud. tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD).

En Ibiza a .....de.....de 20

IBIZA NURSE SERVICE S.L

CARTA DENEGACIÓN ANTE EL EJERCICIO DEL DERECHO DE SUPRESIÓN

Con fecha .....,
D./Dª....., con DNI....., solicitó la supresión de los siguientes datos personales obrantes en nuestro sistema de información:

- _____
- _____

ó
D./Dª....., con D.N.I....., en nombre y representación de D./Dª....., solicitó la supresión de los siguientes datos personales obrantes en nuestro sistema de información:

- _____
- _____

IBIZA NURSE SERVICE S.L, como Responsable del Tratamiento, y en cumplimiento de lo dispuesto en el artículo 15 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales relativo a la Protección de las Personas físicas y los artículos 12 y 17 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, **no accede a lo solicitado**, debido a:

☐ El tratamiento es necesario para ejercer el derecho a la libertad de expresión e información.
☐ La existencia de obligaciones legales que impiden la supresión de los datos por parte del Responsable del Tratamiento.
☐ El tratamiento es necesario por razones de interés público en el ámbito de la salud pública.
☐ El tratamiento tiene fines de archivo en interés público, de investigación científica o histórica, o estadísticos.
☐ El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones.
☐ El derecho de supresión ha sido ejercitado en los últimos **seis meses** en relación con los mismos datos, no habiendo acreditado el interesado una causa legítima para poder volver a ejercitarlo.
☐ Por causar un perjuicio a intereses legítimos del interesado o de terceros
☐ No existencia de datos personales del interesado en los sistemas de información del profesional.
☐ Otros motivos (indicar).....

Ud. puede ejercer otros derechos en protección de datos, como el acceso, la rectificación, la limitación del tratamiento, la portabilidad o la oposición a dicho tratamiento de sus datos.
En cualquier situación, Ud. tiene derecho a presentar una reclamación o a recabar la tutela de la Agencia Española de Protección de Datos, o de las Entidades competentes en su caso, en los términos establecidos en la normativa vigente en materia de protección de datos, y conforme a disposiciones reglamentarias reflejadas en el 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.
En Ibiza a .....de.....de 20..
IBIZA NURSE SERVICE S.L

CARTA CONTESTACIÓN ANTE EL EJERCICIO DEL DERECHO DE LIMITACIÓN DEL TRATAMIENTO

Con fecha ……,

D./Dª....., con DNI....., solicitó la limitación del tratamiento de los siguientes datos personales obrantes en nuestro sistema de información:

- _____
- _____
- _____
- _____

ó

D./Dª....., con D.N.I....., en nombre y representación de D./Dª....., solicitó la limitación del tratamiento de los siguientes datos personales obrantes en nuestro sistema de información:

- _____
- _____
- _____
- _____

IBIZA NURSE SERVICE S.L, como Responsable del Tratamiento, en cumplimiento de lo dispuesto en el artículo 16 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales relativo a la Protección de las Personas físicas y los artículos 12 y 18 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, **accede a lo solicitado**, procediendo a la limitación del tratamiento de dichos datos, obrantes en su sistema de información, **en el plazo máximo de un mes a contar desde la fecha de recepción de la solicitud del ejercicio del derecho de oposición.**

Ud. puede ejercer otros derechos en protección de datos, como el acceso, la rectificación, la supresión, la portabilidad o la oposición a dicho tratamiento de sus datos. En cualquier situación, Ud. tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD).

En Ibiza a .....de.....de 20

IBIZA NURSE SERVICE S.L

CARTA DENEGACIÓN ANTE EL EJERCICIO DEL DERECHO DE LIMITACIÓN DEL TRATAMIENTO

Con fecha .....,
D./Dª....., con DNI....., solicitó la limitación del tratamiento de los siguientes datos personales obrantes en nuestro sistema de información:

- _____
- _____

ó
D./Dª....., con D.N.I....., en nombre y representación de D./Dª....., solicitó la limitación del tratamiento de los siguientes datos personales obrantes en nuestro sistema de información:

- _____
- _____

IBIZA NURSE SERVICE S.L, como Responsable del Tratamiento, y en cumplimiento de lo dispuesto en el artículo 16 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales relativo a la Protección de las Personas físicas y en los artículos 12 y 18 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, **no accede a lo solicitado**, debido a:

☐ El Responsable del Tratamiento ha verificado la licitud del tratamiento.
☐ El Responsable del Tratamiento ha verificado la necesidad del tratamiento.
☐ El interesado no necesita la limitación del tratamiento de sus datos para la formulación, el ejercicio o la defensa de reclamaciones.
☐ El Responsable del Tratamiento ha verificado que sus propios intereses legítimos prevalecen sobre los del interesado.
☐ El derecho de acceso ha sido ejercitado en los últimos **seis meses** en relación con los mismos datos, no habiendo acreditado el interesado una causa legítima para poder volver a ejercitarlo.
☐ No existencia de datos personales del interesado en los sistemas de información del profesional.
☐ Otros motivos……

Ud. puede ejercer otros derechos en protección de datos, como el acceso, la rectificación, la supresión, la portabilidad o la oposición a dicho tratamiento de sus datos.
En cualquier situación, Ud. tiene derecho a presentar una reclamación o a recabar la tutela de la Agencia Española de Protección de Datos, o de las Entidades competentes en su caso, en los términos establecidos en la normativa vigente en materia de protección de datos, y conforme a disposiciones reglamentarias reflejadas en el 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.

En Ibiza a .....de.....de 20

IBIZA NURSE SERVICE S.L

CARTA CONTESTACIÓN ANTE EL EJERCICIO DEL DERECHO A LA PORTABILIDAD DE LOS DATOS

Con fecha.....,

D./Dª....., (en adelante el interesado) con D.N.I....., solicitó la portabilidad de todos o parte de los datos personales de los que es titular y que se encuentran en nuestro sistema de información.

ó

D./Dª....., con D.N.I....., en nombre y representación de D./Dª....., solicitó la portabilidad de todos o parte de los datos personales que se encuentran en nuestro sistema de información.

IBIZA NURSE SERVICE S.L, como Responsable del Tratamiento, en cumplimiento de lo dispuesto en el artículo 17 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales relativo a la Protección de las Personas físicas y en los artículos 12 y 20 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, **accede a lo solicitado**, comprometiéndose a transmitir dichos datos **en el plazo máximo de un mes a contar desde la fecha de recepción de la solicitud del ejercicio del derecho de portabilidad** (Marcar con una X lo que proceda):

☐ Enviar al interesado los datos personales que le haya facilitado previamente, así como los derivados directamente del uso del servicio prestado, en un formato estructurado, de uso común y lectura mecánica.
☐ Transmitir directamente los datos objeto de la solicitud a otro responsable del tratamiento.

Ud. puede ejercer otros derechos en protección de datos, como la rectificación, la supresión, la limitación del tratamiento o la oposición a dicho tratamiento de sus datos. En cualquier situación, Ud. tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD).

En Ibiza a .....de.....de 20..

IBIZA NURSE SERVICE S.L

CARTA DENEGACIÓN ANTE EL EJERCICIO DEL DERECHO A LA PORTABILIDAD DE LOS DATOS

Con fecha.....,

D./Dª....., (en adelante el interesado) con D.N.I....., solicitó la portabilidad de todos o parte de los datos personales de los que es titular y que se encuentran en nuestro sistema de información.

ó

D./Dª....., con D.N.I....., en nombre y representación de D./Dª....., solicitó la portabilidad de todos o parte de los datos personales que se encuentran en nuestro sistema de información.

IBIZA NURSE SERVICE S.L, como Responsable del Tratamiento, en cumplimiento de lo dispuesto en el artículo 17 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales relativo a la Protección de las Personas físicas y en los artículos 12 y 20 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, **no accede a lo solicitado**, debido a:

☐ Por afectar negativamente a los derechos y libertades de terceros.
☐ El tratamiento no está basado en el consentimiento del interesado o en un contrato.
☐ El tratamiento no se efectúa por medios automatizados.
☐ El derecho de portabilidad ha sido ejercitado en los últimos **seis meses** en relación con los mismos datos, no habiendo acreditado el interesado una causa legítima para poder volver a ejercitarlo.
☐ No existencia de datos personales del interesado en los sistemas de información del profesional.
☐ Otros motivos (indicar).....

Ud. puede ejercer otros derechos en protección de datos, como la rectificación, la supresión, la limitación del tratamiento o la oposición a dicho tratamiento de sus datos.

En cualquier situación, Ud. tiene derecho a presentar una reclamación o a recabar la tutela de la Agencia Española de Protección de Datos, o de las Entidades competentes en su caso, en los términos establecidos en la normativa vigente en materia de protección de datos, y conforme a disposiciones reglamentarias reflejadas en el 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.

En Ibiza a .....de.....de 20..

IBIZA NURSE SERVICE S.L

CARTA CONTESTACIÓN ANTE EL EJERCICIO DEL DERECHO DE OPOSICIÓN

Con fecha ……,

D./Dª....., con DNI....., solicitó la oposición al tratamiento de los siguientes datos personales obrantes en nuestro sistema de información:

- _____
- _____
- _____
- _____

ó

D./Dª....., con D.N.I....., en nombre y representación de D./Dª....., solicitó la oposición al tratamiento de los siguientes datos personales obrantes en nuestro sistema de información:

- _____
- _____
- _____
- _____

IBIZA NURSE SERVICE S.L, como Responsable del Tratamiento, en cumplimiento de lo dispuesto en el artículo 18 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales relativo a la Protección de las Personas físicas y los artículos 12 y 21 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, **accede a lo solicitado**, procediendo a la interrupción del tratamiento de dichos datos, obrantes en su sistema de información, **en el plazo máximo de un mes a contar desde la fecha de recepción de la solicitud del ejercicio del derecho de oposición.**

Ud. puede ejercer otros derechos en protección de datos, como el acceso, la rectificación, la supresión, la limitación del tratamiento, o la portabilidad de sus datos. En cualquier situación, Ud. tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD).

En Ibiza a .....de.....de 20

IBIZA NURSE SERVICE S.L

CARTA DENEGACIÓN ANTE EL EJERCICIO DEL DERECHO DE OPOSICIÓN

Con fecha .....,

D./Dª....., con DNI....., solicitó la oposición al tratamiento de los siguientes datos personales obrantes en nuestro sistema de información:

- _____
- _____

ó

D./Dª....., con D.N.I....., en nombre y representación de D./Dª....., solicitó la oposición al tratamiento de los siguientes datos personales obrantes en nuestro sistema de información:

- _____
- _____

IBIZA NURSE SERVICE S.L, como Responsable del Tratamiento, y en cumplimiento de lo dispuesto en el artículo 18 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales relativo a la Protección de las Personas físicas y en los artículos 12 y 21 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, **no accede a lo solicitado**, debido a:

☐ Acreditación de motivos legítimos imperiosos para el tratamiento, por parte del Responsable del Tratamiento.
☐ El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones.
☐ El derecho de acceso ha sido ejercitado en los últimos **seis meses** en relación con los mismos datos, no habiendo acreditado el interesado una causa legítima para poder volver a ejercitarlo.
☐ No existencia de datos personales del interesado en los sistemas de información del profesional.
☐ Otros motivos……

Ud. puede ejercer otros derechos en protección de datos, como el acceso, la rectificación, la supresión, la limitación del tratamiento, o la portabilidad de sus datos.
En cualquier situación, Ud. tiene derecho a presentar una reclamación o a recabar la tutela de la Agencia Española de Protección de Datos, o de las Entidades competentes en su caso, en los términos establecidos en la normativa vigente en materia de protección de datos, y conforme a disposiciones reglamentarias reflejadas en el 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.

En Ibiza a .....de.....de 20

IBIZA NURSE SERVICE S.L

ANEXO XIII. Nombramientos: DPO y Responsables

NOMBRAMIENTO DEL DPO

El presente nombramiento debe ser firmado por el Delegado de Protección de Datos (DPO).

Nombramiento:

IBIZA NURSE SERVICE S.L, como Responsable del Tratamiento, designa a **…….** como Delegado de Protección de Datos (DPO) para todos los tratamientos de datos realizados por la Sociedad.

Como DPO,se encargará de llevar a cabo las "**Funciones y obligaciones del Delegado de Protección de Datos**" enumeradas en el apartado 4.4 del Manual de Protección de Datos, así como todas aquellas obligaciones que la normativa estatal y europea vigente en protección de datos y, especialmente, el Reglamento Europeo de Protección de Datos (RGPD), impone a los DPO.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde a los Responsables y a los Encargados de Tratamiento.

Fecha

Firma

NOMBRAMIENTO DE RESPONSABLES FUNCIONALES

→ El presente nombramiento debe ser firmado por el Responsable Funcional de las Actividades de Tratamiento **CLIENTES/PACIENTES/PROVEEDORES/GESTIÓN DE RRHH/SELECCIÓN DE PERSONAL,** recogidas en el **Anexo I** del presente Manual de Protección de Datos.

Nombramiento:

IBIZA NURSE SERVICE S.L, como Responsable del Tratamiento, designa a **Mª VICTORIA CEGARRA GUTIERREZ** como Responsable Funcional de las Actividades de Tratamiento **CLIENTES/PACIENTES/PROVEEDORES/GESTIÓN DE RRHH/SELECCIÓN DE PERSONAL.**

Como Responsable Funcional, **Mª VICTORIA CEGARRA GUTIERREZ** se encargará de llevar a cabo las "**Funciones y obligaciones de los Responsables Funcionales**" enumeradas en el apartado 4.4 del Manual de Protección de Datos, así como todas aquellas que sean necesarias para colaborar con el Delegado de Protección de Datos, el Gestor de Solicitudes de Ejercicio de Derechos y el Responsable de Seguridad Técnico en el cumplimiento de la normativa estatal y europea vigente en protección de datos y, especialmente, en el Reglamento Europeo de Protección de Datos (RGPD).

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde a los Responsables del Tratamiento, a los Encargados de Tratamiento y al Delegado de Protección de Datos (DPO) de la Sociedad.

Fecha

Firma

→ El presente nombramiento debe ser firmado por el Responsable Funcional de la Actividad de Tratamiento , recogida en el **Anexo I** del presente Manual de Protección de Datos.

