SandaS GRC
Privacidad

INFORME DE EVALUACIÓN DE IMPACTO EN MATERIA DE PROTECCIÓN DE DATOS

Hospital público de Gotan

ADAPTADO AL RGPD

14 de diciembre de 2025

Índice

1. Identificación del Proyecto

RESPONSABLE DEL TRATAMIENTO
Hospital público de Gotan
TÍTULO DE PROYECTO DE EIPD
Evaluación de Impacto en Protección de Datos (EIPD): Migración de Datos de Salud y Seguridad Pública al Cloud de Gotan
NÚMERO DE REGISTRO DE EIPD
EIPD-GOTHAM-HOSPITAL-001/2025
FECHA EIPD
11 de diciembre de 2025 - 11 de febrero de 2026
RESPONSABLE/S DEL PROYECTO
Alfred Pennyworth Cargo: Responsable de Seguridad Función: Secretario / Responsable Técnico de Riesgos ***Bruce Wayne*** Cargo: Delegado de Protecci?n de Datos (DPD) Función: Miembro Permanente / Asesor Jurídico y de Cumplimiento ***Tim Drake*** Cargo: Responsable de TI y Sistemas Función: Miembro / Representante Técnico de Infraestructura.

2. Análisis del motivo por el que se realiza la EIPD

LOS SIGUIENTES TRATAMIENTOS ESTÁN OBLIGADOS A REALIZAR LA EIPD
- HISTORIAL CLÍNICO Y GESTIÓN SANITARIA

3. Flujos de Datos Personales 11-12-2025

A continuación se muestra la información relativa a las siguientes categorías de actividades de tratamiento, llevadas a cabo por parte de Hospital público de Gotan conforme a lo dispuesto en el artículo 30 RGPD.

3.1. Tratamiento - HISTORIAL CLÍNICO Y GESTIÓN SANITARIA

FICHEROS CON DATOS ASOCIADOS
Historial clínico y gestión sanitaria
ARCHIVOS AUTOMATIZADOS
Sistema informático de historias clínicas (sihc)
CATEGORÍAS DE DATOS PERSONALES
CATEGORÍAS DE DATOS DE CARÁCTER IDENTIFICATIVO NIF/DNI Nº SS / Mutualidad Nombre y Apellidos Tarjeta Sanitaria Dirección Postal Teléfono **CATEGORÍAS ESPECIALES DE DATOS** Origen racial o étnico Opiniones religiosas Datos genéticos Datos relativos a la salud Vida sexual
ORIGEN DE LOS DATOS
El propio interesado o su representante legal Otras personas físicas Registros públicos Administraciones Públicas
COLECTIVOS O CATEGORIAS DE INTERESADOS
Pacientes Personas de contacto Padres o tutores Representante legal Beneficiarios

CATEGORIAS DE DESTINATARIOS DE CESIONES
Fuerzas y cuerpos de seguridad: Cesión obligatoria en caso de requerimiento judicial, denuncia de delitos, o para la colaboración necesaria que afecten a la seguridad pública y a la vida de las personas. Entidades aseguradoras: Para la gestión de la facturación y el cobro de la asistencia sanitaria prestada a pacientes cubiertos por seguros privados, mutuas de accidentes o convenios. Interesados legítimos: Para atender el ejercicio del derecho de acceso a la historia clínica de un paciente por parte de sus herederos, tutores o representantes legalmente autorizados. Entidades sanitarias: Para garantizar la continuidad y calidad de la asistencia sanitaria del paciente, permitiendo el intercambio de información clínica con otros hospitales, centros de salud o niveles de atención.
FINALIDADES
Proporcionar asistencia sanitaria y garantizar la continuidad asistencial, así como cumplir obligaciones legales en materia de salud.
FINALIDADES. DATOS ADICIONALES
La finalidad del tratamiento implica el uso específico de datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad
INTERESADOS OBJETO DEL TRATAMIENTO
El número de afectados es + de 100.000
EXTENSIÓN GEOGRÁFICA DEL TRATAMIENTO
Nacional
OPERACIONES
- Eliminación de los datos una vez cumplido el plazo de conservación, de acuerdo con los procedimientos internos de borrado seguro. - Mantenimiento de las historias clínicas de forma estructurada en la base de datos central. - Migración masiva de datos desde el servidor local al entorno Cloud de No problem S.L. - Acceso remoto y controlado a la historia clínica por el personal asistencial y médico para el diagnóstico y tratamiento, utilizando credenciales y permisos definidos (Control de Acceso Basado en Roles - RBAC) - Transmisión de datos cifrados a otros centros sanitarios, organismos de Seguridad Social o autoridades judiciales

BASE LEGITIMADORA
Cumplimiento de una obligación legal Protección de los intereses vitales del interesado

4. Plan de proyecto

Las fases que se han seguido han sido las siguientes:

1. Definición de alcance y planificación
2. Preparación
3. Necesidad y proporcionalidad
4. Gestión de riesgos:
4.1.Apreciación de riesgos
4.2.Identificación de riesgos
4.3.Análisis de riesgos
4.4.Evaluación de riesgos
5.Consultas
6. Tratamiento del riesgo
7. Emisión de informe

5. Consultas efectuadas

A continuación se indican los datos de los consultados así como las opiniones manifestadas por estos.

CUESTIÓN	
¿La ubicación geográfica del centro de datos (cloud) de No problem S.L. implica una Transferencia Internacional de Datos?	
FECHA	28 de noviembre de 2025
RESPONSABLE DE DAR RESPUESTA	Bruce Wayne
ESTADO	Pendiente de respuesta

CUESTIÓN	
Riesgos del Proveedor: ¿Cuáles son los cinco principales riesgos técnicos identificados por No problem S.L. en su CPD que podrían afectar la disponibilidad, integridad o confidencialidad de las Historias Clínicas del Hospital de Gotan?	
FECHA	11 de diciembre de 2025

RESPONSABLE DE DAR RESPUESTA	No problem S.L. (Encargado del Tratamiento)
ESTADO	Pendiente de respuesta

CUESTIÓN	
Visión del Paciente: ¿Qué riesgos perciben los pacientes y las asociaciones de usuarios sobre la confidencialidad y la accesibilidad de sus Historias Clínicas al migrar al cloud de No problem S.L.?	
FECHA	10 de diciembre de 2025
RESPONSABLE DE DAR RESPUESTA	Comité de Ética e Investigación
ESTADO	Pendiente de respuesta

6. Consultas a la Autoridad de Contol efectuadas

CUESTIÓN	
¿Cuál es el procedimiento más adecuado para gestionar la obligación de borrado una vez cumplido el plazo legal de conservación, en un entorno de Cloud Computing, garantizando que el proveedor cumpla con la supresión total de las copias de seguridad?	
FECHA	13 de diciembre de 2025
ESTADO	Pendiente de respuesta
RESPUESTA	

CUESTIÓN	
La EIPD identifica que el Tratamiento de Historias Clínicas en cloud entraña un Riesgo Residual elevado. A pesar de las medidas de mitigación, ¿es necesaria la Consulta Previa obligatoria a esta Autoridad de Control antes de la migración del sistema?	
FECHA	13 de diciembre de 2025
ESTADO	Pendiente de respuesta
RESPUESTA	

CUESTIÓN	
Tratamiento de historias clínicas en SaaS sin mitigación completa de escenarios de alto riesgo	
FECHA	8 de diciembre de 2025
ESTADO	Contestada
RESPUESTA	
Mayor segregación de datos en el sistema SaaS. Incorporar controles de autenticación reforzada (MFA) y cifrado extremo a extremo. Establecer un proceso de revisión de accesos con alertas ante accesos no autorizados.	

CUESTIÓN	
Uso de tecnología biométrica para acceso a las historias clínicas	
FECHA	9 de diciembre de 2025
ESTADO	Pendiente de respuesta
RESPUESTA	

7. Metodología

7.1. Requisitos de la Metodología

Toda metodología de gestión de riesgos debe cumplir los siguientes requisitos:

Metódica	No deje lugar a la improvisación.
Objetiva	El método utilizado debe ser objetivo y no depender de la arbitrariedad.
Repetible	Debe permitir conseguir resultados repetibles en el tiempo.
Documentada	Toda modificación, concreción o criterio adoptado respecto de la presente metodología deberá registrarse en este documento al objeto de que cualquier persona autorizada pueda consultarla y continuarla.

Por tanto los riesgos que inicialmente están por encima de dicho nivel y deben ser tratados

son los que se listan a continuación:

7.2. Tipo de Metodología

Para la elaboración de la presente metodología se ha considerado lo establecido en la "ISO 31000:2009 Gestión del Riesgo- Principios y Directrices".

Se han seguido las siguientes fases:

1. Apreciación del riesgo, lo que incluye:
    a) Identificación de riesgos.
    b) Análisis de riesgos.
    c) Evaluación de riesgos.
2. Tratamiento de los riesgos.

7.3. Análisis de los Escenarios de Riesgo

Una vez determinado los diferentes escenarios de riesgo, hay que estimar cuán vulnerable es el tratamiento de datos, en dos sentidos:

- **Frecuencia:** Cada cuánto se materializa el escenario del riesgo.
- **Impacto:** Supuesta la materialización del escenario del riesgo, estimación del daño o perjuicio que ocasionará.

7.3.1. Criterio de valoración de la frecuencia de materialización de una amenaza

La frecuencia pone en perspectiva la degradación, pues una amenaza puede ser de terribles consecuencias pero de muy improbable materialización; mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulando un daño considerable.

Se valora la frecuencia de materialización de una amenaza en base a la siguiente escala y criterio con la correspondiente equivalencia:

NOMBRE	*DESCRIPCIÓN*
>= 1 vez cada 100 años	Se produce al menos una vez cada 100 años
>= 1 vez cada 10 años	Se produce al menos una vez cada 10 años
>= 1 vez al año	Se produce al menos una vez al año
>= 10 veces al año	Se produce al menos 10 veces al año
>= 100 veces al año	Se produce al menos 100 veces al año

7.4. Criterios de impacto

Concepto. El impacto mide (o estima) el daño causado por un escenario del riesgo en el supuesto de que ocurriera.

Valoración. Al respecto se valora el impacto en un tratamiento caso de verse afectado por escenario de riesgo en base a la siguiente escala (por defecto) y criterio:

A la hora de evaluar los posibles impactos, se han considerado los siguientes criterios: Pena, pérdida de clientes, pérdidas económicas y daños reputacionales. Como criterio general, se atenderá a lo dispuesto en la siguiente tabla:

Pérdida de clientes

IMPACTO	NOMBRE	DESCRIPCIÓN
N/A	N/A	
=< 10% clientes	=< 10% clientes	Un porcentaje de hasta un 10 por ciento de la cartera de clientes decide no continuar con los servicios o productos ofrecidos.
=< 30% clientes	=< 30% clientes	Un porcentaje de hasta un 30 por ciento de la cartera de clientes decide no continuar con los servicios o productos ofrecidos.
> 30% clientes	> 30% clientes	Un porcentaje de más del 30 por ciento de la cartera de clientes decide no continuar con los servicios o productos ofrecidos.

Daño Reputacional

IMPACTO	NOMBRE	DESCRIPCIÓN
N/A	N/A	
Muy Bajo	Muy Bajo	Se origina un daño en la reputación que podría ser perjudicial en la captación de nuevos clientes.
Bajo	Bajo	Se origina un daño en la reputación que podría ser perjudicial en clientes indecisos.
Medio	Medio	Se origina un daño en la reputación que podría ser perjudicial en clientes consolidados.
Alto	Alto	El daño reputacional es grave puesto que provoca noticias en prensa de ámbito local.
Muy Alto	Muy Alto	El daño reputacional es grave puesto que provoca noticias en prensa de ámbito nacional.

Pérdida Económica

IMPACTO	NOMBRE	DESCRIPCIÓN
N/A	N/A	

=< 10% de la facturación anual	=< 10% de la facturación anual	Perdida económica que suponga hasta un 10 por ciento de la facturación anual.
=< 30% de la facturación anual	=< 30% de la facturación anual	Perdida económica que suponga hasta un 30 por ciento de la facturación anual.
> 30% de la facturación anual	> 30% de la facturación anual	Perdida económica que suponga más de un 30 por ciento de la facturación anual.

Sanciones

IMPACTO	*NOMBRE*	*DESCRIPCIÓN*
N/A	N/A	
Apercibimiento o sin sanción	Apercibimiento o sin sanción	Apercibimiento o sin sanción
Grave	Grave	10.000.0000€ ó 2% facturación anual
Muy Grave	Muy Grave	20.000.0000€ ó 4% facturación anual

Derechos y Libertades

IMPACTO	*NOMBRE*	*DESCRIPCIÓN*
N/A	N/A	
Despreciable	Despreciable	Los interesados no se verán prácticamente afectados o encontrarán alguna pequeña inconveniencia
Limitado	Limitado	Los interesados podrán encontrar inconveniencias no significativas.
Significativo	Significativo	Los interesados encontrarán consecuencias significativas que deberían poder superar sin dificultades serias
Máximo	Máximo	Los interesados encontrarán consecuencias significativas o incluso irreversibles, que no podrán llegar a superarse.

7.5. Evaluación de los escenarios de riesgo

El valor del riesgo es el resultado de poner en unión para cada escenario de riesgo la probabilidad y el posible impacto.

La fórmula utilizada para el cálculo del Riesgo Inicial es: **RI=PXI**RIESGO = FRECUENCIA x IMPACTO

De esta manera, se genera la siguiente matriz de riesgo:

		IMPACTO				
		Muy Bajo	*Bajo*	*Medio*	*Alto*	*Muy Alto*
FRECUENCIA	>= 1 vez cada 100 años	Muy Bajo	Bajo	Bajo	Medio	Medio
	>= 1 vez cada 10 años	Bajo	Bajo	Medio	Medio	Alto
	>= 1 vez al año	Bajo	Medio	Medio	Alto	Alto
	>= 10 veces al año	Medio	Medio	Alto	Alto	Muy Alto
	>= 100 veces al año	Medio	Alto	Alto	Muy Alto	Muy Alto

El umbral de riesgos determinado como aceptable es el siguiente: MEDIO

7.6. Tratamiento del Riesgo

El análisis de riesgos determina impactos y riesgos.

- Los impactos recogen daños absolutos, independientemente de que sea más o menos probable que se dé la circunstancia.
- El riesgo pondera la probabilidad de que ocurra.
- El impacto refleja el daño posible, mientras que el riesgo refleja el daño probable.

Si los riesgos obtenidos son despreciables, se ha terminado. Si no, debemos de tomar las medidas necesarias para minimizar en lo posible el riesgo.
Para cada uno de los Riesgos relevantes, que no entren en los Criterios de Aceptación, deberemos adoptar una decisión sobre su tratamiento.

A estos efectos, para cada riesgo decidiremos:

Ignorar el riesgo	No hacer nada, aunque hay que tener en cuenta que ignorar el riesgo, siempre es arriesgada y hay que tomarla con prudencia y justificación. Las razones que pueden llevar a esta aceptación son: • Cuando el impacto es asumible. • Cuando el riesgo es asumible. • Cuando el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo.
Mitigar	Mediante la implantación de controles que reduzcan el riesgo por

	debajo del umbral establecido. Esta reducción o mitigación del riesgo se refiere a una de dos opciones: • Reducir el impacto causado por un escenario del riesgo. • Reducir la probabilidad de que un escenario del riesgo se materialice.
Evitarlo	Anulando, excluyendo o sustituyendo el elemento o funcionalidad del diseño. No siempre es posible ya que puede provocar una pérdida esencial de funcionalidad.

Las distintas opciones de tratamiento del riesgo serán denominadas comúnmente "salvaguardas".

A efectos prácticos, dependiendo de la decisión tomada, ésta afectará al cálculo del riesgo de dos formas:

- Reduciendo la frecuencia de los escenarios del riesgo.
- Se llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que el escenario del riesgo se materialice.
- Hay salvaguardas que directamente limitan el posible impacto, mientras que otras permiten detectar inmediatamente el origen para frenar el daño avance. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.

El valor del riesgo final obtenido tras aplicarle el tratamiento adecuado es el Riesgo Final.

- Si éste se encuentra por debajo del nivel de riesgo aceptable, se considera aceptado.
- En caso contrario, si todavía supera dicho nivel, podemos seguir aplicando soluciones posibles, o bien ignorarlo, si lo consideramos necesario, en cuyo caso se requerirá una justificación explícita de esa decisión.

8. Evaluación de Riesgos

Por tanto los riesgos que inicialmente están por encima de dicho nivel y deben ser tratados son los que se listan a continuación:

ESCENARIOS DE RIESGOS A TRATAR	*RIESGO INICIAL*
Dificultar o imposibilitar el ejercicio de los derechos ARCO	Medio
Carencia de procedimientos y herramientas para la gestión de los derechos ARCO	Alto
Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales	Alto
Tratamiento ilícito. No concurrencia de las condiciones previstas por el RGPD	Medio

Tratamiento de categorías especiales de datos personales sin la concurrencia de una de las circunstancias previstas por el art 9. RGPD.	Medio
Realizar un tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sin la supervisión de las autoridades públicas o en base a disposición legal, comunitaria o estatal.	Medio
No facilitar al interesado toda la información requerida en el momento de la recogida de sus datos personales.	Alto
No aplicar medidas técnicas y organizativas apropiadas teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas a fin de garantizar y poder demostrar que el tratamiento es conforme al RGPD.	Alto
No aplicar en el momento de determinar los medios de tratamiento y/o en el propio momento del tratamiento medidas técnicas y organizativas apropiadas que garanticen la efectividad de los principios de protección.	Alto
No aplicar medidas técnicas y organizativas apropiadas tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento	Medio
Datos personales accesibles, sin intervención de la persona, a un número indeterminado de personas. (Protección de datos desde el diseño y por defecto)	Alto
No aplicar las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, sólo sean objeto de tratamietno los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento	Alto
Falta de diligencia (o dificultad para demostrarla) en la elección del encargado del tratamiento.	Medio
Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervidar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad.	Alto
No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos ARCOP presentados ante los encargados de tratamiento	Medio
Dificultad para conseguir la portabilidad de los datos personales a otros entornos una vez finalizado el contrato	Medio