Nombramiento:

IBIZA NURSE SERVICE S.L, como Responsable del Tratamiento, designa a **……..** como Responsable Funcional de la Actividad de Tratamiento **…… .**

Como Responsable Funcional,se encargará de llevar a cabo las "**Funciones y obligaciones de los Responsables Funcionales**" enumeradas en el apartado 4.4 del Manual de Protección de Datos, así como todas aquellas que sean necesarias para colaborar con el Delegado de Protección de Datos, el Gestor de Solicitudes de Ejercicio de Derechos y el Responsable de Seguridad Técnico en el cumplimiento de la normativa estatal y europea vigente en protección de datos y, especialmente, en el Reglamento Europeo de Protección de Datos (RGPD).

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde a los Responsables del Tratamiento, a los Encargados de Tratamiento y al Delegado de Protección de Datos (DPO) de la Sociedad.

Fecha

Firma

NOMBRAMIENTO DEL RESPONSABLE DE SEGURIDAD TÉCNICO

El presente nombramiento debe ser firmado por el Responsable de Seguridad Técnico.

Nombramiento:

IBIZA NURSE SERVICE S.L, como Responsable del Tratamiento, designa a **Mª VICTORIA CEGARRA GUTIERREZ** como Responsable de Seguridad Técnico para la correcta implantación de las medidas de seguridad en los sistemas de información de la Sociedad.

Como Responsable de Seguridad Técnico, **Mª VICTORIA CEGARRA GUTIERREZ** se encargará de llevar a cabo las "**Funciones y obligaciones del Responsable de Seguridad Técnico**" enumeradas en el apartado 4.4 del Manual de Protección de Datos, así como todas aquellas que sean necesarias para colaborar con el Delegado de Protección de Datos, el Gestor de Solicitudes de Ejercicio de Derechos y los Responsables Funcionales en el cumplimiento de la normativa estatal y europea vigente en protección de datos y, especialmente, en el Reglamento Europeo de Protección de Datos (RGPD).

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde a los Responsables del Tratamiento, a los Encargados de Tratamiento y al Delegado de Protección de Datos (DPO) de la Sociedad.

Fecha

Firma

NOMBRAMIENTO DEL GESTOR DE SOLICITUDES DE EJERCICIO DE DERECHOS

El presente nombramiento debe ser firmado por el Gestor de Solicitudes de Ejercicio de Derechos.

Nombramiento:

IBIZA NURSE SERVICE S.L, como Responsable del Tratamiento, designa a **Mª VICTORIA CEGARRA GUTIERREZ** como Gestor de Solicitudes de Ejercicio de Derechos, de acuerdo al procedimiento establecido en el presente 7 del Manual de Protección de Datos.

Como Gestor de Solicitudes de Ejercicio de Derechos, **Mª VICTORIA CEGARRA GUTIERREZ** se encargará de atender, gestionar y contestar en plazo las solicitudes de ejercicio de derechos de los interesados dirigidas a **IBIZA NURSE SERVICE S.L,** de acuerdo al procedimiento establecido en el apartado 7 del Manual de Protección de Datos y en sus Anexos **XI** y **XII**, así como a la normativa estatal y europea vigente en protección de datos y, especialmente, en el Reglamento Europeo de Protección de Datos (RGPD).

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde a los Responsables del Tratamiento, a los Encargados de Tratamiento y al Delegado de Protección de Datos (DPO) de la Sociedad.

Fecha

Firma

ANEXO XIV. Cláusulas Informativas

- Empleados
- Estudiantes en prácticas
- Candidatos
- Potenciales Clientes
- Clientes
- Proveedores
- Facturas
- Firma para Correos Electrónicos (Opcional)

Empleados

(La presente cláusula han de firmarla todos los empleados de la Sociedad como Anexo al contrato de trabajo que hayan firmado, bien en el momento de la contratación) En el caso de que no se realicen tratamientos con huellas biométricas de empleados, no se traten imágenes con fines de videovigilancia, no se lleven a cabo grabaciones de sonidos o no se empleen dispositivos de geolocalización, podrá eliminarse la parte de la cláusula marcada en rojo).

Nombre:

Apellidos:

DNI:

Le informamos que los datos personales que nos facilitó para la realización del contrato laboral y los datos que nos facilite durante su relación laboral, serán tratados por **IBIZA NURSE SERVICE S.L** con la finalidad de Recursos Humanos, Gestión de Nóminas, Prevención de Riesgos Laborales, Análisis de perfiles. Le informamos que para la realización de estas gestiones es necesario que sus datos sean cedidos a entidades financieras (para el pago de nómina), a la administración pública con competencia en la materia, a organismos de la Seguridad Social y a la Administración Tributaria, a la Fundación Tripartita, a entidades aseguradoras, a la Mutua de Accidente de Trabajo y Servicios de Prevención, a Sindicatos y Juntas de Personal, y a las Fuerzas y Cuerpos de Seguridad.

Política Interna de Garantía de los Derechos Digitales en el ámbito laboral

De acuerdo con el art. 20 del Estatuto de los Trabajadores (ET), el trabajador está obligado a realizar el trabajo convenido con diligencia debida y colaboración. En base a este artículo, **IBIZA NURSE SERVICE S.L** puede adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad.

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 **IBIZA NURSE SERVICE S.L** , a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia, grabación de sonidos y geolocalización.

A la hora de tomar la decisión de instalar un sistema de videovigilancia, de grabación de sonidos o de geolocalización, o un control de acceso o presencia a través de huella digital, **IBIZA NURSE SERVICE**

S.L tendrá en cuenta el **triple juicio de proporcionalidad** exigido por la normativa de protección de datos:

- Idoneidad: que la medida implantada sea susceptible de conseguir el objetivo propuesto.
- Necesidad: que no exista otra medida más moderada para conseguir dicha finalidad
- Proporcionalidad: que la medida implantada sea ponderada o equilibrada, es decir, que tal medida aporta más beneficios o ventajas a la empresa que perjuicios a los trabajadores (intromisión en la privacidad de los trabajadores).

Desconexión digital de los trabajadores ***– lo dispuesto en este apartado queda sujeto a lo establecido en negociación colectiva o en lo acordado con los representantes de los trabajadores***

Los trabajadores de **IBIZA NURSE SERVICE S.L** tienen derecho a la desconexión digital con el fin de garantizar, fuera del horario laboral, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

Por esto motivo, salvo causa de fuerza mayor o circunstancias excepcionales:

- la Dirección de **IBIZA NURSE SERVICE S.L** debe procurar evitar enviar comunicaciones electrónicas o realizar llamadas a sus trabajadores fuera del horario laboral,
- los trabajadores de **IBIZA NURSE SERVICE S.L** tienen derecho a no ser molestados en su tiempo libre y a no contestar en caso de recibir comunicaciones electrónicas o llamadas fuera del horario laboral o en vacaciones.

Los trabajadores de **IBIZA NURSE SERVICE S.L** pueden incluir en la firma de sus mails el siguiente texto o uno similar:

> **Nuestro horario de desconexión digital es nuestro tiempo no laboral:**
> de lunes a jueves, de __h a __h; viernes a partir de las __h; sábados, domingos y festivos.

IBIZA NURSE SERVICE S.L enviará periódicamente recordatorios a Directivos y a trabajadores, por ejemplo, a través de píldoras informativas, en el que se refuerce la concienciación del personal sobre el uso razonable de las herramientas tecnológicas puestas a disposición de los trabajadores y se procure evitar el riesgo de fatiga informática, especialmente en los supuestos de realización total o parcial del trabajo a distancia o en el domicilio del trabajador.

Dispositivos digitales - ***en la elaboración de esta política deberán participar los representantes de los trabajadores***

Salvo autorización expresa de **IBIZA NURSE SERVICE S.L** , en general se prohíbe el uso de los equipos, dispositivos digitales, correo electrónico e Internet para cualquier utilización que no esté relacionada de forma directa con las tareas y labores a realizar por el trabajador.

No obstante, el trabajador podrá utilizar los equipos y dispositivos digitales (smartphones tablets, portátiles…) que **IBIZA NURSE SERVICE S.L** ha puesto a su disposición, para uso personal en horario de descanso o fuera de la jornada laboral o en caso de emergencia, siempre teniendo en cuenta que el trabajador está obligado a cumplir con lo dispuesto sobre el uso del correo electrónico, de Internet, de aplicaciones y de dispositivos móviles en el apartado "Funciones y Obligaciones del Personal o Usuarios" del **Manual de Protección de Datos** de **IBIZA NURSE SERVICE S.L**.

Con la finalidad de llevar un control de la actividad productiva y de las obligaciones laborales y estatutarias de los trabajadores establecidas en el art. 20.3 ET, así como para controlar la integridad de los dispositivos digitales (ordenadores, portátiles, tablets, smartphone, etc.) puestos a disposición de los trabajadores para desarrollar sus funciones, **IBIZA NURSE SERVICE S.L** puede tener acceso a dichos dispositivos y a los contenidos derivados de su uso (equipos, aplicaciones, internet, correo electrónico, comunicaciones electrónicas, etc.). Por ejemplo, **IBIZA NURSE SERVICE S.L** podrá llevar a cabo controles sobre el volumen de información transmitida en los correos electrónicos, revisión del contenido de los correos electrónicos, el flujo de comunicaciones electrónicas, el acceso a determinadas páginas previamente bloqueadas (redes sociales, páginas de descarga de software…), la duración de las visitas a páginas web, etc.

Los resultados de estos controles podrán ser utilizadas en sede disciplinaria laboral.

Igualmente, **IBIZA NURSE SERVICE S.L** podrá acceder al contenido de los equipos, dispositivos digitales y correos electrónicos una vez el trabajador haya finalizado sus relaciones con la empresa, así como en tiempos prolongados de vacaciones o bajas laborales, con la única finalidad de poder continuar con la labor llevada a cabo por el trabajador y atender los proyectos puestos en marcha por el trabajador.

Para llevar a cabo estas labores de control y continuación de proyectos**IBIZA NURSE SERVICE S.L** garantizará la intimidad de los trabajadores, evitando el acceso a correos electrónicos o a contenidos que se hayan detectado como personales.

En caso de que **IBIZA NURSE SERVICE S.L,** por incidencias técnicas, necesite acceder de forma remota al equipo o a los dispositivos digitales puestos a disposición de los trabajadores, éstos serán previamente avisados y técnicamente deberán poder aceptar o denegar dicho acceso remoto, con la única excepción de que la empresa sospeche de actividades ilegales por parte del trabajador.

Huella biométrica– ***se recomienda informar previamente a los representantes de los trabajadores de la adopción de esta medida***

Respetando en todo momento la intimidad de los trabajadores, **IBIZA NURSE SERVICE S.L**puede hacer uso de la información obtenida a través del sistema de control de acceso y/o presencia con la finalidad de responder a la necesidad de seguridad de las instalaciones, de los bienes y de las personas que en ellas se encuentran, así como para control de la actividad productiva y de las obligaciones laborales y estatutarias de los trabajadores establecidas en el art. 20.3 ET.

Los resultados de estos controles podrán ser utilizadas en sede disciplinaria laboral.

IBIZA NURSE SERVICE S.L informará previamente a los trabajadores de la instalación de este sistema y su finalidad.

Videovigilancia ***– deberá informarse a los representantes de los trabajadores de la adopción de esta medida***

Respetando en todo momento la intimidad de los trabajadores, **IBIZA NURSE SERVICE S.L** puede hacer uso de las imágenes grabadas por las cámaras de videovigilancia, con la finalidad de responder a la necesidad de seguridad de las instalaciones, de los bienes y de las personas que en ellas se encuentran, así como para control de la actividad productiva y de las obligaciones laborales y estatutarias de los trabajadores establecidas en el art. 20.3 ET.

Los resultados de estos controles podrán ser utilizadas en sede disciplinaria laboral.

IBIZA NURSE SERVICE S.L colocará carteles de aviso en todas las zonas videovigiladas o en los accesos a dichas zonas. En ningún caso se instalarán cámaras de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores, en vestuarios, aseos, comedores o análogos.

Las imágenes grabadas serán conservadas durante un plazo máximo de un mes.

De conformidad con lo establecido en la L.O. 1/1982 de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen autorizo a **IBIZA NURSE SERVICE S.L** a incluir mis imágenes en los medios y soportes de comunicación (páginas web, revistas, videos, medios de comunicación, memorias, carteles, etc.) que considere oportuno, con el fin de difundir los servicios y productos que la empresa ofrece. **IBIZA NURSE SERVICE S.L** no podrá utilizar estas imágenes para finalidades distintas.

□ **NO** autorizo dicho tratamiento

□ **SI** autorizo dicho tratamiento

En el caso de que el trabajador, como usuario autorizado, acceda a datos personales cuyo Responsable o Encargado del Tratamiento sea **IBIZA NURSE SERVICE S.L**, manifiesta que tiene pleno conocimiento del Manual de Protección de Datos que se encuentra en dicha Sociedad y de las obligaciones que, en materia de protección de datos, le conciernen en su condición de usuario, entre las que se encuentra el **deber de secreto profesional** respecto a los datos personales a los que tenga acceso, incluso una vez finalizada su relación con **IBIZA NURSE SERVICE S.L.**

Grabación de sonidos* – *deberá informarse a los representantes de los trabajadores de la adopción de esta medida

Respetando en todo momento la intimidad de los trabajadores y siempre que exista un riesgo relevante en la seguridad de las instalaciones, de los bienes y de las personas que en ellas se encuentran, derivados de la actividad que se desarrolle en el centro de trabajo, respetando el principio de intervención mínima, **IBIZA NURSE SERVICE S.L** puede hacer uso de los sonidos grabados por los sistemas de grabación.

IBIZA NURSE SERVICE S.L informará previamente a los trabajadores de la instalación de sistemas de grabación de sonidos y de su ubicación. En ningún caso se instalarán sistemas de grabación de sonidos en lugares destinados al descanso o esparcimiento de los trabajadores, en vestuarios, aseos, comedores o análogos.

Los sonidos grabados serán conservados durante un plazo máximo de un mes.

Geolocalización – deberá informarse a los representantes de los trabajadores de la adopción de esta medida

Respetando en todo momento la intimidad de los trabajadores, **IBIZA NURSE SERVICE S.L** puede tratar los datos de geolocalización para control de la actividad productiva y de las obligaciones laborales y estatutarias de los trabajadores establecidas en el art. 20.3 ET.

Los resultados de estos controles podrán ser utilizadas en sede disciplinaria laboral.

IBIZA NURSE SERVICE S.L informará previamente al trabajador sobre la ubicación del sistema de geolocalización.

El trabajador tiene derecho a desactivar dicho sistema en horario de descanso o fuera de la jornada laboral.