El responsable y el encargado del tratamiento no aplican medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.	Alto
No consultar a la autoridad de control antes de proceder a un tratamiento, cuando una vez realizada la EIPD, el mismo entrañe un alto riesgosi el responsable no toma medidas para mitigarlo.	Medio
Ejercicio de Derechos ARSOPL: Carencia de conocimiento por parte del personal de qué hacer si recibe una petición de derechos ARSOPL	Alto
Ejercicio de Derechos ARSOPL: Falta de definición de la persona/s que gestionarán las peticiones de derechos ARSOPL	Alto
Datos especialmente protegidos: Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso y específico cuando éste sea la causa que legitima el tratamiento o cesión de datos sensibles. Ej: no incluir casilla para consentimiento para el tratamiento de datos con fines de investigación o tratar datos religiosos sin consentimiento	Alto
Datos especialmente protegidos: Asunción errónea de la existencia de una habilitación legal para el tratamiento o cesión de datos sensibles	Alto
Datos especialmente protegidos: Facilitar información sobre los pacientes a cualquier persona no autorizada o utilizando medios que no permitan la correcta identificación del destinatario (teléfono, etc…)	Alto
Datos especialmente protegidos: No registrar los accesos a las Historias Clínicas	Alto
Datos especialmente protegidos: Enviar información clínica, a través de redes de telecomunicaciones, sin cifrar	Alto
Datos especialmente protegidos: Existencia de errores técnicos u organizativos que propicien la falta de integridad de la información, permitiendo la existencia de registros duplicados o duplicidad de HC del mismo paciente, con informaciones diferentes o contradictorias, lo que puede derivar en la toma de decisiones erróneas Ej: que la aplicación que gestiona los datos de usuarios permita dar de alta dos usuarios con el mismo NIF	Alto
Datos especialmente protegidos: Falta de definición de los plazos de conservación de la distinta tipología de datos personales, en consonancia con el plazo de conservación de la HC	Alto
Datos especialmente protegidos: No tener un procedimiento específico para la atención de las solicitudes de acceso a la Historia Clínica conforme a lo	Alto

establecido en la Ley de Autonomía del Paciente y en la normativa autonómica	
Tratamientos por encargo: Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas	Alto
Legitimación del Tratamiento: Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales Ej: publicar imágenes de residentes en las redes sociales sin la previa autorización e información de los mismos o facilitar datos a entidades colaboradoras sin una causa legal.	Alto
Legitimación del Tratamiento: Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros Ej: si recibimos imágenes de otro centro para realizar la memoria anual de actividades, no poder garantizar que estas imágenes se obtuvieron lícitamente por el emisor	Medio
Deber de secreto: Deficiencias que pueden permitir accesos no autorizados a datos personales en soporte automatizado por parte de los empleados y colaboradores Ej: incorrecta definición de los perfiles de usuarios que permite el acceso a información asistencial a personal de otro área que no necesita conocer dicha información	Alto
Seguridad: Existe el riesgo de pérdida de confidencialidad y/o integridad de la información en su transmisión (comunicaciones), a través del correo electrónico u otros medios	Alto
Seguridad: Existe el riesgo de no poder recuperar la información que se haya podido eliminar accidental o intencionadamente	Alto
Seguridad en Redes y comunicaciones: Cuando el acceso se realiza a través de Internet, la comunicación se debe cifrar a través de protocolos criptográficos (TLS / SSL).	Alto
Seguridad en Redes y comunicaciones: El tráfico hacia y desde el sistema de TI debe ser monitorizado y controlado a través de cortafuegos y sistemas de detección de intrusos	Alto
Seguridad en Redes y comunicaciones: El acceso remoto al sistema de TI debería evitarse en general. En los casos en que esto sea absolutamente necesario, debe realizarse solo bajo el control y monitorización de una persona específica de la Organización, a través de VPN	Alto

9. Tratamiento de Riesgos

La forma en que se trata cada riesgo, los controles a adoptar, las personas encargadas, el plazo y el nivel de riesgo residual que se alcanzará una vez adoptados los mismos son los siguientes:

ESCENARIO DE RIESGO	
Dificultar o imposibilitar el ejercicio de los derechos ARCO	
NIVEL DE RIESGO INICIAL	Medio
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	

C.RGPD-AEPD.ARCO.1.a - Implantar sistemas que permitan a los afectados acceder de forma fácil, directa y con la apropiada seguridad a sus datos personales, así como ejercitar sus derechos ARCO
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 18-dic-2025

C.RGPD-AEPD.ARCO.1.b - Evitar sistemas de ejercicio de los derechos ARCO que impliquen solicitar una remuneración
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 18-dic-2025

C.RGPD-AEPD.ARCO.1.c - Evitar establecer procedimientos poco transparentes, complejos y laboriosos
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 18-dic-2025

C.RGPD-AEPD.ARCO.1.d - Formar a todo personal para que conozca qué ha de hacer si recibe una petición de derecho ARCO o ha de informar a los afectados sobre cómo ejercerla
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 18-dic-2025

C.RGPD-AEPD.ARCO.1.e - Definir qué personas o departamentos se ocuparán de gestionar los derechos ARCO y formarlos adecuadamente
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 18-dic-2025

NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO	
Carencia de procedimientos y herramientas para la gestión de los derechos ARCO	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD-AEPD.ARCO.2.a - Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen que todos los empleados conocen cómo actuar ante un ejercicio de derechos ARCO y que pueden suministrar la información adecuada a los afectados **Responsable de Implantación:** Bruce Wayne **Supervisor:** Alfred Pennyworth **Fecha Límite Implantación:** 17-dic-2026 C.RGPD-AEPD.ARCO.2.b - Formación de los empleados encargados de gestionar los ejercicios de derechos ARCO **Responsable de Implantación:** Bruce Wayne **Supervisor:** Alfred Pennyworth **Fecha Límite Implantación:** 25-mar-2027	
NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO	
Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD-AEPD.ARCO.3.a - Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, cancelaciones y oposiciones a las organizaciones a las que se hayan cedido los datos personales de que	

se trate **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 18-dic-2025 C.RGPD-AEPD.ARCO.3.b - Establecimiento de acuerdos y procedimientos de gestión y comunicación con los cesionarios de la información que garanticen la correcta actualización de los datos personales cedidos **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 18-dic-2025 C.RGPD-AEPD.ARCO.3.c - Formación de los empleados encargados de gestionar los ejercicios de derechos ARCO **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 18-dic-2025

NIVEL DE RIESGO RESIDUAL	Alto

ESCENARIO DE RIESGO	
Tratamiento ilícito. No concurrencia de las condiciones previstas por el RGPD	
NIVEL DE RIESGO INICIAL	Medio
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO	
Tratamiento de categorías especiales de datos personales sin la concurrencia de una de las circunstancias previstas por el art 9. RGPD.	
NIVEL DE RIESGO INICIAL	Medio
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO	
Realizar un tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sin la supervisión de las autoridades públicas o en base a disposición legal, comunitaria o estatal.	
NIVEL DE RIESGO INICIAL	Medio
TRATAMIENTO DEL RIESGO	Evitar
JUSTIFICACIÓN	
El Hospital debe evitar activamente tratar datos penales que no deriven estrictamente de una obligación legal (ej., un protocolo médico-legal) o de la supervisión judicial/policial. La mitigación no es suficiente; se debe imponer la prohibición de tratamiento no justificado.	
NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO	
No facilitar al interesado toda la información requerida en el momento de la recogida de sus datos personales.	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD-AEPD.CAL.4 - Suministrar información transparente y clara sobre las finalidades para las que se tratarán los datos personales, en particular, a través de una política de privacidad visible y accesible C.RGPD-AEPD.CAL.5 - Proporcionar información sobre los criterios utilizados en la toma de decisiones y permitir a los afectados impugnar la decisión y solicitar que sea revisada por una persona	
NIVEL DE RIESGO RESIDUAL	Alto

ESCENARIO DE RIESGO
No aplicar medidas técnicas y organizativas apropiadas teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas a fin de garantizar y poder demostrar que el tratamiento es conforme al RGPD.

NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.U.E.32.01 - Aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 11-dic-2025	
NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO
No aplicar en el momento de determinar los medios de tratamiento y/o en el propio momento del tratamiento medidas técnicas y organizativas apropiadas que garanticen la efectividad de los principios de protección.

NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.U.E.25.01 - Aplicar, tanto en el momento de determinar los los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas. **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 20-may-2026 C.U.E.32.01 - Aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 30-jun-2026	
NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO

No aplicar medidas técnicas y organizativas apropiadas tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento

NIVEL DE RIESGO INICIAL	Medio
TRATAMIENTO DEL RIESGO	Mitigar

CONTROLES
C.RGPD-APDCAT.OBGL.21 - 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 riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, conforme al art. 32 RGPD

NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO
Datos personales accesibles, sin intervención de la persona, a un número indeterminado de personas. (Protección de datos desde el diseño y por defecto)

NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar

CONTROLES
C.U.E.25 - Garantizar que por defecto, los datos personales no son accesibles, sin la intervención de la persona, a un número indeterminado de personas. **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 17-dic-2025 C.U.E.25.02 - Aplicar las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, sólo sean de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 17-dic-2025

NIVEL DE RIESGO RESIDUAL	Alto

ESCENARIO DE RIESGO	
No aplicar las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, sólo sean objeto de tratamietno los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD-AEPD.CAL.1.a - Revisar de forma exhaustiva los flujos de información para detectar si se solicitan datos personales que luego no son utilizados en ningún proceso **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 20-dic-2025 C.MAN.MIN.02 - El DPD revisará todos los formularios y funciones del SIHC para asegurar que solo se solicitan y procesan los datos personales estrictamente necesarios para cada finalidad específica (Minimización). **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 20-dic-2025	
NIVEL DE RIESGO RESIDUAL	Alto

ESCENARIO DE RIESGO	
Falta de diligencia (o dificultad para demostrarla) en la elección del encargado del tratamiento.	
NIVEL DE RIESGO INICIAL	Medio
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.U.E.28.01 - Establecer un procedimiento que proporcione garantías suficientes de cumplimiento de las obligaciones estipuladas en el contrato de acceso a datos, así como la correcta adopción de las medidas de seguridad por parte del encargado de tratamiento. **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne	

Fecha Límite Implantación: 18-dic-2025

NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO	
Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervidar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad.	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.U.E.28.02 - Establecer mecanismos y procedimientos que garanticen el control sobre las actividades de los subcontratistas que pueda elegir un encargado de tratamiento. C.U.E.28.03 - Establecer procedimientos que garanticen que el encargado de tratamiento informará al responsable debidamente acerca de las peticiones de ejercicio de los derechos ARCOP que se le hayan formulado respecto a los tratamientos de datos personales que efectúa por su cuenta.	
NIVEL DE RIESGO RESIDUAL	Alto

ESCENARIO DE RIESGO	
No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos ARCOP presentados ante los encargados de tratamiento	
NIVEL DE RIESGO INICIAL	Medio
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD-AEPD.ARCO.3.a - Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, cancelaciones y oposiciones a las organizaciones a las que se hayan cedido los datos personales de que se trate **Responsable de Implantación:** Alfred Pennyworth	

Supervisor: Bruce Wayne
Fecha Límite Implantación: 18-dic-2025

C.RGPD-AEPD.ARCO.3.b - Establecimiento de acuerdos y procedimientos de gestión y comunicación con los cesionarios de la información que garanticen la correcta actualización de los datos personales cedidos
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 18-dic-2025

C.RGPD-AEPD.ARCO.3.c - Formación de los empleados encargados de gestionar los ejercicios de derechos ARCO
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 18-dic-2025

NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO
Dificultad para conseguir la portabilidad de los datos personales a otros entornos una vez finalizado el contrato

NIVEL DE RIESGO INICIAL	Medio
TRATAMIENTO DEL RIESGO	Mitigar

CONTROLES
C.U.E.28.04 - Establecer un procedimiento para garantizar la portabilidad de los datos personales a otros entornos, una vez finalizado el contrato **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 18-dic-2025

NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO
El responsable y el encargado del tratamiento no aplican medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

NIVEL DE RIESGO INICIAL	Alto

TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	

C.RGPD-AEPD.SEG.6.a - Adoptar medidas de cifrado –adecuadas al riesgo y al estado de la tecnología– de los datos personales almacenados y compartidos a través de redes de telecomunicaciones (en particular, si son públicas y/o inalámbricas) para minimizar el riesgo de que terceros no autorizados accedan a ellos ante un hipotético fallo de seguridad
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 20-dic-2025

C.U.E.32.01 - Aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 20-dic-2025

C.RGPD.SAN.SEG.12 - Seguridad: Adoptar medidas de cifrado - adecuadas al riesgo y al estado de la tecnología - de los datos personales almacenados y compartidos a través de redes de telecomunicaciones (en particular, si son públicas y/o inalámbricas) para minimizar el riesgo de que terceros no autorizados accedan a ellos ante un hipotético fallo de seguridad
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 20-dic-2025

C.RGPD.SAN.SEG.26 - Política de uso correcto de portátiles, smarthphone, y dispositivos móviles Medidas de seguridad para el acceso de los usuarios a los dispositivos (usuario/contraseña), Cifrado del disco duro. .
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 20-dic-2025

C.RGPD.SAN.SEG.30 - Realizar copias de seguridad, que incluya toda la información de la organización y se encuentren cifradas
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 20-dic-2025

C.RGPD.SAN.SEG.38 - Implementación de protocolos de cifrado de comunicaciones en todos los servicios con salida a internet
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne

Fecha Límite Implantación: 20-dic-2025

C.RGPD.SAN.SEG.43 - Implementar mecanismos de cifrado para el envío, a través de redes de telecomunicaciones, de información sensible
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 20-dic-2025

C.MAN.EIPD.01 - Auditoría del Diseño (Privacy by Design): Realizar una auditoría técnica (gap analysis) sobre la arquitectura del SIHC de No problem S.L. para confirmar que implementa medidas técnicas de seguridad (cifrado total, seudonimización por defecto) en el diseño de la solución cloud antes de la migración.
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 20-dic-2025

NIVEL DE RIESGO RESIDUAL	Alto

ESCENARIO DE RIESGO
No consultar a la autoridad de control antes de proceder a un tratamiento, cuando una vez realizada la EIPD, el mismo entrañe un alto riesgosi el responsable no toma medidas para mitigarlo.

NIVEL DE RIESGO INICIAL	Medio
TRATAMIENTO DEL RIESGO	Mitigar

CONTROLES
C.U.E.36 - Establecer un procedimiento de consultas a la autoridad de control antes de proceder a un tratamiento, cuando una vez realizada la EIPD, el mismo entrañe un alto riesgo si el responsable no toma medidas para mitigarlo. **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 18-dic-2025

NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO
Ejercicio de Derechos ARSOPL: Carencia de conocimiento por parte del personal de qué

hacer si recibe una petición de derechos ARSOPL	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD-AEPD.ARCO.2.a - Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen que todos los empleados conocen cómo actuar ante un ejercicio de derechos ARCO y que pueden suministrar la información adecuada a los afectados **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 20-dic-2025 C.RGPD-AEPD.ARCO.2.b - Formación de los empleados encargados de gestionar los ejercicios de derechos ARCO **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 20-dic-2025 C.RGPD-AEPD.ARCO.3.b - Establecimiento de acuerdos y procedimientos de gestión y comunicación con los cesionarios de la información que garanticen la correcta actualización de los datos personales cedidos **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 20-dic-2025 C.RGPD-AEPD.ARCO.3.c - Formación de los empleados encargados de gestionar los ejercicios de derechos ARCO **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 20-dic-2025	
NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO
Ejercicio de Derechos ARSOPL: Falta de definición de la persona/s que gestionarán las peticiones de derechos ARSOPL

NIVEL DE RIESGO INICIAL	Alto

TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.MAN.ORG.01 - Creación de Unidad de Gestión ARCOP: Definir la Unidad de Gestión de Derechos ARCOP del Hospital, asignando formalmente a la persona o equipo (ej., el equipo de Archivo y Documentación) la responsabilidad primaria de recibir, registrar y coordinar la respuesta a todas las solicitudes de los pacientes. **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 20-dic-2025	
NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO	
Datos especialmente protegidos: Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso y específico cuando éste sea la causa que legitima el tratamiento o cesión de datos sensibles. Ej: no incluir casilla para consentimiento para el tratamiento de datos con fines de investigación o tratar datos religiosos sin consentimiento	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD-AEPD.CEP.1.b - Establecer procedimientos que garanticen la obtención del consentimiento expreso (y por escrito cuando sea necesario) y que permitan probar que se cuenta con él. **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 12-dic-2025	
NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO	
Datos especialmente protegidos: Asunción errónea de la existencia de una habilitación legal para el tratamiento o cesión de datos sensibles	
NIVEL DE RIESGO INICIAL	Alto

TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD-AEPD.GEN.2.a - Formación apropiada del personal sobre protección de datos en el sector específico de que se trate **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 12-dic-2025 C.MAN.MIN.02 - El DPD revisará todos los formularios y funciones del SIHC para asegurar que solo se solicitan y procesan los datos personales estrictamente necesarios para cada finalidad específica (Minimización). **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 12-dic-2025	
NIVEL DE RIESGO RESIDUAL	Alto

ESCENARIO DE RIESGO	
Datos especialmente protegidos: Facilitar información sobre los pacientes a cualquier persona no autorizada o utilizando medios que no permitan la correcta identificación del destinatario (teléfono, etc…)	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD-AEPD.SEG.6.e - Construir canales seguros y con verificación de identidad para la distribución de información de seguridad (códigos de usuario, contraseñas, etc.) **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 20-dic-2025 C.RGPD-APDCAT.OBGL.15 - El registro de actividades de tratamiento deberá mantenerse actualizado en todo momento **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 20-dic-2025	