Ud. puede ejercer sus derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento de sus datos dirigiéndose a **IBIZA NURSE SERVICE S.L**, C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares) o a **info@ibizanurseservice.com**, 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).

En Ibiza a .....de.....de 20

Firma del trabajador:

Estudiantes en prácticas

La Sociedad pone en conocimiento de los estudiantes en prácticas que, conforme al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD-GDD), quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal, están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular o, en su caso, con el responsable del mismo.

Por ello, el que suscribe declara expresa y formalmente conocer:

- La obligación de guardar secreto que le incumbe con relación a los datos personales a los que está autorizado a acceder en virtud de su responsabilidad profesional, laboral o de cualquier otra naturaleza que ostenta, o con relación a los datos de esa naturaleza a los que accediese por cualquier otra circunstancia.

- Las consecuencias sancionadoras de orden administrativo y penal que puede acarrear su incumplimiento, así como las eventuales indemnizaciones por responsabilidad de daños y perjuicios que la infracción puede llevar aparejadas.

- Y a estos efectos, declara expresa y formalmente su compromiso de cumplir con este deber de guardar secreto, aceptando y asumiendo, en otro caso, su responsabilidad personal frente al titular de los datos personales para resarcirle personalmente de los daños y perjuicios que se le pudieren irrogar al titular como consecuencia de su incumplimiento culpable, aceptando asimismo las consecuencias sancionadoras de orden laboral o profesional que se arbitren al efecto por los procedimientos legalmente procedentes.

En cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD-GDD), por la que se regula la cesión o comunicación de datos de carácter personal por parte del Responsable a terceros, le informamos de que sus datos personales podrán serán comunicados a los Organismos y Administraciones públicas que corresponda.

Nombre y Apellidos:

DNI:

Fecha y firma

Política Interna de Garantía de los Derechos Digitales

De acuerdo al convenio de colaboración, el estudiante en prácticas está obligado a realizar el trabajo convenido con diligencia debida y colaboración. En base a este artículo, **IBIZA NURSE SERVICE S.L** puede adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el estudiante en prácticas de sus obligaciones y deberes ~~laborales~~, guardando en su adopción y aplicación la consideración debida a su dignidad.

De acuerdo con el art. 20 bis ET, los estudiantes en prácticas tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por **IBIZA NURSE SERVICE S.L** , a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia, grabación de sonidos y geolocalización.

A la hora de tomar la decisión de instalar un sistema de videovigilancia, de grabación de sonidos o de geolocalización, o un control de acceso o presencia a través de huella digital, **IBIZA NURSE SERVICE S.L** tendrá en cuenta el **triple juicio de proporcionalidad** exigido por la normativa de protección de datos:

- Idoneidad: que la medida implantada sea susceptible de conseguir el objetivo propuesto.
- Necesidad: que no exista otra medida más moderada para conseguir dicha finalidad
- Proporcionalidad: que la medida implantada sea ponderada o equilibrada, es decir, que tal medida aporta más beneficios o ventajas a la empresa que perjuicios a los trabajadores (intromisión en la privacidad de los trabajadores).

Desconexión digital de los estudiante en prácticas

Los estudiantes en prácticas de **IBIZA NURSE SERVICE S.L** tienen derecho a la desconexión digital con el fin de garantizar, fuera del horario laboral, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

Por esto motivo, salvo causa de fuerza mayor o circunstancias excepcionales:

- la Dirección de **IBIZA NURSE SERVICE S.L** debe procurar evitar enviar comunicaciones electrónicas o realizar llamadas a sus estudiantes en prácticas fuera del horario laboral,
- los estudiante en prácticas de **IBIZA NURSE SERVICE S.L** tienen derecho a no ser molestados en su tiempo libre y a no contestar en caso de recibir comunicaciones electrónicas o llamadas fuera del horario laboral o en vacaciones.

Los estudiante en prácticas de **IBIZA NURSE SERVICE S.L** pueden incluir en la firma de sus mails el siguiente texto o uno similar:

> **Nuestro horario de desconexión digital es nuestro tiempo no laboral:**
> de lunes a jueves, de __h a __h; viernes a partir de las __h; sábados, domingos y festivos.

IBIZA NURSE SERVICE S.L enviará periódicamente recordatorios a estudiantes en prácticas, por ejemplo, a través de píldoras informativas, en el que se refuerce la concienciación del personal sobre el uso razonable de las herramientas tecnológicas puestas a disposición de los estudiantes en prácticas y se procure evitar el riesgo de fatiga informática, especialmente en los supuestos de realización total o parcial del trabajo a distancia o en el domicilio del estudiante en prácticas .

Dispositivos digitales

Salvo autorización expresa de **IBIZA NURSE SERVICE S.L** , en general se prohíbe el uso de los equipos, dispositivos digitales, correo electrónico e Internet para cualquier utilización que no esté relacionada de forma directa con las tareas y labores a realizar por el estudiante en prácticas.

No obstante, el estudiante en prácticas podrá utilizar los equipos y dispositivos digitales (smartphones tablets, portátiles…) que **IBIZA NURSE SERVICE S.L** ha puesto a su disposición, para uso personal en horario de descanso o fuera de la jornada laboral o en caso de emergencia, siempre teniendo en cuenta que el estudiante en prácticas está obligado a cumplir con lo dispuesto sobre el uso del correo electrónico, de Internet, de aplicaciones y de dispositivos móviles en el apartado “Funciones y Obligaciones del Personal o Usuarios” del **Manual de Protección de Datos** de **IBIZA NURSE SERVICE S.L**.

Con la finalidad de llevar un control de las prácticas, así como para controlar la integridad de los dispositivos digitales (ordenadores, portátiles, tablets, smartphone, etc.) puestos a disposición de los estudiantes en prácticas para desarrollar sus funciones, **IBIZA NURSE SERVICE S.L** puede tener acceso a dichos dispositivos y a los contenidos derivados de su uso (equipos, aplicaciones, internet,

correo electrónico, comunicaciones electrónicas, etc.). Por ejemplo, **IBIZA NURSE SERVICE S.L** podrá llevar a cabo controles sobre el volumen de información transmitida en los correos electrónicos, revisión del contenido de los correos electrónicos, el flujo de comunicaciones electrónicas, el acceso a determinadas páginas previamente bloqueadas (redes sociales, páginas de descarga de software…), la duración de las visitas a páginas web, etc.

Igualmente, **IBIZA NURSE SERVICE S.L** podrá acceder al contenido de los equipos, dispositivos digitales y correos electrónicos una vez el estudiante en prácticas haya finalizado sus relaciones con la empresa, así como en tiempos prolongados de vacaciones o bajas laborales, con la única finalidad de poder continuar con la labor llevada a cabo por el estudiante en prácticas y atender los proyectos puestos en marcha por el estudiante en prácticas.

Para llevar a cabo estas labores de control y continuación de proyectos **IBIZA NURSE SERVICE S.L** garantizará la intimidad de los estudiantes en prácticas, evitando el acceso a correos electrónicos o a contenidos que se hayan detectado como personales.

En caso de que **IBIZA NURSE SERVICE S.L,** por incidencias técnicas, necesite acceder de forma remota al equipo o a los dispositivos digitales puestos a disposición de los estudiante en prácticas, éstos serán previamente avisados y técnicamente deberán poder aceptar o denegar dicho acceso remoto, con la única excepción de que la empresa sospeche de actividades ilegales por parte del estudiante en prácticas.

Huella biométrica

Respetando en todo momento la intimidad de los estudiante en prácticas, **IBIZA NURSE SERVICE S.L** puede hacer uso de la información obtenida a través del sistema de control de acceso y/o presencia con la finalidad de responder a la necesidad de seguridad de las instalaciones, de los bienes y de las personas que en ellas se encuentran, así como para evaluar la realización de las prácticas.

Los resultados de estos controles podrán ser utilizados en la evaluación de las prácticas

IBIZA NURSE SERVICE S.L informará previamente a los estudiante en prácticas de la instalación de este sistema y su finalidad.

Videovigilancia

Respetando en todo momento la intimidad de los estudiante en prácticas, **IBIZA NURSE SERVICE S.L** puede hacer uso de las imágenes grabadas por las cámaras de videovigilancia, con la finalidad de responder a la necesidad de seguridad de las instalaciones, de los bienes y de las personas que en ellas se encuentran**,** así como para control de las prácticas

Los resultados de estos controles podrán ser utilizadas en la evaluación de las prácticas.

IBIZA NURSE SERVICE S.L colocará carteles de aviso en todas las zonas videovigiladas o en los accesos a dichas zonas. En ningún caso se instalarán cámaras de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores y estudiantes en prácticas, en vestuarios, aseos, comedores o análogos.

Las imágenes grabadas serán conservadas durante un plazo máximo de un mes.

Grabación de sonidos

Respetando en todo momento la intimidad de los estudiantes en prácticas y siempre que exista un riesgo relevante en la seguridad de las instalaciones, de los bienes y de las personas que en ellas se encuentran, derivados de la actividad que se desarrolle en el centro de trabajo, respetando el principio de intervención mínima, **IBIZA NURSE SERVICE S.L** puede hacer uso de los sonidos grabados por los sistemas de grabación.

IBIZA NURSE SERVICE S.L informará previamente a los estudiantes en prácticas de la instalación de sistemas de grabación de sonidos y de su ubicación. En ningún caso se instalarán sistemas de grabación de sonidos en lugares destinados al descanso o esparcimiento de los trabajadores, en vestuarios, aseos, comedores o análogos.

Los sonidos grabados serán conservados durante un plazo máximo de un mes.

Geolocalización

Respetando en todo momento la intimidad de los estudiante en prácticas, **IBIZA NURSE SERVICE S.L** puede tratar los datos de geolocalización para control de la realización de las prácticas

IBIZA NURSE SERVICE S.L informará previamente al estudiante en prácticas sobre la ubicación del sistema de geolocalización.

El estudiante en prácticas tiene derecho a desactivar dicho sistema en horario de descanso o fuera de la jornada laboral.

Ud. puede ejercer sus derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento de sus datos dirigiéndose a **IBIZA NURSE SERVICE S.L**, C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares) o a **info@ibizanurseservice.com**, 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).

En Ibiza a .....de.....de 20

Firma del estudiante en prácticas:

Candidatos

(La presente cláusula debe facilitarse a las personas que entreguen su cv a la Sociedad)

Nombre:

Apellidos:

DNI:

De conformidad con el RGPD y de la LOPD-GDD, le informamos que sus datos personales, procedentes de una empresa de selección de personal, serán tratados por **IBIZA NURSE SERVICE S.L** con la finalidad de gestionar los procesos de selección de los puestos vacantes que genere la Sociedad.

Este tratamiento de datos es necesario para la aplicación de medidas precontractuales (toma de decisiones previa a la contratación laboral).

No se realizarán cesiones de datos de sus datos personales.

Igualmente, le informamos que transcurrido un año desde la recepción de los datos, éstos serán eliminados.

Ud. puede ejercer sus derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento de sus datos dirigiéndose a **IBIZA NURSE SERVICE S.L**, C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares) o a **info@ibizanurseservice.com**, 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).

En Ibiza a .....de.....de 20

Firma del candidato:

Potenciales Clientes

(La siguiente cláusula deberá ser firmada con sus potenciales clientes. En el caso de que no se realicen envíos comerciales, podrá eliminarse la parte de la cláusula marcada en rojo).

De conformidad con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales relativo a la Protección de las Personas físicas, y conforme a disposiciones reglamentarias reflejadas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, le informamos que sus datos personales serán tratados por **IBIZA NURSE SERVICE S.L** con la finalidad de gestionar su consulta; y, si nos da su consentimiento marcando la casilla correspondiente, enviarle comunicaciones comerciales que puedan ser de su interés.

- Marque esta casilla si desea recibir comunicaciones comerciales.

Sus datos no serán cedidos a terceros. El tratamiento de sus datos se llevará a cabo en base el interés legítimo en atender su solicitud. Sus datos serán conservados por el plazo estrictamente necesario para dar contestación a su solicitud.

Ud. puede ejercer sus derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento de sus datos dirigiéndose a **IBIZA NURSE SERVICE S.L**, C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares) o a **info@ibizanurseservice.com**, 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).

En Ibiza a .....de.....de 20

Firma del cliente:

Clientes

(La siguiente cláusula deberá ser incluida en todos los nuevos contratos que firmen con sus clientes y, en su defecto, en los documentos que intercambien con ellos. En el caso de que no se realicen envíos comerciales, podrá eliminarse la parte de la cláusula marcada en rojo).

De conformidad con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales relativo a la Protección de las Personas físicas, y conforme a disposiciones reglamentarias reflejadas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, le informamos que sus datos personales serán tratados por **IBIZA NURSE SERVICE S.L** con la finalidad de Gestión contable, fiscal y administrativa de los datos de los clientes; mantener las relaciones contractuales, comerciales y profesionales que nos unen a Usted; En base a la relación existente, podremos enviar comunicaciones sobre servicios similares a los contratados, basado en el interés legítimo en informar de servicios que puedan ser de su interés. Ud. puede oponerse libremente a recibir las comunicaciones comerciales que podamos enviarle y que puedan resultar de su interés, sin que ello condicione la ejecución del contrato.

Le informamos que para la realización de estas gestiones es necesario que sus datos sean cedidos a los Organismos y Administraciones Públicas que corresponda, Consejería de Sanidad y a las entidades bancarias con las que trabajamos.

Estos tratamientos de datos son necesarios para la ejecución del contrato con su empresa y para la satisfacción de los intereses legítimos perseguidos por ambas partes. Igualmente, le informamos que sus datos serán conservados mientras se mantenga la relación mercantil o durante los plazos establecidos por la legislación fiscal.

Igualmente, le informamos que sus datos serán conservados mientras se mantenga la relación mercantil o durante los plazos establecidos por la legislación fiscal.

Ud. puede ejercer sus derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento de sus datos dirigiéndose a **IBIZA NURSE SERVICE S.L**, C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares) o a **info@ibizanurseservice.com**, 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).

- Marque esta casilla si desea recibir comunicaciones comerciales.

En Ibiza a .....de.....de 20

Firma del cliente:

Proveedores

(La siguiente cláusula deberá ser incluida en todos los nuevos contratos que firmen con sus proveedores y, en su defecto, en los documentos que intercambien con ellos. En el caso de que no se realicen envíos comerciales, podrá eliminarse la parte de la cláusula marcada en rojo)

De conformidad con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales relativo a la Protección de las Personas físicas, y conforme a disposiciones reglamentarias reflejadas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, le informamos que sus datos personales serán tratados por **IBIZA NURSE SERVICE S.L** con la finalidad de Gestión contable, fiscal y administrativa de los datos de los proveedores; mantener las relaciones contractuales, comerciales y profesionales que nos unen a Usted, y, si nos da su consentimiento marcando la casilla correspondiente, enviarle comunicaciones comerciales que puedan ser de su interés.

Le informamos que para la realización de estas gestiones, sus datos personales serán comunicados a los Organismos y Administraciones públicas que corresponda, y a las entidades bancarias con las que trabajamos.

Estos tratamientos de datos son necesarios para la aplicación de medidas precontractuales (toma de decisiones previa a la contratación mercantil) o, en su caso, la ejecución del contrato con su empresa, así como para la satisfacción de los interés legítimos perseguidos por ambas partes.

Ud. puede oponerse libremente a recibir comunicaciones comerciales, sin que ello condicione la ejecución del contrato.

Igualmente, le informamos que sus datos serán conservados mientras se mantenga la relación mercantil o durante los plazos establecidos por la legislación fiscal.

Ud. puede ejercer sus derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento de sus datos dirigiéndose a **IBIZA NURSE SERVICE S.L** C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares) o a **info@ibizanurseservice.com**, 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).

- Marque esta casilla si desea recibir comunicaciones comerciales.

En Ibiza a .....de.....de 20..

Firma del proveedor:

Facturas

De conformidad con el RGPD y de la LOPD-GDD, le informamos que los datos personales que figuran en este documento son tratados por **IBIZA NURSE SERVICE S.L** con la finalidad de cumplir con la prestación de servicios y las obligaciones legales al respecto. Dichos datos son tratados de manera confidencial, cumpliendo con las medidas de seguridad establecidas en materia de protección de datos. Como titular de los datos, usted podrá ejercitar los derechos que le reconoce la normativa aplicable al efecto, ejerciendo los mismos ante **IBIZA NURSE SERVICE S.L** (C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares)) ó a través de correo electrónico (**info@ibizanurseservice.com**).

Firma para Correos Electrónicos (Opcional)

Este mensaje y sus archivos adjuntos son confidenciales y únicamente podrán ser usados por la persona o entidad a la que van dirigidos. Este mensaje puede contener información confidencial o legalmente protegida. No hay renuncia a la confidencialidad o secreto profesional por cualquier transmisión defectuosa o errónea. Si usted ha recibido este mensaje por error notifíqueselo inmediatamente al remitente.

De conformidad con el RGPD y de la LOPD-GDD, le informamos que sus datos personales son tratados por **IBIZA NURSE SERVICE S.L** con la finalidad de gestionar y mantener las relaciones profesionales que nos unen con Usted. Sus datos podrán ser cedidos a las entidades y administraciones públicas necesarias para la realización de dicha gestión. Este tratamiento de datos es necesario para mantener dicha relación profesional. Los datos se eliminarán cuando finalicen los plazos de prescripción marcados por la ley, conservándose únicamente para atender posibles reclamaciones. Ud. puede ejercer sus derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento de sus datos dirigiéndose a **IBIZA NURSE SERVICE S.L** C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares) o a **info@ibizanurseservice.com**, 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).

ANEXO XV. Contratos de prestación de servicios

Contrato con PROVEEDORES de prestación de servicios con acceso a datos personales

(El siguiente contrato ha de ser firmado con los proveedores de servicios con acceso a datos personales responsabilidad de IBIZA NURSE SERVICE S.L)

Ibiza, a ..... de ..... de 20..

Reunidos

De una parte, D/Dña. _____, mayor de edad, con NIF _____, en nombre y representación de **IBIZA NURSE SERVICE S.L**, con C.I.F. nº **B13656897** y con domicilio en C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares), en adelante el responsable del tratamiento.

De otra parte, D/Dña. _____, mayor de edad, con NIF _____, en nombre y representación de **NIN DE CARDONA SL,** con C.I.F. nº **B30808372** y con domicilio en Plaza Castellini nº3 4º Derecha; 30201 Cartagena (Murcia), en adelante el encargado del tratamiento.

Manifiestan

I. Que el responsable del tratamiento se dedica a **la prestación de servicios sanitarios en entornos sanitarios privados y a domicilio**

II. Que el encargado del tratamiento se dedica a **la prestación de servicios de asesoramiento asesoria contable, fiscal y laboral**

III. Que, ambas partes se reconocen mutuamente la capacidad legal necesaria para contratar y obligarse, y, en especial, para celebrar el presente Contrato, llevándolo a efecto conforme a las siguientes:

Estipulaciones

1. Objeto del encargo del tratamiento

Mediante las presentes cláusulas se habilita al encargado del tratamiento para tratar por cuenta del responsable del tratamiento, los datos personales necesarios para prestar el **servicio de Gestión contable, fiscal, administrativa y laboral**

El tratamiento consistirá en **Gestión de impuestos, facturas, gestiones frente a la administración pública, elaboración de contratos, gestión de nóminas, seguros sociales y otros usos relacionados con temas laborales**

Concreción de los tratamientos a realizar: **Recogida de datos, Registro en los sistemas,Almacenamiento,Consulta,Supresión**

2. Identificación de la información afectada
Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el responsable del tratamiento pone a disposición del encargado del tratamiento, la información que se describe a continuación:

- **Categoría de interesados: Trabajadores, Candidatos, Clientes, Proveedores, Otros**

- **Categoría de datos: Datos identificativos, Datos de características personales, Datos de circunstancias sociales, Datos académicos y profesionales, Datos de detalles de empleo, Datos económicos, financieros y de seguros, Otros**

3. Duración
La duración del acuerdo está vinculado a la duración del contrato principal

4. Obligaciones del encargado del tratamiento
El encargado del tratamiento y todo su personal se obliga a:

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

b) Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.

   Si el encargado del tratamiento considera que alguna de las instrucciones infringe el Reglamento Europeo General de Protección de Datos (RGPD) o la normativa española vigente de protección de datos personales, el encargado informará inmediatamente al responsable.

c) Con la plena aplicación 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 (RGPD) estará obligado a llevar, por escrito, un **registro** de todas las categorías de **actividades de tratamiento** efectuadas por cuenta del responsable, que contenga:

   - El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.

   - Las categorías de tratamientos efectuados por cuenta de cada responsable.

   - En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.

- Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:
    - La seudonimización y el cifrado de datos personales, en su caso.
    - La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes 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.
    - El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d) **No comunicar los datos a terceras personas**, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.

El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

e) **Subcontratación**

No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, excepto los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.

Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de una semana, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido.

El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

f) Mantener el deber de secreto respecto a los datos personales a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

g) Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

h) Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i) Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j) Asistir al responsable del tratamiento en la respuesta al **ejercicio de los derechos** de acceso, rectificación, supresión y oposición.

   También deberá asistir al responsable del tratamiento en la respuesta al ejercicio del derecho a la limitación del tratamiento, del derecho a la portabilidad de datos y al derecho a no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles).

   Cuando las personas afectadas ejerzan alguno de estos derechos ante el encargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección **info@ibizanurseservice.com**. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

k) **Derecho de información**

   Corresponde al responsable del tratamiento facilitar el derecho de información en el momento de la recogida de los datos.

l) **Notificación de violaciones de la seguridad de los datos**

   El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas y a través de **info@ibizanurseservice.com**, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

   No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

   Si se dispone de ella se facilitará, como mínimo, la información siguiente:

   - Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

   - El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

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

Corresponderá al responsable del tratamiento comunicar las violaciones de la seguridad de los datos a la Autoridad de Protección de Datos.

La comunicación contendrá, como mínimo, la información siguiente:

- Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

- Nombre y datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

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

Corresponderá al responsable del tratamiento comunicar en el menor tiempo posible las violaciones de la seguridad de los datos a los interesados, cuando sea probable que la violación suponga un alto riesgo para los derechos y las libertades de las personas físicas.

La comunicación debe realizarse en un lenguaje claro y sencillo y deberá, como mínimo:

- Explicar la naturaleza de la violación de datos.

- Indicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

- Describir las posibles consecuencias de la violación de la seguridad de los datos personales.

Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

m) Únicamente en el caso de que sea necesario, el encargado del tratamiento dará apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos.

n) Dará apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

o) Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

p) El encargado del tratamiento deberá implantar las medidas de seguridad que sean acordes a la evaluación de riesgos que hayan podido realizar o a los códigos de conducta, sello, certificación u otro estándar de seguridad que les sean aplicables. En todo caso, deberá implantar mecanismos para:

- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
- Seudonimizar y cifrar los datos personales, en caso de resultar necesario.

q) El encargado del tratamiento deberá designar un delegado de protección de datos y comunicar su identidad y datos de contacto al responsable, si está obligado a ello por lo dispuesto en el RGPD o normativa española vigente en protección de datos.

r) **Destino de los datos**

Devolver al responsable del tratamiento y, si procede, los soportes donde consten, una vez cumplida la prestación.; y destruir cualquier copia que esté en su poder.

Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado al responsable del tratamiento.

No obstante, el encargado puede conservar una copia, con los datos debidamente boqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

5. Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

- Entregar al encargado los datos a los que se refiere la cláusula 1 de este documento.

- Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado, si están obligados a ello por lo dispuesto en el RGPD o normativa española vigente en protección de datos.

- Realizar las consultas previas que corresponda.

- Velar, de forma previa y durante todo el tratamiento, por el cumplimiento de la normativa vigente en protección de datos por parte del encargado.

- Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

6. Cláusula informativa

Ambas partes se informan que los datos personales contenidos en el presente contrato y los proporcionados durante la relación negocial serán objeto de tratamiento por la otra parte, con la finalidad de llevar a cabo la gestión de la relación contractual generada con la firma del presente documento. Los datos podrán ser cedidos a la administración pública en los casos previstos por la ley y a las entidades bancarias necesarias para realizar dicha gestión. Sus datos serán conservados mientras se mantenga la relación mercantil o durante los plazos establecidos por la legislación fiscal. Este tratamiento de datos es imprescindible para la ejecución del presente contrato. El ejercicio de cualquiera de los derechos de protección de datos puede interponerse en las direcciones indicadas en el encabezamiento del presente contrato, indicando como referencia “Protección de datos”. En cualquier situación, Ud. tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD).

- ☐ Marque esta casilla si desea recibir comunicaciones comerciales por parte del responsable del tratamiento.
- ☐ Marque esta casilla si desea recibir comunicaciones comerciales por parte del encargado del tratamiento.

Ud. puede oponerse libremente a recibir comunicaciones comerciales, sin que ello condicione la ejecución del contrato.

7. Normativa aplicable

Igualmente, si el presente contrato continúa vigente en el momento en el que se aprueben modificaciones en la vigente normativa española de protección de datos, las partes se compromete a firmar un Anexo con nuevas condiciones en materia de protección de datos para dar pleno cumplimiento a dicha normativa.

Ambas partes, en prueba de su conformidad, firman el presente contrato, por duplicado ejemplar, en el lugar y fecha indicados ut supra.

El Responsable del tratamiento **El Encargado del tratamiento.**

Ibiza, a ..... de ..... de 20..

Reunidos

De una parte, D/Dña. _____, mayor de edad, con NIF _____, en nombre y representación de **IBIZA NURSE SERVICE S.L**, con C.I.F. nº **B13656897** y con domicilio en C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares), en adelante el responsable del tratamiento.

De otra parte, D/Dña. _____, mayor de edad, con NIF _____, en nombre y representación de **……,**con C.I.F. nº **……..** y con domicilio en **……,**en adelante el encargado del tratamiento.

Manifiestan

I. Que el responsable del tratamiento se dedica a **la prestación de servicios sanitarios en entornos sanitarios privados y a domicilio**

II. Que el encargado del tratamiento se dedica a **…….. .**

III. Que, ambas partes se reconocen mutuamente la capacidad legal necesaria para contratar y obligarse, y, en especial, para celebrar el presente Contrato, llevándolo a efecto conforme a las siguientes:

Estipulaciones

1. Objeto del encargo del tratamiento

Mediante las presentes cláusulas se habilita al encargado del tratamiento para tratar por cuenta del responsable del tratamiento, los datos personales necesarios para prestar el **servicio de …….. .**

El tratamiento consistirá en **…… .**

Concreción de los tratamientos a realizar:

2. Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el responsable del tratamiento pone a disposición del encargado del tratamiento, la información que se describe a continuación:

- **Categoría de interesados:**
- **Categoría de datos:**

3. Duración

La duración del acuerdo está vinculado a la duración del contrato principal

4. Obligaciones del encargado del tratamiento

El encargado del tratamiento y todo su personal se obliga a:

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

b) Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.

   Si el encargado del tratamiento considera que alguna de las instrucciones infringe el Reglamento Europeo General de Protección de Datos (RGPD) o la normativa española vigente de protección de datos personales, el encargado informará inmediatamente al responsable.

c) Con la plena aplicación 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 (RGPD) estará obligado a llevar, por escrito, un **registro** de todas las categorías de **actividades de tratamiento** efectuadas por cuenta del responsable, que contenga:

   - El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.

   - Las categorías de tratamientos efectuados por cuenta de cada responsable.

   - En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.

   - Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:
     - La seudonimización y el cifrado de datos personales, en su caso.
     - La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes 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.
     - El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d) **No comunicar los datos a terceras personas**, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.

   El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

   Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea

aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

e) **Subcontratación**

No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, excepto los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.

Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de una semana, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido.

El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

f) Mantener el deber de secreto respecto a los datos personales a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

g) Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

h) Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i) Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j) Asistir al responsable del tratamiento en la respuesta al **ejercicio de los derechos** de acceso, rectificación, supresión y oposición.

También deberá asistir al responsable del tratamiento en la respuesta al ejercicio del derecho a la limitación del tratamiento, del derecho a la portabilidad de datos y al derecho a no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles).

Cuando las personas afectadas ejerzan alguno de estos derechos ante el encargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección **info@ibizanurseservice.com**. La comunicación debe hacerse de forma inmediata y en ningún

caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

k) **Derecho de información**

Corresponde al responsable del tratamiento facilitar el derecho de información en el momento de la recogida de los datos.

l) **Notificación de violaciones de la seguridad de los datos**

El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas y a través de **info@ibizanurseservice.com**, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

- Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

- El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

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

Corresponderá al responsable del tratamiento comunicar las violaciones de la seguridad de los datos a la Autoridad de Protección de Datos.