NIVEL DE RIESGO RESIDUAL	Alto

ESCENARIO DE RIESGO	
Datos especialmente protegidos: No registrar los accesos a las Historias Clínicas	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD-AEPD.SEG.4 - Establecer mecanismos de registro de acciones sobre los datos personales o logging así como herramientas fiables y flexibles de explotación de los ficheros de auditoría resultantes **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 20-dic-2025 C.RGPD-APDCAT.OBGL.15 - El registro de actividades de tratamiento deberá mantenerse actualizado en todo momento **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 20-dic-2025	
NIVEL DE RIESGO RESIDUAL	Alto

ESCENARIO DE RIESGO	
Datos especialmente protegidos: Enviar información clínica, a través de redes de telecomunicaciones, sin cifrar	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD.SAN.SEG.42 - Implementar mecanismos de trazabilidad que permitan, en este caso, tener controlados todos los accesos a esta información **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 20-dic-2025	

C.RGPD.SAN.SEG.43 - Implementar mecanismos de cifrado para el envío, a través de redes de telecomunicaciones, de información sensible

NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO	
Datos especialmente protegidos: Existencia de errores técnicos u organizativos que propicien la falta de integridad de la información, permitiendo la existencia de registros duplicados o duplicidad de HC del mismo paciente, con informaciones diferentes o contradictorias, lo que puede derivar en la toma de decisiones erróneas Ej: que la aplicación que gestiona los datos de usuarios permita dar de alta dos usuarios con el mismo NIF	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.MAN.CAL.01 - Control de Unicidad de Identidad: Implementar controles técnicos de unicidad en el nuevo SIHC de No problem S.L. para garantizar que no se pueden crear dos registros de paciente con el mismo NIF/Identificador Único, y realizar un proceso de depuración de duplicados en la fase de migración.	
NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO	
Datos especialmente protegidos: Falta de definición de los plazos de conservación de la distinta tipología de datos personales, en consonancia con el plazo de conservación de la HC	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD-AEPD.CAL.8.a - Definir claramente los plazos de cancelación de todos los datos personales de los sistemas de información **Responsable de Implantación:** Alfred Pennyworth	

Supervisor: Bruce Wayne
Fecha Límite Implantación: 27-dic-2025

C.RGPD-AEPD.CAL.8.b - Establecer controles automáticos dentro de los sistemas de información para avisar de la cercanía de los plazos de cancelación de la información
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 27-dic-2025

NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO	
Datos especialmente protegidos: No tener un procedimiento específico para la atención de las solicitudes de acceso a la Historia Clínica conforme a lo establecido en la Ley de Autonomía del Paciente y en la normativa autonómica	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD.SAN.SEG.16 - Seguridad: Construir canales seguros y con verificación de identidad para la distribución de información de seguridad (códigos de usuario, contraseñas, etc.)	
NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO	
Tratamientos por encargo: Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD.PUBLI-OFFLINE.ENC.02 - Se formalizará un contrato o acto jurídico conforme al art 28 RGPD con el tercero prestador del servicio de publicidad y prospección comercial **Responsable de Implantación:** Bruce Wayne	

Supervisor: Bruce Wayne
Fecha Límite Implantación: 16-dic-2025

C.RGPD.PUBLI-OFFLINE.ENC.04 - Los contratos o actos jurídicos entre el Responsable y el Encargado de tratamiento deberá contemplar todos los extremos recogidos en el art 28 RGPD
Responsable de Implantación: Bruce Wayne
Supervisor: Bruce Wayne
Fecha Límite Implantación: 16-dic-2025

C.RGPD.PUBLI-ONLINE.ENC.02 - Se formalizará un contrato o acto jurídico conforme al art 28 RGPD con el tercero prestador del servicio de ervicio de publicidad y prospección comercial
Responsable de Implantación: Bruce Wayne
Supervisor: Bruce Wayne
Fecha Límite Implantación: 16-dic-2025

C.RGPD.PUBLI-ONLINE.ENC.04 - Los contratos o actos jurídicos entre el Responsable y el Encargado de tratamiento deberá contemplar todos los extremos recogidos en el art 28 RGPD
Responsable de Implantación: Bruce Wayne
Supervisor: Bruce Wayne
Fecha Límite Implantación: 16-dic-2025

C.RGPD-APDCAT.OBGL..11 - La relación entre el reasponsable y el encargado del tratamiento será establecida mediante un contrato o acto jurídico que vincule al encargado respecto del responsable y establezca 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, con arreglo al art. 28 RGPD.
Responsable de Implantación: Bruce Wayne
Supervisor: Bruce Wayne
Fecha Límite Implantación: 16-dic-2025

NIVEL DE RIESGO RESIDUAL	Alto

ESCENARIO DE RIESGO
Legitimación del Tratamiento: Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales Ej: publicar imágenes de residentes en las redes sociales sin la previa autorización e información de los mismos o facilitar datos a entidades colaboradoras sin una causa legal.

NIVEL DE RIESGO INICIAL	Alto

TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD-AEPD.GEN.2.b - Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas de privacidad de la organización relativas a las legislaciones sectoriales que afectan a la organización, así como de las sanciones aparejadas al incumplimiento de las mismas. C.RGPD-AEPD.LEG.2.b - Revisar las posibilidades que ofrece la legislación de protección de datos para permitir el tratamiento de datos personales y asegurar que este encaja en alguna de ellas	
NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO	
Legitimación del Tratamiento: Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros Ej: si recibimos imágenes de otro centro para realizar la memoria anual de actividades, no poder garantizar que estas imágenes se obtuvieron lícitamente por el emisor	
NIVEL DE RIESGO INICIAL	Medio
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD-AEPD.CEP.1.b - Establecer procedimientos que garanticen la obtención del consentimiento expreso (y por escrito cuando sea necesario) y que permitan probar que se cuenta con él. **Responsable de Implantación:** Bruce Wayne **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 19-dic-2025 C.MAN.MIN.03 - Auditoría de Campos de Recogida: El DPD y el RTIS auditarán y ajustarán todos los módulos de recogida de datos del nuevo SIHC (formularios de ingreso, consentimiento, etc.) para eliminar cualquier campo que solicite información que no sea estrictamente necesaria para la finalidad declarada. **Responsable de Implantación:** Bruce Wayne **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 19-dic-2025	

NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO	
Deber de secreto: Deficiencias que pueden permitir accesos no autorizados a datos personales en soporte automatizado por parte de los empleados y colaboradores Ej: incorrecta definición de los perfiles de usuarios que permite el acceso a información asistencial a personal de otro área que no necesita conocer dicha información	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD-AEPD.ET.3.a - Establecer mecanismos y procedimientos que garanticen el control sobre las actividades de los subcontratistas que pueda elegir un encargado de tratamiento **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 20-dic-2025	
NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO	
Seguridad: Existe el riesgo de pérdida de confidencialidad y/o integridad de la información en su transmisión (comunicaciones), a través del correo electrónico u otros medios	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD-AEPD.SEG.6.a - Adoptar medidas de cifrado –adecuadas al riesgo y al estado de la tecnología– de los datos personales almacenados y compartidos a través de redes de telecomunicaciones (en particular, si son públicas y/o inalámbricas) para minimizar el riesgo de que terceros no autorizados accedan a ellos ante un hipotético fallo de seguridad **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Bruce Wayne **Fecha Límite Implantación:** 20-dic-2025	

C.RGPD.SAN.SEG.12 - Seguridad: Adoptar medidas de cifrado - adecuadas al riesgo y al estado de la tecnología - de los datos personales almacenados y compartidos a través de redes de telecomunicaciones (en particular, si son públicas y/o inalámbricas) para minimizar el riesgo de que terceros no autorizados accedan a ellos ante un hipotético fallo de seguridad
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 20-dic-2025

C.RGPD.SAN.SEG.26 - Política de uso correcto de portátiles, smarthphone, y dispositivos móviles Medidas de seguridad para el acceso de los usuarios a los dispositivos (usuario/contraseña), Cifrado del disco duro. .
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 20-dic-2025

C.RGPD.SAN.SEG.38 - Implementación de protocolos de cifrado de comunicaciones en todos los servicios con salida a internet
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 20-dic-2025

C.RGPD.SAN.SEG.43 - Implementar mecanismos de cifrado para el envío, a través de redes de telecomunicaciones, de información sensible
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 20-dic-2025

NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO	
Seguridad: Existe el riesgo de no poder recuperar la información que se haya podido eliminar accidental o intencionadamente	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD.SAN.SEG.28 - Normas de gestión soportes. Contratos de encargo de tratamiento con medidas de seguridad exigidas al prestador de servicios.	