La comunicación contendrá, como mínimo, la información siguiente:

- Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

- Nombre y datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

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

Corresponderá al responsable del tratamiento comunicar en el menor tiempo posible las violaciones de la seguridad de los datos a los interesados, cuando sea probable que la violación suponga un alto riesgo para los derechos y las libertades de las personas físicas.

La comunicación debe realizarse en un lenguaje claro y sencillo y deberá, como mínimo:

- Explicar la naturaleza de la violación de datos.

- Indicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

- Describir las posibles consecuencias de la violación de la seguridad de los datos personales.

Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

m) Únicamente en el caso de que sea necesario, el encargado del tratamiento dará apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos.

n) Dará apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

o) Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

p) El encargado del tratamiento deberá implantar las medidas de seguridad que sean acordes a la evaluación de riesgos que hayan podido realizar o a los códigos de conducta, sello, certificación u otro estándar de seguridad que les sean aplicables. En todo caso, deberá implantar mecanismos para:

- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
- Seudonimizar y cifrar los datos personales, en caso de resultar necesario.

q) El encargado del tratamiento deberá designar un delegado de protección de datos y comunicar su identidad y datos de contacto al responsable, si está obligado a ello por lo dispuesto en el RGPD o normativa española vigente en protección de datos.

r) **Destino de los datos**

…… y, si procede, los soportes donde consten, una vez cumplida la prestación.; y destruir cualquier copia que esté en su poder.

Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado al responsable del tratamiento.

No obstante, el encargado puede conservar una copia, con los datos debidamente boqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

5. Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

- Entregar al encargado los datos a los que se refiere la cláusula 1 de este documento.
- Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado, si están obligados a ello por lo dispuesto en el RGPD o normativa española vigente en protección de datos.
- Realizar las consultas previas que corresponda.
- Velar, de forma previa y durante todo el tratamiento, por el cumplimiento de la normativa vigente en protección de datos por parte del encargado.
- Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

6. Cláusula informativa

Ambas partes se informan que los datos personales contenidos en el presente contrato y los proporcionados durante la relación negocial serán objeto de tratamiento por la otra parte, con la finalidad de llevar a cabo la gestión de la relación contractual generada con la firma del presente documento. Los datos podrán ser cedidos a la administración pública en los casos previstos por la ley y a las entidades bancarias necesarias para realizar dicha gestión. Sus datos serán conservados mientras se mantenga la relación mercantil o durante los plazos establecidos por la legislación fiscal. Este tratamiento de datos es imprescindible para la ejecución del presente contrato. El ejercicio de cualquiera de los derechos de protección de datos puede interponerse en las direcciones indicadas en el encabezamiento del presente contrato, indicando como referencia "Protección de datos". En cualquier situación, Ud. tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD).

- ☐ Marque esta casilla si desea recibir comunicaciones comerciales por parte del responsable del tratamiento.
- ☐ Marque esta casilla si desea recibir comunicaciones comerciales por parte del encargado del tratamiento.

Ud. puede oponerse libremente a recibir comunicaciones comerciales, sin que ello condicione la ejecución del contrato.

7. Normativa aplicable

Igualmente, si el presente contrato continúa vigente en el momento en el que se aprueben modificaciones en la vigente normativa española de protección de datos, las partes se compromete a firmar un Anexo con nuevas condiciones en materia de protección de datos para dar pleno cumplimiento a dicha normativa.

Ambas partes, en prueba de su conformidad, firman el presente contrato, por duplicado ejemplar, en el lugar y fecha indicados ut supra.

El Responsable del tratamiento **El Encargado del tratamiento.**

Contrato con CLIENTES de prestación de servicios con acceso a datos personales

(El siguiente contrato ha de ser firmado con los clientes a los que IBIZA NURSE SERVICE S.L preste algún servicio con acceso a datos personales responsabilidad del cliente)

Ibiza, a ..... de ..... de 20..

Reunidos

De una parte, D/Dña. _____, mayor de edad, con NIF _____, en nombre y representación de **……..……..…..**,con C.I.F. nº **……** y con domicilio en **……..……..……..**,en adelante el responsable del tratamiento.

De otra parte, D/Dña. _____, mayor de edad, con NIF _____, en nombre y representación de **IBIZA NURSE SERVICE S.L**, con C.I.F. nº **B13656897** y con domicilio en C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares), en adelante el encargado del tratamiento.

Manifiestan

I. Que el responsable del tratamiento se dedica a **…… .**

II. Que el encargado del tratamiento se dedica a **la prestación de servicios sanitarios en entornos sanitarios privados y a domicilio**

III. Que, ambas partes se reconocen mutuamente la capacidad legal necesaria para contratar y obligarse, y, en especial, para celebrar el presente Contrato, llevándolo a efecto conforme a las siguientes:

Estipulaciones

1. Objeto del encargo del tratamiento

Mediante las presentes cláusulas se habilita al encargado del tratamiento para tratar por cuenta del responsable del tratamiento, los datos personales necesarios para prestar el **servicio de …… .**

El tratamiento consistirá en **…….. .**

Concreción de los tratamientos a realizar:

2. Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el responsable del tratamiento pone a disposición del encargado del tratamiento, la información que se describe a continuación:

- **Categoría de interesados:**
- **Categoría de datos:**

3. Duración
La duración del acuerdo está vinculado a la duración del contrato principal

4. Obligaciones del encargado del tratamiento
El encargado del tratamiento y todo su personal se obliga a:

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

b) Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.

Si el encargado del tratamiento considera que alguna de las instrucciones infringe el Reglamento Europeo General de Protección de Datos (RGPD) o la normativa española vigente de protección de datos personales, el encargado informará inmediatamente al responsable.

c) Con la plena aplicación 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 (RGPD) estará obligado a llevar, por escrito, un **registro** de todas las categorías de **actividades de tratamiento** efectuadas por cuenta del responsable, que contenga:

- El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.

- Las categorías de tratamientos efectuados por cuenta de cada responsable.

- En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.

- Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:
    - La seudonimización y el cifrado de datos personales, en su caso.
    - La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes 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.
    - El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d) No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.

El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable

identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

e) **Subcontratación**

No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, excepto los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.

Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de una semana, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido.

El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

f) Mantener el deber de secreto respecto a los datos personales a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

g) Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

h) Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i) Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j) Asistir al responsable del tratamiento en la respuesta al **ejercicio de los derechos** de acceso, rectificación, supresión y oposición.

También deberá asistir al responsable del tratamiento en la respuesta al ejercicio del derecho a la limitación del tratamiento, del derecho a la portabilidad de datos y al derecho a no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles).

Cuando las personas afectadas ejerzan alguno de estos derechos ante el encargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección **info@ibizanurseservice.com**. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

k) **Derecho de información**

Corresponde al responsable del tratamiento facilitar el derecho de información en el momento de la recogida de los datos.

l) **Notificación de violaciones de la seguridad de los datos**

El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas y a través de **info@ibizanurseservice.com**, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

- Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

- El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

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

Corresponderá al responsable del tratamiento comunicar las violaciones de la seguridad de los datos a la Autoridad de Protección de Datos.

La comunicación contendrá, como mínimo, la información siguiente:

- Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

- Nombre y datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

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

Corresponderá al responsable del tratamiento comunicar en el menor tiempo posible las violaciones de la seguridad de los datos a los interesados, cuando sea probable que la violación suponga un alto riesgo para los derechos y las libertades de las personas físicas.

La comunicación debe realizarse en un lenguaje claro y sencillo y deberá, como mínimo:

- Explicar la naturaleza de la violación de datos.

- Indicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

- Describir las posibles consecuencias de la violación de la seguridad de los datos personales.

Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

m) Únicamente en el caso de que sea necesario, el encargado del tratamiento dará apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos.

n) Dará apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

o) Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

p) El encargado del tratamiento deberá implantar las medidas de seguridad que sean acordes a la evaluación de riesgos que hayan podido realizar o a los códigos de conducta, sello, certificación u otro estándar de seguridad que les sean aplicables. En todo caso, deberá implantar mecanismos para:

- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
- Seudonimizar y cifrar los datos personales, en caso de resultar necesario.

q) El encargado del tratamiento deberá designar un delegado de protección de datos y comunicar su identidad y datos de contacto al responsable, si está obligado a ello por lo dispuesto en el RGPD o normativa española vigente en protección de datos.

r) **Destino de los datos**

…… y, si procede, los soportes donde consten, una vez cumplida la prestación.; y destruir cualquier copia que esté en su poder.

Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado al responsable del tratamiento.

No obstante, el encargado puede conservar una copia, con los datos debidamente boqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

5. Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

- Entregar al encargado los datos a los que se refiere la cláusula 2 de este documento.
- Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado, si están obligados a ello por lo dispuesto en el RGPD o normativa española vigente en protección de datos.
- Realizar las consultas previas que corresponda.
- Velar, de forma previa y durante todo el tratamiento, por el cumplimiento de la normativa vigente en protección de datos por parte del encargado.
- Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

6. Cláusula informativa

Ambas partes se informan que los datos personales contenidos en el presente contrato y los proporcionados durante la relación negocial serán objeto de tratamiento por la otra parte, con la finalidad de llevar a cabo la gestión de la relación contractual generada con la firma del presente documento. Los datos podrán ser cedidos a la administración pública en los casos previstos por la ley y a las entidades bancarias necesarias para realizar dicha gestión. Sus datos serán conservados mientras se mantenga la relación mercantil o durante los plazos establecidos por la legislación fiscal. Este tratamiento de datos es imprescindible para la ejecución del presente contrato. El ejercicio de cualquiera de los derechos de protección de datos puede interponerse en las direcciones indicadas en el encabezamiento del presente contrato, indicando como referencia "Protección de datos". En cualquier situación, Ud. tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD).

- ☐ Marque esta casilla si desea recibir comunicaciones comerciales por parte del responsable del tratamiento.
- ☐ Marque esta casilla si desea recibir comunicaciones comerciales por parte del encargado del tratamiento.

Ud. puede oponerse libremente a recibir comunicaciones comerciales, sin que ello condicione la ejecución del contrato.

7. Normativa aplicable

Igualmente, si el presente contrato continúa vigente en el momento en el que se aprueben modificaciones en la vigente normativa española de protección de datos, las partes se compromete a firmar un Anexo con nuevas condiciones en materia de protección de datos para dar pleno cumplimiento a dicha normativa.

Ambas partes, en prueba de su conformidad, firman el presente contrato, por duplicado ejemplar, en el lugar y fecha indicados ut supra.

El Responsable del tratamiento **El Encargado del tratamiento.**

Acuerdo de confidencialidad con prestadores de servicios sin acceso a datos personales

Ibiza, a ..... de ..... de 2.02…

Reunidos

De una parte,D/Dña. _____, mayor de edad, con NIF _____, en nombre y representación de **IBIZA NURSE SERVICE S.L**, con C.I.F. nº **B13656897** y con domicilio en C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares), en adelante el responsable del tratamiento.

De otra parte,D/Dña. _____, mayor de edad, con NIF _____, en nombre y representación de **……,**con C.I.F. nº **……** y con domicilio en **……**.,en adelante el prestador del servicio.

Reconociéndose ambas partes capacidad para contratar, proceden, en consecuencia, a suscribir el siguiente **ACUERDO DE CONFIDENCIALIDAD**.

ESTIPULACIONES

PRIMERA.- En virtud del presente acuerdo, el prestador del servicio se compromete a que cualquier información propiedad de la entidad prestataria a la que tenga acceso como consecuencia de la prestación del servicio de **……**.,tendrá la consideración de información confidencial y será tratada de acuerdo con lo establecido en el presente documento.
SEGUNDA.- A los efectos del presente acuerdo, se considera información propiedad de la entidad prestataria toda aquella que, dentro de las instalaciones de la empresa, esté contenida en papeles, libros, cuentas, grabaciones, programas de ordenador, procedimientos, documentos de todo tipo o tecnología, con independencia del soporte que la contenga.
TERCERA.- La obligación de confidencialidad que deberá ser cumplida por el prestador de servicios comprende lo siguiente:

- Se prohíbe que el prestador de servicios acceda a la información propiedad de la entidad prestataria, siempre y cuando tal acceso no sea imprescindible para la realización de sus tareas.
- En el caso de que en la realización de las tareas que le son propias acceda a información propiedad de la entidad prestataria, no podrá destruirla ni revelarla a ninguna otra persona o entidad ni tampoco utilizarla con fines propios.
- Asimismo, tampoco podrá sacar de las instalaciones de la entidad prestataria ningún tipo de información cualquiera que sea el soporte que la contenga.

CUARTA.- La obligación de confidencialidad persistirá aún después de resuelto el contrato de prestación de servicios del que trae causa el presente acuerdo de confidencialidad, por un período indefinido.
QUINTA.- El incumplimiento de la obligación de confidencialidad plasmada en este documento, por parte del prestador de servicios, facultará a la entidad prestataria a reclamar por la vía legal que

estime más procedente, la indemnización de los daños y perjuicios ocasionados. Es obligación del prestador de servicios informar a los empleados que ejecuten el servicio contratado en las instalaciones del Responsable del Tratamiento sobre los términos del presente acuerdo, especialmente sobre el debido deber de confidencialidad.

SEXTA.- El presente Acuerdo de Confidencialidad se regirá por la Legislación Española, y cualquier disputa, controversia o conflicto en cuanto a la interpretación o ejecución del presente Acuerdo será sometido a la jurisdicción de los Tribunales de **Ibiza** con exclusión de cualquier otro que pudiera corresponder a las partes, al que en este momento renuncian.

SÉPTIMA.- Ambas partes se informan que los datos personales contenidos en el presente contrato y los proporcionados durante la relación negocial serán objeto de tratamiento por la otra parte, con la finalidad de llevar a cabo la gestión de la relación contractual generada con la firma del presente documento. Los datos podrán ser cedidos a la administración pública en los casos previstos por la ley y a las entidades bancarias necesarias para realizar dicha gestión. Sus datos serán conservados mientras se mantenga la relación mercantil o durante los plazos establecidos por la legislación fiscal. Este tratamiento de datos es imprescindible para la ejecución del presente contrato. El ejercicio de cualquiera de los derechos de protección de datos puede interponerse en las direcciones indicadas en el encabezamiento del presente contrato, indicando como referencia "Protección de datos". En cualquier situación, Ud. tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD).

- Marque esta casilla si desea recibir comunicaciones comerciales por parte del responsable del tratamiento.
- Marque esta casilla si ~~NO~~ desea recibir comunicaciones comerciales por parte del encargado del tratamiento.

Ud. puede oponerse libremente a recibir comunicaciones comerciales, sin que ello condicione la ejecución del contrato.

OCTAVA.- El presente acuerdo tiene una duración vinculada al del contrato principal.

Y para que así conste a los efectos oportunos, las partes contratantes proceden a rubricar este contrato en el lugar y fecha ut supra reseñado.

El Responsable del tratamiento **El Prestador del servicio**

ANEXO XVI. Notificación de brechas de seguridad

En el presente Anexo se recoge una plantilla con los datos que la empresa deberá completar en el formulario de notificación de brechas de seguridad de la AEPD: https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/procedimientoBrechaSeguridad.jsf

Los campos marcados con asterisco son campos obligatorios

FORMULARIO DE NOTIFICACIÓN DE BRECHAS DE SEGURIDAD			
Datos identificativos			
Datos de la notificación	* Tipo de notificación	☐ Completa	
		☐ Inicial	
		☐ Adicional	
	* Si el tipo de notificación es Adicional, indicar:	Referencia notificación previa	
		Fecha notificación previa	
Identificación del Delegado de Protección de Datos (DPD) o persona de contacto	* NIF / NIE		
	* Nombre		
	* Apellidos		
	* Cargo		
	* Dirección		
	* Localidad		
	* País		
	* Código postal		
	* Provincia		
	Teléfono		
	Correo electrónico		
Identificación del responsable del tratamiento	* Nombre de la organización		
	* Tipo de organización	☐ Pública	
		☐ Privada	
	* NIF		
	* Si la dirección es distinta del DPD o persona de	* Dirección	
		* Localidad	

FORMULARIO DE NOTIFICACIÓN DE BRECHAS DE SEGURIDAD			
Datos identificativos			
	contacto, indicar:	* País	
		Código postal	
		* Provincia	
		Teléfono	
		Correo electrónico	
Identificación del encargado del tratamiento	* Si hay otra organización implicada en el incidente, indicar:	* Nombre de la organización	
		* Tipo de organización	☐ Pública
			☐ Privada
		* NIF	
		* Dirección	
		* País	
		* Código postal	
		* Provincia	
		* Localidad	
		Teléfono	
		Correo electrónico	
Información temporal de la brecha	* Fecha de detección de la brecha		☐ Exacta
			☐ Estimada
	* Medios de detección de la brecha		
	* Justificación de notificación tardía (pasadas 72 horas desde la detección)		
	* Fecha inicio de la brecha		☐ Exacta
			☐ Estimada
	* ¿Esta resuelta la brecha?	☐ Sí	
		☐ No	

FORMULARIO DE NOTIFICACIÓN DE BRECHAS DE SEGURIDAD			
Datos identificativos			
	* Si la brecha está resuelta, indicar la fecha de resolución		☐ Exacta
			☐ Estimada
Sobre la brecha	* Resumen del incidente		
	* Tipología	☐ Brecha de confidencialidad (acceso no autorizado)	
		☐ Brecha de integridad (modificación no autorizada)	
		☐ Brecha de disponibilidad (desaparición o pérdida)	
	* Medio por el que se ha materializado la brecha	☐ Dispositivo perdido o robado	
		☐ Documentación perdida, robada o depositada en localización insegura	
		☐ Correo perdido o abierto	
		☐ Hacking	
		☐ Malware (e.j. ransomware)	
		☐ Phising	
		☐ Eliminación incorrecta de datos personales en formato papel	
		☐ Datos personales residuales en dispositivos obsoletos	
		☐ Datos personales mostrados al individuo incorrecto	
		☐ Publicación no intencionada	
		☐ Revelación verbal no autorizada de datos personales	
		☐ Datos personales enviados por error	
		☐ Otros medios	
	* Contexto	☐ Interna (acción no intencionada)	
		☐ Interna (acción intencionada)	

FORMULARIO DE NOTIFICACIÓN DE BRECHAS DE SEGURIDAD		
Datos identificativos		
		☐ Externa (acción no intencionada)
		☐ Externa (acción intencionada)
		☐ Otros contextos
	* Medidas preventivas aplicadas antes de la brecha	
Información suplementaria		
Sobre los datos afectados	* Categoría de los datos afectados	☐ Datos básicos (nombre, apellidos, fecha de nacimiento)
		☐ Sobre condenas e infracciones penales
		☐ Datos económicos o financieros
		☐ Datos de localización
		☐ DNI, NIE y/o Pasaporte
		☐ Credenciales de acceso o identificación
		☐ Datos de contacto
		☐ Datos de Perfiles
		☐ Otros
	* Categorías especiales de datos	☐ Sobre la religión o creencia
		☐ Todavía desconocidos
		☐ Genéticos
		☐ Sobre la vida sexual
		☐ Sobre el origen racial o étnico
		☐ De salud
		☐ Sobre la afiliación sindical
		☐ Sobre la opinión política
		☐ Biométricos
		☐ Otros
	* Número aproximado de registros de datos	

FORMULARIO DE NOTIFICACIÓN DE BRECHAS DE SEGURIDAD		
Datos identificativos		
	personales afectados	
Sobre los sujetos afectados	* Perfil de los sujetos afectados	☐ Clientes
		☐ Estudiantes
		☐ Usuarios
		☐ Pacientes
		☐ Empleados
		☐ Suscriptores
		☐ Menores
		☐ Otros
	* Número aproximado de personas afectadas	
Posibles consecuencias	Brecha de confidencialidad	☐ Divulgación a terceros/difusión en internet
		☐ Enriquecimiento de otras bases de datos
		☐ Los datos pueden ser explotados con otros fines
		☐ Otros
	* Naturaleza del impacto potencial sobre los sujetos	☐ Perdida de control sobre sus datos personales
		☐ Usurpación de identidad
		☐ Reidentificación no autorizada
		☐ Limitación de sus derechos
		☐ Fraude
		☐ Perdida de confidencialidad de datos afectados por secreto profesional
		☐ Discriminación
		☐ Financiero
		☐ Daños a la reputación
		☐ Otros

<table>
<tr><th colspan="4">FORMULARIO DE NOTIFICACIÓN DE BRECHAS DE SEGURIDAD</th></tr>
<tr><td colspan="4">Datos identificativos</td></tr>
<tr><td rowspan="5"></td><td rowspan="4">* Severidad de las consecuencias para los individuos</td><td colspan="2">☐ Baja</td></tr>
<tr><td colspan="2">☐ Media</td></tr>
<tr><td colspan="2">☐ Alta</td></tr>
<tr><td colspan="2">☐ Muy alta</td></tr>
<tr><td>* Medidas tomadas para solucionar la brecha y minimizar el impacto sobre los afectados</td><td colspan="2"></td></tr>
<tr><td rowspan="10">Comunicación a los interesados</td><td rowspan="4">¿Se ha comunicado la brecha a los interesados?</td><td colspan="2">☐ Sí</td></tr>
<tr><td colspan="2">☐ No, pero serán informados</td></tr>
<tr><td colspan="2">☐ No serán informados</td></tr>
<tr><td colspan="2">☐ Pendiente de decidir</td></tr>
<tr><td rowspan="4">* Si se ha comunicado la brecha a los interesados, indicar:</td><td>Fecha en la que se informó</td><td></td></tr>
<tr><td>Número de sujetos informados</td><td></td></tr>
<tr><td>Medios o herramientas de comunicación</td><td></td></tr>
<tr><td colspan="2">Adjuntar el contenido de la comunicación enviada a los interesados</td></tr>
<tr><td rowspan="2">* Si todavía no se ha comunicado la brecha a los interesados, pero serán informados, indicar:</td><td colspan="2">☐ La fecha en la que se informará a los interesados no es conocida</td></tr>
<tr><td>☐ Fecha en al que se informará</td><td></td></tr>
<tr><td>* Si los interesados no serán informados, indicar:</td><td>Justificación para no informar</td><td></td></tr>
<tr><td colspan="4">Posibles cuestiones de carácter transfronterizo</td></tr>
<tr><td rowspan="4">Implicaciones transfronterizas</td><td rowspan="4">Si hay sujetos de otros Estados miembros de la UE afectados por la brecha, marcar los Estados que puedan estar afectados (A)</td><td>A</td><td>N</td></tr>
<tr><td>☐ Alemania</td><td>☐ Alemania</td></tr>
<tr><td>☐ Austria</td><td>☐ Austria</td></tr>
<tr><td>☐ Bélgica</td><td>☐ Bélgica</td></tr>
</table>

FORMULARIO DE NOTIFICACIÓN DE BRECHAS DE SEGURIDAD			
Datos identificativos			
	y aquellos a los que haya notificado (N) la misma brecha de seguridad	☐ Bulgaria	☐ Bulgaria
		☐ Chipre	☐ Chipre
		☐ Croacia	☐ Croacia
		☐ Dinamarca	☐ Dinamarca
		☐ Francia	☐ Francia
		☐ Eslovaquia	☐ Eslovaquia
		☐ Eslovenia	☐ Eslovenia
		☐ Estonia	☐ Estonia
		☐ Finlandia	☐ Finlandia
		☐ Reino Unido	☐ Reino Unido
		☐ Grecia	☐ Grecia
		☐ Hungría	☐ Hungría
		☐ Irlanda	☐ Irlanda
		☐ Italia	☐ Italia
		☐ Letonia	☐ Letonia
		☐ Lituania	☐ Lituania
		☐ Luxemburgo	☐ Luxemburgo
		☐ Malta	☐ Malta
		☐ Países Bajos	☐ Países Bajos
		☐ Polonia	☐ Polonia
		☐ Portugal	☐ Portugal
		☐ República Checa	☐ República Checa
		☐ Rumanía	☐ Rumanía
		☐ Suecia	☐ Suecia
Adjuntar documentos (tamaño máximo del archivo: 2 MB; tipo de documento: PDF, DOC y DOCX; máximo de ficheros a adjuntar: 5; tamaño máximo total a adjuntar: 4 MB)			

ANEXO XVII. Formulario de Verificación

Marcar con una X en caso de encontrarse en el supuesto descrito:

Evaluación de la necesidad de realizar una EIPD	
No es obligatorio realizar una EIPD si realiza algunos de los siguientes tratamientos de datos:	
	Tratamientos incluidos en la lista publicada por la AEPD (aún no publicada)
	Corresponsables de tratamiento
	Tratamientos sucesivos o adicionales
	Gran escala
	Uso de una base legal específica
	Interfaces de dispositivos electrónicos personales no protegidos contra una lista no autorizada
	Sistemas de información distribuidos territorialmente o transfronterizos
Es obligatorio realizar una EIPD si realiza alguno de los siguientes tratamientos de datos:	
	Tratamientos incluidos en la lista publicada por la AEPD (aún no publicada)
	Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas
	Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que afecten significativamente a las personas físicas
	Tratamiento a gran escala de categorías especiales de datos: origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos o biométricos, salud, vida sexual, orientación sexual
	Tratamiento a gran escala de datos personales relativos a condenas e infracciones penales
	Observación sistemática a gran escala de una zona de acceso público
Puede ser obligatorio realizar una EIPD si trata datos de las siguientes categorías:	
	Datos biométricos dirigidos a identificar de manera unívoca a una persona
	Datos genéticos
	Datos de localización
	Tratamiento para fines científicos o históricos, sin consentimiento
	No poder notificar a los destinatarios de los datos un derecho de rectificación o supresión
	No informar al interesado por ser imposible o exija un esfuerzo desproporcionado o porque informar imposibilite u obstaculice gravemente el logro de los objetivos del tratamiento
	No informar al interesado porque los datos personales deben seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por ley (incluida una obligación de secreto de naturaleza estatutaria)
	Tratamientos que usen nuevas o innovadoras tecnologías
	Migración de datos desde un sistema hasta al menos otro diferente
	Tratamiento de datos de salud realizado con la ayuda de un implante
	Tratamiento de colectivos vulnerables
	Evaluación sistemática y exhaustiva
Puede ser obligatorio realizar una EIPD si pertenece a alguno de los siguientes sectores:	
	Sanidad
	Solvencia patrimonial y crédito
	Generación y uso de perfiles
	Actividades políticas, sindicales o religiosas

	Servicios de telecomunicaciones
	Seguros
	Entidades bancarias y financieras
	Actividades de servicios sociales
	Publicidad
	Partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical
	Prestador de servicios de explotación de redes públicas o servicios de comunicación electrónica (proveedor de servicios de internet)
	Videovigilancia masiva (Videovigilancia de grandes infraestructuras como estaciones de ferrocarril o centros comerciales)
Puede ser obligatorio realizar una EIPD si realiza alguno de los siguientes tratamiento de datos	
	Tratamientos de datos sensibles de forma no meramente incidental o accesoria: origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, salud, vida sexual u orientación sexual
	Tratamientos que datos relativos a condenas o infracciones penales de forma no meramente incidental o accesoria
	Elaborar perfiles personales (referidos a rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, solvencia financiera, localización o movimientos), o predecir comportamientos, hábitos, preferencias, gustos, intereses, etc., de personas identificadas o identificables
	Tomar decisiones automatizadas con efectos jurídicos sobre las personas o que puedan afectarles significativamente
	Realizar una vigilancia sistemática de personas físicas, de acciones realizadas por las mismas, de sus datos personales o de cualquier otro tipo de información obtenida de personas físicas
	Cruzar información de diferentes fuentes u orígenes de datos personales que de alguna manera hagan más rica la información de la que se dispone inicialmente
	Tratar datos de personas en situación de vulneración o de desequilibrio en relación al responsable del tratamiento (menores (especialmente sin son menores de 14 años), discapacitados, trabajadores, estudiantes, pacientes, etc.)
	Tratar datos a gran escala
	Realizar TID fuera de la UE; o a países que no sean Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay y Nueva Zelanda; o a entidades estadounidenses adheridas al Escudo de Privacidad EU-US
	Tratar los datos de forma que exista un riesgo elevado de accesos no autorizados por parte de terceros
	Hacer publicidad y prospección comercial masiva a potenciales clientes
	El tratamiento en sí mismo puede privar a los interesados de sus derechos y libertades o puede impedirles ejercer el control sobres sus datos o el ejercicio un derecho o utilizar un servicio o un contrato
	El tratamiento puede provocar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados
	Otros tratamientos que pudieran tener relevancia o si están previstos en algún código de conducta o en algún estándar definido por un esquema de certificación.