Responsable de Implantación: Bruce Wayne
Supervisor: Bruce Wayne
Fecha Límite Implantación: 18-dic-2025

C.RGPD.SAN.SEG.29 - Copias de seguridad, externalizadas o con medidas de contingencia.
Responsable de Implantación: Bruce Wayne
Supervisor: Bruce Wayne
Fecha Límite Implantación: 18-dic-2025

C.RGPD.SAN.SEG.30 - Realizar copias de seguridad, que incluya toda la información de la organización y se encuentren cifradas
Responsable de Implantación: Bruce Wayne
Supervisor: Bruce Wayne
Fecha Límite Implantación: 18-dic-2025

NIVEL DE RIESGO RESIDUAL	Alto

ESCENARIO DE RIESGO	
Seguridad en Redes y comunicaciones: Cuando el acceso se realiza a través de Internet, la comunicación se debe cifrar a través de protocolos criptográficos (TLS / SSL).	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	

C.RGPD.SAN.SEG.27 - Gestión de la configuración del cortafuegos. Control de tráfico de información. Comunicaciones remotas a través de redes privadas
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 12-dic-2025

C.RGPD.SAN.SEG.38 - Implementación de protocolos de cifrado de comunicaciones en todos los servicios con salida a internet
Responsable de Implantación: Alfred Pennyworth
Supervisor: Bruce Wayne
Fecha Límite Implantación: 12-dic-2025

NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO	
Seguridad en Redes y comunicaciones: El tráfico hacia y desde el sistema de TI debe ser monitorizado y controlado a través de cortafuegos y sistemas de detección de intrusos	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD.SAN.SEG.39 - Implementación de un firewall y de mecanismos IDS	
NIVEL DE RIESGO RESIDUAL	Medio

ESCENARIO DE RIESGO	
Seguridad en Redes y comunicaciones: El acceso remoto al sistema de TI debería evitarse en general. En los casos en que esto sea absolutamente necesario, debe realizarse solo bajo el control y monitorización de una persona específica de la Organización, a través de VPN	
NIVEL DE RIESGO INICIAL	Alto
TRATAMIENTO DEL RIESGO	Mitigar
CONTROLES	
C.RGPD.SAN.SEG.40 - Implementación de VPN para accesos remotos al sistema **Responsable de Implantación:** Alfred Pennyworth **Supervisor:** Alfred Pennyworth **Fecha Límite Implantación:** 20-dic-2025	
NIVEL DE RIESGO RESIDUAL	Medio

10. Conclusiones

Riesgo final ACEPTABLE.

De la EIPD realizada se concluye que el RIESGO FINAL es ACEPTABLE y por tanto la organización será capaz de rebajar el nivel de riesgo del tratamiento a un nivel aceptable y que no entrañe un nivel de riesgo elevado en el derecho a la protección de los datos de los interesados.

ANEXO I: SEGUIMIENTO Y CONTROL

Escenario de Riesgo	RGPD-AEPD.ARCO.1 - Dificultar o imposibilitar el ejercicio de los derechos ARCO
Control	C.RGPD-AEPD.ARCO.1.a - Implantar sistemas que permitan a los afectados acceder de forma fácil, directa y con la apropiada seguridad a sus datos personales, así como ejercitar sus derechos ARCO
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	18 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-AEPD.ARCO.1 - Dificultar o imposibilitar el ejercicio de los derechos ARCO
Control	C.RGPD-AEPD.ARCO.1.b - Evitar sistemas de ejercicio de los derechos ARCO que impliquen solicitar una remuneración
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	18 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-AEPD.ARCO.1 - Dificultar o imposibilitar el ejercicio de los derechos ARCO
Control	C.RGPD-AEPD.ARCO.1.c - Evitar establecer procedimientos poco transparentes, complejos y laboriosos
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	18 de diciembre de 2025

Completado (%)	0%

Escenario de Riesgo	RGPD-AEPD.ARCO.1 - Dificultar o imposibilitar el ejercicio de los derechos ARCO
Control	C.RGPD-AEPD.ARCO.1.d - Formar a todo personal para que conozca qué ha de hacer si recibe una petición de derecho ARCO o ha de informar a los afectados sobre cómo ejercerla
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	18 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-AEPD.ARCO.1 - Dificultar o imposibilitar el ejercicio de los derechos ARCO
Control	C.RGPD-AEPD.ARCO.1.e - Definir qué personas o departamentos se ocuparán de gestionar los derechos ARCO y formarlos adecuadamente
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	18 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-AEPD.ARCO.2 - Carencia de procedimientos y herramientas para la gestión de los derechos ARCO
Control	C.RGPD-AEPD.ARCO.2.a - Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen que todos los empleados conocen cómo actuar ante un ejercicio de derechos ARCO y que pueden suministrar la información adecuada a los afectados
Responsable de Implementación	Bruce Wayne

Supervisor	Alfred Pennyworth
Fecha Límite	17 de diciembre de 2026
Completado (%)	0%

Escenario de Riesgo	RGPD-AEPD.ARCO.2 - Carencia de procedimientos y herramientas para la gestión de los derechos ARCO
Control	C.RGPD-AEPD.ARCO.2.b - Formación de los empleados encargados de gestionar los ejercicios de derechos ARCO
Responsable de Implementación	Bruce Wayne
Supervisor	Alfred Pennyworth
Fecha Límite	25 de marzo de 2027
Completado (%)	0%

Escenario de Riesgo	RGPD-AEPD.ARCO.3 - Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales
Control	C.RGPD-AEPD.ARCO.3.a - Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, cancelaciones y oposiciones a las organizaciones a las que se hayan cedido los datos personales de que se trate
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	18 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-AEPD.ARCO.3 - Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales

Control	C.RGPD-AEPD.ARCO.3.b - Establecimiento de acuerdos y procedimientos de gestión y comunicación con los cesionarios de la información que garanticen la correcta actualización de los datos personales cedidos
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	18 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-AEPD.ARCO.3 - Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales
Control	C.RGPD-AEPD.ARCO.3.c - Formación de los empleados encargados de gestionar los ejercicios de derechos ARCO
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	18 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.13 - No facilitar al interesado toda la información requerida en el momento de la recogida de sus datos personales.
Control	C.RGPD-AEPD.CAL.4 - Suministrar información transparente y clara sobre las finalidades para las que se tratarán los datos personales, en particular, a través de una política de privacidad visible y accesible
Responsable de Implementación	
Supervisor	
Fecha Límite	

Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.13 - No facilitar al interesado toda la información requerida en el momento de la recogida de sus datos personales.
Control	C.RGPD-AEPD.CAL.5 - Proporcionar información sobre los criterios utilizados en la toma de decisiones y permitir a los afectados impugnar la decisión y solicitar que sea revisada por una persona
Responsable de Implementación	
Supervisor	
Fecha Límite	
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.24 - No aplicar medidas técnicas y organizativas apropiadas teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas a fin de garantizar y poder demostrar que el tratamiento es conforme al RGPD.
Control	C.U.E.32.01 - Aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	11 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.25.01 - No aplicar en el momento de determinar los medios de tratamiento y/o en el propio momento del tratamiento medidas técnicas y organizativas apropiadas que garanticen la efectividad de los principios de protección.
Control	C.U.E.25.01 - Aplicar, tanto en el momento de determinar los los medios de tratamiento como en el momento del propio tratamiento,

	medidas técnicas y organizativas apropiadas.
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de mayo de 2026
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.25.01 - No aplicar en el momento de determinar los medios de tratamiento y/o en el propio momento del tratamiento medidas técnicas y organizativas apropiadas que garanticen la efectividad de los principios de protección.
Control	C.U.E.32.01 - Aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	30 de junio de 2026
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.25.01 - No aplicar medidas técnicas y organizativas apropiadas tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento
Control	C.RGPD-APDCAT.OBGL.21 - 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 riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, conforme al art. 32 RGPD
Responsable de Implementación	
Supervisor	
Fecha Límite	

Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.25.02 - Datos personales accesibles, sin intervención de la persona, a un número indeterminado de personas. (Protección de datos desde el diseño y por defecto)
Control	C.U.E.25 - Garantizar que por defecto, los datos personales no son accesibles, sin la intervención de la persona, a un número indeterminado de personas.
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	17 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.25.02 - Datos personales accesibles, sin intervención de la persona, a un número indeterminado de personas. (Protección de datos desde el diseño y por defecto)
Control	C.U.E.25.02 - Aplicar las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, sólo sean de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	17 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.25.02 - No aplicar las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, sólo sean objeto de tratamietno los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento
Control	C.RGPD-AEPD.CAL.1.a - Revisar de forma exhaustiva los flujos de información para detectar si se solicitan datos personales que luego no son utilizados en ningún proceso

Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.25.02 - No aplicar las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, sólo sean objeto de tratamietno los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento
Control	C.MAN.MIN.02 - El DPD revisará todos los formularios y funciones del SIHC para asegurar que solo se solicitan y procesan los datos personales estrictamente necesarios para cada finalidad específica (Minimización).
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.28.01 - Falta de diligencia (o dificultad para demostrarla) en la elección del encargado del tratamiento.
Control	C.U.E.28.01 - Establecer un procedimiento que proporcione garantías suficientes de cumplimiento de las obligaciones estipuladas en el contrato de acceso a datos, así como la correcta adopción de las medidas de seguridad por parte del encargado de tratamiento.
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	18 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.28.02 - Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervidar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad.
Control	C.U.E.28.02 - Establecer mecanismos y procedimientos que garanticen el control sobre las actividades de los subcontratistas que pueda elegir un encargado de tratamiento.
Responsable de Implementación	
Supervisor	
Fecha Límite	
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.28.02 - Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervidar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad.
Control	C.U.E.28.03 - Establecer procedimientos que garanticen que el encargado de tratamiento informará al responsable debidamente acerca de las peticiones de ejercicio de los derechos ARCOP que se le hayan formulado respecto a los tratamientos de datos personales que efectúa por su cuenta.
Responsable de Implementación	
Supervisor	
Fecha Límite	
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.28.03 - No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos ARCOP presentados ante los encargados de tratamiento
Control	C.RGPD-AEPD.ARCO.3.a - Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen la

	comunicación de rectificaciones, cancelaciones y oposiciones a las organizaciones a las que se hayan cedido los datos personales de que se trate
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	18 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.28.03 - No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos ARCOP presentados ante los encargados de tratamiento
Control	C.RGPD-AEPD.ARCO.3.b - Establecimiento de acuerdos y procedimientos de gestión y comunicación con los cesionarios de la información que garanticen la correcta actualización de los datos personales cedidos
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	18 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.28.03 - No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos ARCOP presentados ante los encargados de tratamiento
Control	C.RGPD-AEPD.ARCO.3.c - Formación de los empleados encargados de gestionar los ejercicios de derechos ARCO
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	18 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.28.04 - Dificultad para conseguir la portabilidad de los datos personales a otros entornos una vez finalizado el contrato
Control	C.U.E.28.04 - Establecer un procedimiento para garantizar la portabilidad de los datos personales a otros entornos, una vez finalizado el contrato
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	18 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.32.01 - El responsable y el encargado del tratamiento no aplican medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
Control	C.RGPD-AEPD.SEG.6.a - Adoptar medidas de cifrado –adecuadas al riesgo y al estado de la tecnología– de los datos personales almacenados y compartidos a través de redes de telecomunicaciones (en particular, si son públicas y/o inalámbricas) para minimizar el riesgo de que terceros no autorizados accedan a ellos ante un hipotético fallo de seguridad
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.32.01 - El responsable y el encargado del tratamiento no aplican medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
Control	C.U.E.32.01 - Aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
Responsable de Implementación	Alfred Pennyworth

Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.32.01 - El responsable y el encargado del tratamiento no aplican medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
Control	C.RGPD.SAN.SEG.12 - Seguridad: Adoptar medidas de cifrado - adecuadas al riesgo y al estado de la tecnología - de los datos personales almacenados y compartidos a través de redes de telecomunicaciones (en particular, si son públicas y/o inalámbricas) para minimizar el riesgo de que terceros no autorizados accedan a ellos ante un hipotético fallo de seguridad
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.32.01 - El responsable y el encargado del tratamiento no aplican medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
Control	C.RGPD.SAN.SEG.26 - Política de uso correcto de portátiles, smarthphone, y dispositivos móviles Medidas de seguridad para el acceso de los usuarios a los dispositivos (usuario/contraseña), Cifrado del disco duro. .
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.32.01 - El responsable y el encargado del tratamiento no aplican medidas técnicas y organizativas apropiadas

	para garantizar un nivel de seguridad adecuado al riesgo.
Control	C.RGPD.SAN.SEG.30 - Realizar copias de seguridad, que incluya toda la información de la organización y se encuentren cifradas
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.32.01 - El responsable y el encargado del tratamiento no aplican medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
Control	C.RGPD.SAN.SEG.38 - Implementación de protocolos de cifrado de comunicaciones en todos los servicios con salida a internet
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.32.01 - El responsable y el encargado del tratamiento no aplican medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
Control	C.RGPD.SAN.SEG.43 - Implementar mecanismos de cifrado para el envío, a través de redes de telecomunicaciones, de información sensible
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.32.01 - El responsable y el encargado del tratamiento no aplican medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
Control	C.MAN.EIPD.01 - Auditoría del Diseño (Privacy by Design): Realizar una auditoría técnica (gap analysis) sobre la arquitectura del SIHC de No problem S.L. para confirmar que implementa medidas técnicas de seguridad (cifrado total, seudonimización por defecto) en el diseño de la solución cloud antes de la migración.
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD-GEN.R.U.E.36 - No consultar a la autoridad de control antes de proceder a un tratamiento, cuando una vez realizada la EIPD, el mismo entrañe un alto riesgosi el responsable no toma medidas para mitigarlo.
Control	C.U.E.36 - Establecer un procedimiento de consultas a la autoridad de control antes de proceder a un tratamiento, cuando una vez realizada la EIPD, el mismo entrañe un alto riesgo si el responsable no toma medidas para mitigarlo.
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	18 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.ARSOPL.04 - Ejercicio de Derechos ARSOPL: Carencia de conocimiento por parte del personal de qué hacer si recibe una petición de derechos ARSOPL
Control	C.RGPD-AEPD.ARCO.2.a - Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen que todos los empleados conocen cómo actuar ante un ejercicio de derechos ARCO y que pueden suministrar la información adecuada

	a los afectados
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.ARSOPL.04 - Ejercicio de Derechos ARSOPL: Carencia de conocimiento por parte del personal de qué hacer si recibe una petición de derechos ARSOPL
Control	C.RGPD-AEPD.ARCO.2.b - Formación de los empleados encargados de gestionar los ejercicios de derechos ARCO
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.ARSOPL.04 - Ejercicio de Derechos ARSOPL: Carencia de conocimiento por parte del personal de qué hacer si recibe una petición de derechos ARSOPL
Control	C.RGPD-AEPD.ARCO.3.b - Establecimiento de acuerdos y procedimientos de gestión y comunicación con los cesionarios de la información que garanticen la correcta actualización de los datos personales cedidos
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.ARSOPL.04 - Ejercicio de Derechos ARSOPL: Carencia de conocimiento por parte del personal de qué hacer si

	recibe una petición de derechos ARSOPL
Control	C.RGPD-AEPD.ARCO.3.c - Formación de los empleados encargados de gestionar los ejercicios de derechos ARCO
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.ARSOPL.05 - Ejercicio de Derechos ARSOPL: Falta de definición de la persona/s que gestionarán las peticiones de derechos ARSOPL
Control	C.MAN.ORG.01 - Creación de Unidad de Gestión ARCOP: Definir la Unidad de Gestión de Derechos ARCOP del Hospital, asignando formalmente a la persona o equipo (ej., el equipo de Archivo y Documentación) la responsabilidad primaria de recibir, registrar y coordinar la respuesta a todas las solicitudes de los pacientes.
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.ET.01 - Tratamientos por encargo: Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas
Control	C.RGPD.PUBLI-OFFLINE.ENC.02 - Se formalizará un contrato o acto jurídico conforme al art 28 RGPD con el tercero prestador del servicio de publicidad y prospección comercial
Responsable de Implementación	Bruce Wayne
Supervisor	Bruce Wayne
Fecha Límite	16 de diciembre de 2025

Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.ET.01 - Tratamientos por encargo: Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas
Control	C.RGPD.PUBLI-OFFLINE.ENC.04 - Los contratos o actos jurídicos entre el Responsable y el Encargado de tratamiento deberá contemplar todos los extremos recogidos en el art 28 RGPD
Responsable de Implementación	Bruce Wayne
Supervisor	Bruce Wayne
Fecha Límite	16 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.ET.01 - Tratamientos por encargo: Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas
Control	C.RGPD.PUBLI-ONLINE.ENC.02 - Se formalizará un contrato o acto jurídico conforme al art 28 RGPD con el tercero prestador del servicio de ervicio de publicidad y prospección comercial
Responsable de Implementación	Bruce Wayne
Supervisor	Bruce Wayne
Fecha Límite	16 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.ET.01 - Tratamientos por encargo: Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas
Control	C.RGPD.PUBLI-ONLINE.ENC.04 - Los contratos o actos jurídicos entre el Responsable y el Encargado de tratamiento deberá contemplar todos los extremos recogidos en el art 28 RGPD
Responsable de Implementación	Bruce Wayne