Completar con la información solicitada:

Teniendo en cuenta las medidas organizativas o técnicas implantadas en la Sociedad para reducir los riesgos que puedan afectar a los derechos y libertades de los individuos, indicar, del 1 al 5 (donde 1 es riesgo bajo y 5 es riesgo alto), el nivel global del riesgo en cuanto a:	
	Probabilidad de que alguno de los tratamientos de datos realizados por la Sociedad pueda suponer un riesgo para los derechos y libertades de los individuos
	Gravedad del riesgo de este tratamiento sobre los derechos y libertades de los individuos en caso de que dicho riesgo se materialice

ANEXO XVIII. Plazos indicativos 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. IBIZA NURSE SERVICE S.L 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
	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

ACTIVIDAD DE TRATAMIENTO	DOCUMENTO	CONSERVACIÓN	ORIGEN DEL CRITERIO
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 10 años (prescripción delito)	Ley 16/2002 (modificada por la Ley 5/2013) y Código Penal
	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
Seguros	Pólizas de seguros	6 años (regla general) 2 años (seguro de daños) 5 años (seguros personales) 10 años (seguro de vida)	Código de Comercio, Ley de Contrato de Seguro, Ley de lucha contra el blanqueo de dinero y la financiación del terrorismo y Código Civil.
Jurídico	Documentos Propiedad Intelectual e Industrial	5 años	Ley de Patentes, Ley de Marcas, Ley de Propiedad Intelectual, Ley de Protección Jurídica del Diseño

ACTIVIDAD DE TRATAMIENTO	DOCUMENTO	CONSERVACIÓN	ORIGEN DEL CRITERIO
	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 XIX. Página web. Cláusula informativa y política de cookies

(La siguiente cláusula ha de estar permanentemente visible en toda aquella página web o apartado de página web donde se recojan datos personales tales como formularios o introducción de datos para envío de Newsletters. Se aconseja implementar un Checkbox en el que el usuario marque que ha leído y acepta expresamente la presente cláusula)

De conformidad con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales relativo a la Protección de las Personas físicas, y conforme a disposiciones reglamentarias reflejadas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, le informamos que sus datos personales serán tratados por **IBIZA NURSE SERVICE S.L**, con el fin de gestionar su solicitud y el mantenimiento de las relaciones profesionales y comerciales con usted. Sus datos no serán cedidos a terceros. Este tratamiento de datos es necesario para atender su solicitud. Sus datos serán conservados hasta que Usted se dé de baja del servicio y/o pasado un tiempo prudencial desde que atendamos su solicitud. Ud. puede ejercer sus derechos de acceso, rectificación, supresión, portabilidad y limitación del tratamiento de sus datos dirigiéndose a **IBIZA NURSE SERVICE S.L** C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares) o a **info@ibizanurseservice.com**, 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).

Política de Privacidad

De conformidad con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales relativo a la Protección de las Personas físicas y el Reglamento (UE) 2016/679 de Parlamento Europeo y del Consejo de 27 de abril de 2016, **IBIZA NURSE SERVICE S.L** expone en la siguiente tabla la información básica sobre el tratamiento de datos bajo su responsabilidad:

Responsable del tratamiento	**IBIZA NURSE SERVICE S.L**	Datos de contacto: Dirección: C/ Pais Vasco Nº5 201; 07800 Ibiza (Islas Baleares) Teléfono: Email: **info@ibizanurseservice.com**
Finalidad	Gestión de las solicitudes recibidas	Los datos que nos facilite a través del formulario de contacto habilitado en nuestra web serán tratados de manera confidencial, con la única finalidad de gestionar su consulta. En el caso de que los datos recogidos se utilizasen para una finalidad distinta para la cual hubiesen sido recabados o recogidos se requerirá el consentimiento previo de los interesados. Los datos personales proporcionados se conservarán durante el plazo estrictamente necesario para contestar a su solicitud.
Legitimación	Consentimiento informado del interesado	
Destinatarios	Sus datos personales serán tratados únicamente por **IBIZA NURSE SERVICE S.L** y en ningún caso serán cedidos a terceros.	
Derechos	Acceso, Rectificación, Supresión, Oposición, Portabilidad de los datos, Limitación del tratamiento	Podrá ejercitar los derechos reconocidos en la LOPD-GDD y en el RGPD dirigiéndose a **IBIZA NURSE SERVICE S.L** a través de correo postal o correo electrónico, acompañando copia del documento que acredite debidamente su identidad. En cualquier situación, Ud. tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD).
Información adicional	**IBIZA NURSE SERVICE S.L** se reserva el derecho a modificar su política de protección de datos en el supuesto de que exista un cambio de la legislación vigente, doctrina jurisprudencial o por criterios empresariales. Si se introdujese algún cambio en esta política, el nuevo texto se publicará en esta misma dirección.	

Política de Cookies

1. ¿Qué son las cookies?

Una cookie es un pequeño archivo que se almacena en el ordenador, móvil o tablet de los usuarios al acceder a determinadas páginas web, aplicación o plataforma y que permiten a éstas reconocer a sus usuarios.

Las cookies actualmente son esenciales para el funcionamiento de internet, aportando innumerables ventajas en la prestación de servicios interactivos, facilitándole la navegación y su usabilidad.

Las cookies ayudan a adaptar las webs, aplicaciones o plataformas a sus necesidades personales.

Las cookies no pueden dañar su equipo. En cambio, el que estén activadas pueden ayudar a identificar y resolver errores, así como a mejorar la navegabilidad del usuario.

Las cookies permiten, entre otras cosas, almacenar y recuperar información sobre las preferencias de navegación de un usuario o de su equipo.

Este sitio web, aplicación o plataforma utiliza cookies y/o tecnologías similares que almacenan y recuperan información cuando navegas. En general, estas tecnologías pueden servir para finalidades muy diversas, como, por ejemplo, reconocerte como usuario, obtener información sobre tus hábitos de navegación, o personalizar la forma en que se muestra el contenido.

Los usos concretos que hacemos de estas tecnologías se describen a continuación.

2. ¿Qué cookies utilizamos?

En utilizamos cookies, logs, enlaces y otras tecnologías para almacenar las preferencias del usuario con el fin de mejorar la calidad de nuestros servicios, asegurar el funcionamiento técnico tanto del portal, aplicación o plataforma como de las transacciones realizadas, medir la audiencia de la web y desarrollar nuevas y mejores prestaciones, productos y servicios ofertados.

Propietario de las cookies:

- Utilizamos **cookies propias** que enviamos al equipo terminal del usuario desde un equipo o dominio gestionado por nosotros y desde el que se presta el servicio solicitado por el usuario.

- Utilizamos **cookies de terceros** (por ejemplo, cookies de Facebook, Google, Twitter…) usadas por empresas externas, redes sociales o por complementos externos de contenido (como, por ejemplo, Google Maps). Son enviadas al equipo terminal del usuario desde un equipo o dominio de una entidad tercera que trata los datos obtenidos través de las cookies.

Uso de las cookies:

- Utilizamos **cookies técnicas** que son estrictamente necesarias para que el usuario acceda y navegue en **.**

Son aquellas que permiten al usuario la navegación a través de una página web, plataforma o aplicación y la utilización de las diferentes opciones o servicios que en ella existan, incluyendo aquellas que se utilizan para permitir la gestión y operativa de la página web y habilitar sus funciones y servicios, como, por ejemplo, controlar el tráfico y la comunicación de datos identificar la sesión, acceder a partes de acceso restringido, recordar los elementos que integran un pedido, realizar el proceso de compra de un pedido, gestionar el pago, controlar el fraude vinculado a la seguridad del servicio, realizar la solicitud de inscripción o participación en un evento, contar visitas a efectos de la facturación de licencias del software con el que funciona el servicio (sitio web, plataforma o aplicación), utilizar elementos de seguridad durante la navegación, almacenar contenidos para la difusión de vídeos o sonido, habilitar contenidos dinámicos (por ejemplo, animación de carga de un texto o imagen) o compartir contenidos a través de redes sociales.

También pertenecen a esta categoría, por su naturaleza técnica, aquellas cookies que permiten la gestión, de la forma más eficaz posible, de los espacios publicitarios que, como un elemento más de diseño o "maquetación" del servicio ofrecido al usuario, el editor haya incluido en una página web, aplicación o plataforma en base a criterios como el contenido editado, sin que se recopile información de los usuarios con fines distintos, como puede ser personalizar ese contenido publicitario u otros contenidos.

Estas cookies no requieren el consentimiento informado del usuario.

- Utilizamos **cookies de preferencias o personalización** que son aquellas que, tratadas por nosotros o por terceros, nos permiten recordar información para que el usuario acceda al servicio con determinadas características que pueden diferenciar su experiencia de la de otros usuarios.
  Por ejemplo, el idioma, el número de resultados a mostrar cuando el usuario realiza una búsqueda, el aspecto o contenido del servicio en función del tipo de navegador a través del cual el usuario accede al servicio o de la región desde la que accede al servicio, etc.

  Estas cookies pueden requerir el consentimiento informado del usuario, salvo que sea el propio usuario quien elige esas características (por ejemplo, si selecciona el idioma de un sitio web clicando en el icono de la bandera del país correspondiente).

- Utilizamos **cookies de análisis o medición** que son aquellas que, tratadas por nosotros o por terceros, nos permiten el seguimiento y análisis del comportamiento de los usuarios de los sitios web a los que están vinculadas, incluida la cuantificación de los impactos de los anuncios.
  La información recogida mediante este tipo de cookies se utiliza en la medición de la actividad de los sitios web, aplicación o plataforma, con el fin de introducir mejoras en los productos o servicios ofertados en función del análisis de los datos de uso que hacen los usuarios del servicio.

  Estas cookies requieren el consentimiento informado del usuario.

- Utilizamos **cookies de publicidad comportamental** que son aquellas que, tratadas por nosotros o por terceros, almacenan información del comportamiento de los usuarios obtenida a través de la observación continuada de sus hábitos de navegación, lo que permite desarrollar un perfil específico de navegación de los usuarios para mostrarles publicidad en función del mismo.

Estas cookies requieren el consentimiento informado del usuario.

Tiempo de conservación de las cookies:

- Utilizamos **cookies de sesión** que son cookies diseñadas para recabar y almacenar datos mientras el usuario accede a una página web. Se suelen emplear para almacenar información que solo interesa conservar para la prestación del servicio solicitado por el usuario en una sola ocasión (por ejemplo, una lista de productos adquiridos) y desaparecen al terminar la sesión.

- Utilizamos **cookies persistentes** que son aquellas en las que los datos siguen almacenados en el terminal y pueden ser accedidos y tratados durante un periodo definido por el responsable de la cookie, y que puede ir de unos minutos a varios años.

Este tipo de información obtenida a través de las cookies no será comunicado a terceros, ni utilizado para comunicaciones no solicitadas.

3. ¿Cómo pueden nuestros usuarios gestionar las cookies que utilizamos?

Los usuarios de pueden gestionar las cookies y, por lo tanto, rechazarlas de forma unitaria o en su totalidad, en el **Panel de Configuración.**

Si se desactivan o rechazan las cookies, puede ocurrir que algunas de las funciones y/o servicios no funcionen adecuadamente.

El portal, aplicación o plataforma no ejerce control sobre los sitios web mostrados como resultado de su búsqueda, enlaces o accesos desde nuestro directorio. Estos otros sitios web pueden colocar sus propias cookies o solicitarle información personal.

4. ¿Cómo pueden nuestros usuarios deshabilitar las cookies en los principales navegadores?

Normalmente es posible dejar de aceptar las cookies del navegador, o dejar de aceptar las cookies de un servicio en particular.

Todos los navegadores modernos permiten **cambiar la configuración de cookies**.

Estos ajustes normalmente se encuentran en las 'opciones' o 'Preferencias' del menú de su navegador.

Aunque puede variar ligeramente de una versión de navegador a otra, la configuración de la política de cookies para los navegadores más utilizados es la siguiente:

- **Internet Explorer:** Herramientas -> Opciones de Internet -> Privacidad -> Configuración.
- **Firefox:** Preferencias -> Privacidad y Seguridad
- **Chrome:** Preferencias -> Configuración -> Mostrar opciones avanzadas -> Privacidad y Seguridad
- **Safari:** Preferencias -> Privacidad.
- **Opera:** Configuración -> Privacidad y seguridad.

Para más información, puede consultar el soporte o la ayuda de su navegador o a través de los siguientes enlaces: Safari, Chrome, Firefox, Explorer, Opera.

Muchos navegadores permiten activar un modo privado mediante el cual las cookies se borran siempre después de su visita. Dependiendo de cada navegador este modo privado, puede tener diferentes nombres. A continuación, encontrará una lista de los navegadores más comunes y los diferentes nombres de este "modo privado":

- Internet Explorer 8 y superior - Navegación Privada
- Safari 2 y superior - Navegación Privada
- Opera 10.5 y superior - Navegación Privada
- FireFox 3.5 y superior - Navegación Privada
- Google Chrome 10 y superior – Incógnito

5. ¿Cómo puedo deshabilitar las cookies de terceros?

Tenga en cuenta que, si acepta las cookies de terceros, deberá eliminarlas desde las opciones del navegador o desde el sistema ofrecido por el propio tercero.

Si se desea conocer las condiciones de privacidad y uso de cookies de terceros, puede acceder las políticas de cookies de:

- Facebook: https://es-es.facebook.com/help/cookies
- Twitter: https://twitter.com/privacy
- Youtube: https://www.google.es/intl/es/policies/technologies/cookies/
- Linkedin: https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out?trk=microsites-frontend_legal_cookie-policy
- Google: https://www.google.es/intl/es/policies/technologies/cookies/

6. ¿Qué ocurre si no acepto las cookies de la web?

En caso de que el usuario no permita la instalación de cookies en su navegador es posible que no pueda acceder a alguna de las secciones de nuestro sitio web.

7. ¿Se realizan transferencias internacionales de mis datos?

Según los artículos 44 y siguientes del Reglamento Europeo de Protección de Datos (RGPD) serán legítimas las transferencias basadas en una decisión de adecuación de la Comisión Europea o en caso de existan garantías adecuadas mediante un instrumento jurídicamente vinculante y exigible entre autoridades y organismos públicos, o mediante normas corporativas vinculantes, o cláusulas tipo adoptadas o aprobadas por la Comisión, o mediante códigos de conducta o mecanismos de certificación. En caso contrario, será necesaria la autorización de la Autoridad de Control competente o, en su defecto, el consentimiento explícito del interesado u otro de los supuestos recogidos en el art. 49 RGPD.

Le informamos que **IBIZA NURSE SERVICE S.L** no realiza transferencias internacionales de sus datos o sí realiza transferencias internacionales de sus datos a _____, basado en (decisión de adecuación de la Comisión, cláusulas contractuales tipo, etc.), con la finalidad _____ o realiza transferencias internacionales de datos a _____, basado en el consentimiento explícito que el usuario nos otorga en el **Banner de Cookies**, con la finalidad _____.

En cuanto a las cookies de terceros, puedes informarte de las transferencias a terceros países que, en su caso, realizan los terceros identificados en esta política de cookies en sus correspondientes políticas (ver los enlaces facilitados anteriormente).

8. ¿Se elabora un perfil de mi navegación y se toman decisiones automatizadas que puedan afectarme jurídica o significativamente?

Le informamos que **IBIZA NURSE SERVICE S.L** no realiza elaboración de perfiles de su navegación que lleven a la toma de decisiones automatizadas que puedan afectarle jurídica o significativamente o sí realiza elaboración de perfiles de su navegación y se toman decisiones automatizadas que puedan afectarle jurídica o significativamente. (En este caso, deberá describirse la lógica utilizada para la toma de decisiones automatizada con efectos jurídicos para los usuarios o que les afecten significativamente, así como la importancia y las consecuencias previstas de dicho tratamiento para el usuario).

9. ¿Se realiza un tratamiento de mis datos sensibles?

Le informamos que **IBIZA NURSE SERVICE S.L** no realiza tratamientos de datos sensibles o sí realiza tratamientos de los siguientes datos sensibles: _____, con la finalidad _____, basado en el consentimiento explícito que el usuario nos otorga en el **Banner de Cookies**.

10. Más información

Para más información sobre cookies y sus derechos como usuario puede consultar la Guía sobre el uso de cookies elaborada por la Agencia Española de Protección de Datos (AEPD)

Para más información sobre el tratamiento de sus datos personales puede acceder a la **Política de Privacidad** de **IBIZA NURSE SERVICE S.L**

Banner de cookies

Esta información debe facilitarse a los usuarios antes del uso de las cookies, incluida, en su caso, su instalación. El banner deberá mantenerse hasta que el usuario realice la acción requerida para la obtención del consentimiento o su rechazo.

A continuación, se ofrecen varias opciones de texto a incluir en el banner de cookies.

El contenido de estos textos deberá modificarse según a quién vaya dirigido el aviso y el tipo de cookies utilizadas

Cookies

Si tienes menos de 14 años, pide a tu padre, madre o tutor que lea este mensaje. Indicar año de nacimiento: _____ (este dato no se almacenará, se utilizará sólo para comprobar el consentimiento).
En utilizamos cookies, propias y de terceros, **de personalización** para mejorar la calidad del producto o servicio ofrecido; **de análisis** para medir la audiencia y analizar el comportamiento de los usuarios; y **de publicidad comportamental** para ofrecer publicidad personalizada a partir de los hábitos de navegación de los usuarios (por ejemplo, páginas visitadas).
Puede obtener más información en nuestra **Política de Cookies**.
(Ud. o Tu padre, madre o tutor) puede aceptar todas las cookies pulsando el botón "Aceptar Cookies" o rechazarlas pulsando el botón "Rechazar Cookies". También puede gestionar estas cookies y, por lo tanto, aceptarlas o rechazarlas de forma unitaria o en su totalidad, en el **Panel de Configuración.**

Aceptar Cookies **Rechazar Cookies**

☐ Marque esta casilla si consiente la transferencia internacional de sus datos a _____, con la finalidad de _____. Le informamos que esta transferencia se realiza sin un nivel adecuado de protección o de garantías adecuadas para proteger sus datos personales.
☐ Marque esta casilla si consiente la elaboración de un perfil de su navegación y la toma de decisiones automatizadas que puedan afectarle jurídica o significativamente.
☐ Marque esta casilla si consiente que, para dichos fines de análisis y de elaboración de perfiles a partir de sus hábitos de navegación para mostrarte publicidad personalizada, utilicemos categorías especiales de datos (mencionar aquí las categorías especiales de datos que se utilicen en cada caso)

Cookies

Si tienes menos de 14 años, pide a tu padre, madre o tutor que lea este mensaje. Indicar año de nacimiento: _____ (este dato no se almacenará, se utilizará sólo para comprobar el consentimiento).
En utilizamos cookies, propias y de terceros, **de personalización** para mejorar la calidad del producto o servicio ofrecido; **de análisis** para medir la audiencia y analizar el comportamiento de los usuarios; y **de publicidad comportamental** para ofrecer publicidad personalizada a partir de los hábitos de navegación de los usuarios (por ejemplo, páginas visitadas).
Puede obtener más información en nuestra **Política de Cookies**.
(Ud. o Tu padre, madre o tutor) puede aceptar todas las cookies pulsando el botón "Aceptar Cookies" o configurarlas o rechazar su uso en el **Panel de Configuración.**

Aceptar Cookies

☐ Marque esta casilla si consiente la transferencia internacional de sus datos a _____, con la finalidad de _____. Le informamos que esta transferencia se realiza sin un nivel adecuado de protección o de garantías adecuadas para proteger sus datos personales.
☐ Marque esta casilla si consiente la elaboración de un perfil de su navegación y la toma de decisiones automatizadas que puedan afectarle jurídica o significativamente.
☐ Marque esta casilla si consiente que, para dichos fines de análisis y de elaboración de perfiles a partir de sus hábitos de navegación para mostrarte publicidad personalizada, utilicemos categorías especiales de datos (mencionar aquí las categorías especiales de datos que se utilicen en cada caso)

Cookies

Si tienes menos de 14 años, pide a tu padre, madre o tutor que lea este mensaje. Indicar año de nacimiento: _____ (este dato no se almacenará, se utilizará sólo para comprobar el consentimiento).
En utilizamos cookies, propias y de terceros, **de personalización** para mejorar la calidad del producto o servicio ofrecido; **de análisis** para medir la audiencia y analizar el comportamiento de los usuarios; y **de publicidad comportamental** para ofrecer publicidad personalizada a partir de los hábitos de navegación de los usuarios (por ejemplo, páginas visitadas).
Puede obtener más información en nuestra **Política de Cookies**.
(Ud. o Tu padre, madre o tutor) puede aceptar todas las cookies pulsando el botón "Aceptar Cookies" o configurarlas o rechazar su uso pulsando el botón "Configurar Cookies"

Aceptar Cookies **Configurar Cookies**

☐ Marque esta casilla si consiente la transferencia internacional de sus datos a _____, con la finalidad de _____. Le informamos que esta transferencia se realiza sin un nivel adecuado de protección o de garantías adecuadas para proteger sus datos personales.
☐ Marque esta casilla si consiente la elaboración de un perfil de su navegación y la toma de decisiones automatizadas que puedan afectarle jurídica o significativamente.
☐ Marque esta casilla si consiente que, para dichos fines de análisis y de elaboración de perfiles a partir de sus hábitos de navegación para mostrarte publicidad personalizada, utilicemos categorías especiales de datos (mencionar aquí las categorías especiales de datos que se utilicen en cada caso)

Panel de Configuración de Cookies

Utilizamos **cookies técnicas** necesarias para el funcionamiento y la prestación de los servicios ofrecidos.

Respecto al resto de cookies, a través del presente **Panel de Configuración**, puede aceptar o rechazarlas en su totalidad o puede seleccionar qué tipo de cookies quiere aceptar y cuáles quiere rechazar.

Para obtener más información, acceda a nuestra **Política de Cookies**.

- **Acepto todas las cookies**
- **Rechazo todas las cookies**

Selección de cookies que el usuario puede aceptar o rechazar:

- **Cookies de preferencias o personalización**
  - Propias – indicar plazo de conservación
  - Terceros (puede ser un desplegable)
    - Google – indicar plazo de conservación
    - Facebook – indicar plazo de conservación
    - Twitter – indicar plazo de conservación
    - Doubleclick – indicar plazo de conservación
    - etc.
- **Cookies de análisis o medición**
  - Propias – indicar plazo de conservación
  - Terceros (puede ser un desplegable)
    - Google – indicar plazo de conservación
    - Facebook – indicar plazo de conservación
    - Twitter – indicar plazo de conservación
    - Doubleclick – indicar plazo de conservación
    - etc.
- **Cookies de publicidad comportamental**
  - Propias – indicar plazo de conservación
  - Terceros (puede ser un desplegable)
    - Google – indicar plazo de conservación
    - Facebook – indicar plazo de conservación
    - Twitter – indicar plazo de conservación
    - Doubleclick – indicar plazo de conservación
    - etc.
- **Otro tipo de cookies**
  - Propias – indicar plazo de conservación
  - Terceros (puede ser un desplegable)
    - Google – indicar plazo de conservación
    - Facebook – indicar plazo de conservación
    - Twitter – indicar plazo de conservación
    - Doubleclick – indicar plazo de conservación
    - etc.

Tenga en cuenta que, si acepta las cookies de terceros, deberá eliminarlas desde las opciones del navegador o desde el sistema ofrecido por el propio tercero.

Al pulsar "Guardar configuración", se guardará la selección de cookies que haya realizado. Si no ha seleccionado ninguna opción, pulsar este botón equivaldrá a rechazar todas las cookies.

Guardar configuración

Transferencias internacionales de datos (incluir este punto únicamente en el caso de que se pretenda realizar una transferencia sin nivel de adecuación o de garantías apropiadas, ya que será necesario el consentimiento explícito del usuario)

Si Usted ha marcado la casilla correspondiente del Banner de Cookies, sus datos, recogidos a través de las cookies _____, serán transferidos a _____, con la finalidad de _____. Le informamos que esta transferencia se realiza sin un nivel adecuado de protección o de garantías adecuadas para proteger sus datos personales.

En cuanto a las cookies de terceros, puedes informarte de las transferencias a terceros países que, en su caso, realizan los terceros identificados en esta política de cookies en sus correspondientes políticas (ver los enlaces facilitados más adelante).

Elaboración de perfiles y tomas de decisiones automatizadas (incluir este punto únicamente en el caso de que se pretenda realizar elaboraciones de perfiles y toma de decisiones automatizadas que puedan afectar a los usuarios jurídica o significativamente, ya que será necesario el consentimiento explícito del usuario)

Si Usted ha marcado la casilla correspondiente del Banner de Cookies, procederemos a la elaboración de un perfil de su navegación y a la toma de decisiones automatizadas que puedan afectarle jurídica o significativamente. Le informamos que tiene derecho a obtener intervención humana, a expresar su punto de vista y a impugnar la decisión.

Tratamiento de datos sensibles (incluir este punto únicamente en el caso de que se pretenda realizar un tratamiento de datos sensibles, ya que será necesario el consentimiento explícito del usuario)

Si Usted ha marcado la casilla correspondiente del Banner de Cookies, procederemos al tratamiento de los siguientes datos sensibles: _____, con la finalidad de _____.

Cómo deshabilitar las cookies en los principales navegadores

Puede usted permitir o bloquear las cookies, así como borrar sus datos de navegación (incluidas las cookies) desde el navegador que usted utiliza. Consulte las opciones e instrucciones que ofrece su navegador para ello. Tenga en cuenta que, si acepta las cookies de terceros, deberá eliminarlas desde las opciones del navegador.

Aunque puede variar ligeramente de una versión de navegador a otra, la configuración de la política de cookies para los navegadores más utilizados es la siguiente:

- **Internet Explorer:** Herramientas -> Opciones de Internet -> Privacidad -> Configuración
- **Firefox:** Preferencias -> Privacidad y Seguridad
- **Chrome:** Preferencias -> Configuración -> Mostrar opciones avanzadas -> Privacidad y Seguridad
- **Safari:** Preferencias -> Privacidad
- **Opera:** Configuración -> Privacidad y seguridad

Para más información, puede consultar el soporte o la ayuda de su navegador o a través de los siguientes enlaces: Safari, Chrome, Firefox, Explorer, Opera.

Muchos navegadores permiten activar un modo privado mediante el cual las cookies se borran siempre después de su visita. Dependiendo de cada navegador este modo privado, puede tener diferentes nombres. A continuación, encontrará una lista de los navegadores más comunes y los diferentes nombres de este “modo privado”:

- Internet Explorer 8 y superior - Navegación Privada
- Safari 2 y superior - Navegación Privada
- Opera 10.5 y superior - Navegación Privada
- FireFox 3.5 y superior - Navegación Privada
- Google Chrome 10 y superior - Incógnito

Cómo deshabilitar las cookies de terceros

Si se desea conocer las condiciones de privacidad y uso de cookies de terceros, puede acceder las políticas de cookies de:

- Facebook: https://es-es.facebook.com/help/cookies
- Twitter: https://twitter.com/privacy
- Youtube: https://www.google.es/intl/es/policies/technologies/cookies/
- Linkedin: https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out?trk=microsites-frontend_legal_cookie-policy
- Google: https://www.google.es/intl/es/policies/technologies/cookies/

Para obtener más información, acceda a nuestra **Política de Cookies**

ANEXO XX. Sello de calidad y Certificado RGPD / LOPD-GDD

- Aranzadi pone a su disposición un **sello de calidad RGPD**, privado, con una fecha de validez de un año, que corrobora el esfuerzo y compromiso del profesional por implantar y mantener en vigor correctamente los procesos afectados por el nuevo Reglamento de Protección de Datos , contando con nuestra cobertura.
- **Sello de calidad** que podrá utilizar en su **documentación corporativa** y en su **propia Web**, representando para sus clientes, proveedores y usuarios en general, una **garantía de cumplimiento** de la ley en el tratamiento que el profesional realiza de los datos personales.
- Este distintivo posibilita que el profesional destacada con él pueda exhibir ante sus clientes y ante el mercado la calidad de sus servicios y sus sistemas de gestión, **resultando una muy efectiva muestra de su constante preocupación por alcanzar la excelencia profesional**. El sello ayudará a crear confianza en la seriedad y profesionalidad del profesional y en el cumplimiento de las leyes.

CERTIFICADO
RGPD / LOPD-GDD

ARANZADI

Certifica que el programa de cumplimiento de protección de datos es conforme a la normativa vigente de protección de datos y que la entidad está comprometida con el proceso de mejora continua que forma parte de dicho programa para poder cumplir y demostrar que cumple con el principio de responsabilidad proactiva exigido en el reglamento europeo de protección de datos.

IBIZA NURSE SERVICE S.L

La consultoría ha sido realizada 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)**

Este certificado es **válido hasta el 27 de abril de 2024**

Madrid, a 27 de abril de 2023