Supervisor	Bruce Wayne
Fecha Límite	16 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.ET.01 - Tratamientos por encargo: Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas
Control	C.RGPD-APDCAT.OBGL..11 - La relación entre el reasponsable y el encargado del tratamiento será establecida mediante un contrato o acto jurídico que vincule al encargado respecto del responsable y establezca 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, con arreglo al art. 28 RGPD.
Responsable de Implementación	Bruce Wayne
Supervisor	Bruce Wayne
Fecha Límite	16 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.LEG.02 - Legitimación del Tratamiento: Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales Ej: publicar imágenes de residentes en las redes sociales sin la previa autorización e información de los mismos o facilitar datos a entidades colaboradoras sin una causa legal.
Control	C.RGPD-AEPD.GEN.2.b - Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas de privacidad de la organización relativas a las legislaciones sectoriales que afectan a la organización, así como de las sanciones aparejadas al incumplimiento de las mismas.
Responsable de Implementación	
Supervisor	
Fecha Límite	
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.LEG.02 - Legitimación del Tratamiento: Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales Ej: publicar imágenes de residentes en las redes sociales sin la previa autorización e información de los mismos o facilitar datos a entidades colaboradoras sin una causa legal.
Control	C.RGPD-AEPD.LEG.2.b - Revisar las posibilidades que ofrece la legislación de protección de datos para permitir el tratamiento de datos personales y asegurar que este encaja en alguna de ellas
Responsable de Implementación	
Supervisor	
Fecha Límite	
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.LEG.05 - Legitimación del Tratamiento: Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros Ej: si recibimos imágenes de otro centro para realizar la memoria anual de actividades, no poder garantizar que estas imágenes se obtuvieron lícitamente por el emisor
Control	C.RGPD-AEPD.CEP.1.b - Establecer procedimientos que garanticen la obtención del consentimiento expreso (y por escrito cuando sea necesario) y que permitan probar que se cuenta con él.
Responsable de Implementación	Bruce Wayne
Supervisor	Bruce Wayne
Fecha Límite	19 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.LEG.05 - Legitimación del Tratamiento: Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros Ej: si recibimos imágenes de otro centro para realizar la memoria anual de actividades, no poder garantizar que estas imágenes se obtuvieron lícitamente por el

	emisor
Control	C.MAN.MIN.03 - Auditoría de Campos de Recogida: El DPD y el RTIS auditarán y ajustarán todos los módulos de recogida de datos del nuevo SIHC (formularios de ingreso, consentimiento, etc.) para eliminar cualquier campo que solicite información que no sea estrictamente necesaria para la finalidad declarada.
Responsable de Implementación	Bruce Wayne
Supervisor	Bruce Wayne
Fecha Límite	19 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.SEC.02 - Deber de secreto: Deficiencias que pueden permitir accesos no autorizados a datos personales en soporte automatizado por parte de los empleados y colaboradores Ej: incorrecta definición de los perfiles de usuarios que permite el acceso a información asistencial a personal de otro área que no necesita conocer dicha información
Control	C.RGPD-AEPD.ET.3.a - Establecer mecanismos y procedimientos que garanticen el control sobre las actividades de los subcontratistas que pueda elegir un encargado de tratamiento
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.SEG.14 - Seguridad: Existe el riesgo de pérdida de confidencialidad y/o integridad de la información en su transmisión (comunicaciones), a través del correo electrónico u otros medios
Control	C.RGPD-AEPD.SEG.6.a - Adoptar medidas de cifrado –adecuadas al riesgo y al estado de la tecnología– de los datos personales almacenados y compartidos a través de redes de telecomunicaciones (en particular, si son públicas y/o inalámbricas) para minimizar el riesgo de que terceros no autorizados accedan a

	ellos ante un hipotético fallo de seguridad
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.SEG.14 - Seguridad: Existe el riesgo de pérdida de confidencialidad y/o integridad de la información en su transmisión (comunicaciones), a través del correo electrónico u otros medios
Control	C.RGPD.SAN.SEG.12 - Seguridad: Adoptar medidas de cifrado - adecuadas al riesgo y al estado de la tecnología - de los datos personales almacenados y compartidos a través de redes de telecomunicaciones (en particular, si son públicas y/o inalámbricas) para minimizar el riesgo de que terceros no autorizados accedan a ellos ante un hipotético fallo de seguridad
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.SEG.14 - Seguridad: Existe el riesgo de pérdida de confidencialidad y/o integridad de la información en su transmisión (comunicaciones), a través del correo electrónico u otros medios
Control	C.RGPD.SAN.SEG.26 - Política de uso correcto de portátiles, smarthphone, y dispositivos móviles Medidas de seguridad para el acceso de los usuarios a los dispositivos (usuario/contraseña), Cifrado del disco duro. .
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025

Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.SEG.14 - Seguridad: Existe el riesgo de pérdida de confidencialidad y/o integridad de la información en su transmisión (comunicaciones), a través del correo electrónico u otros medios
Control	C.RGPD.SAN.SEG.38 - Implementación de protocolos de cifrado de comunicaciones en todos los servicios con salida a internet
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.SEG.14 - Seguridad: Existe el riesgo de pérdida de confidencialidad y/o integridad de la información en su transmisión (comunicaciones), a través del correo electrónico u otros medios
Control	C.RGPD.SAN.SEG.43 - Implementar mecanismos de cifrado para el envío, a través de redes de telecomunicaciones, de información sensible
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.SEG.16 - Seguridad: Existe el riesgo de no poder recuperar la información que se haya podido eliminar accidental o intencionadamente
Control	C.RGPD.SAN.SEG.28 - Normas de gestión soportes. Contratos de encargo de tratamiento con medidas de seguridad exigidas al prestador de servicios.
Responsable de Implementación	Bruce Wayne

Supervisor	Bruce Wayne
Fecha Límite	18 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.SEG.16 - Seguridad: Existe el riesgo de no poder recuperar la información que se haya podido eliminar accidental o intencionadamente
Control	C.RGPD.SAN.SEG.29 - Copias de seguridad, externalizadas o con medidas de contingencia.
Responsable de Implementación	Bruce Wayne
Supervisor	Bruce Wayne
Fecha Límite	18 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.SEG.16 - Seguridad: Existe el riesgo de no poder recuperar la información que se haya podido eliminar accidental o intencionadamente
Control	C.RGPD.SAN.SEG.30 - Realizar copias de seguridad, que incluya toda la información de la organización y se encuentren cifradas
Responsable de Implementación	Bruce Wayne
Supervisor	Bruce Wayne
Fecha Límite	18 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.SEG.26 - Seguridad en Redes y comunicaciones: Cuando el acceso se realiza a través de Internet, la comunicación se debe cifrar a través de protocolos criptográficos (TLS / SSL).
Control	C.RGPD.SAN.SEG.27 - Gestión de la configuración del cortafuegos. Control de tráfico de información. Comunicaciones remotas a través de redes privadas
Responsable de	Alfred Pennyworth

Implementación	
Supervisor	Bruce Wayne
Fecha Límite	12 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.SEG.26 - Seguridad en Redes y comunicaciones: Cuando el acceso se realiza a través de Internet, la comunicación se debe cifrar a través de protocolos criptográficos (TLS / SSL).
Control	C.RGPD.SAN.SEG.38 - Implementación de protocolos de cifrado de comunicaciones en todos los servicios con salida a internet
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	12 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.SEG.27 - Seguridad en Redes y comunicaciones: El tráfico hacia y desde el sistema de TI debe ser monitorizado y controlado a través de cortafuegos y sistemas de detección de intrusos
Control	C.RGPD.SAN.SEG.39 - Implementación de un firewall y de mecanismos IDS
Responsable de Implementación	
Supervisor	
Fecha Límite	
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.SEG.28 - Seguridad en Redes y comunicaciones: El acceso remoto al sistema de TI debería evitarse en general. En los casos en que esto sea absolutamente necesario, debe realizarse solo bajo el control y monitorización de una persona específica de la Organización, a través de VPN

Control	C.RGPD.SAN.SEG.40 - Implementación de VPN para accesos remotos al sistema
Responsable de Implementación	Alfred Pennyworth
Supervisor	Alfred Pennyworth
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.DEP.01 - Datos especialmente protegidos: Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso y específico cuando éste sea la causa que legitima el tratamiento o cesión de datos sensibles. Ej: no incluir casilla para consentimiento para el tratamiento de datos con fines de investigación o tratar datos religiosos sin consentimiento
Control	C.RGPD-AEPD.CEP.1.b - Establecer procedimientos que garanticen la obtención del consentimiento expreso (y por escrito cuando sea necesario) y que permitan probar que se cuenta con él.
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	12 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.DEP.02 - Datos especialmente protegidos: Asunción errónea de la existencia de una habilitación legal para el tratamiento o cesión de datos sensibles
Control	C.RGPD-AEPD.GEN.2.a - Formación apropiada del personal sobre protección de datos en el sector específico de que se trate
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	12 de diciembre de 2025

Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.DEP.02 - Datos especialmente protegidos: Asunción errónea de la existencia de una habilitación legal para el tratamiento o cesión de datos sensibles
Control	C.MAN.MIN.02 - El DPD revisará todos los formularios y funciones del SIHC para asegurar que solo se solicitan y procesan los datos personales estrictamente necesarios para cada finalidad específica (Minimización).
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	12 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.DEP.05 - Datos especialmente protegidos: Facilitar información sobre los pacientes a cualquier persona no autorizada o utilizando medios que no permitan la correcta identificación del destinatario (teléfono, etc…)
Control	C.RGPD-AEPD.SEG.6.e - Construir canales seguros y con verificación de identidad para la distribución de información de seguridad (códigos de usuario, contraseñas, etc.)
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.DEP.05 - Datos especialmente protegidos: Facilitar información sobre los pacientes a cualquier persona no autorizada o utilizando medios que no permitan la correcta identificación del destinatario (teléfono, etc…)
Control	C.RGPD-APDCAT.OBGL.15 - El registro de actividades de tratamiento deberá mantenerse actualizado en todo momento

Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.DEP.06 - Datos especialmente protegidos: No registrar los accesos a las Historias Clínicas
Control	C.RGPD-AEPD.SEG.4 - Establecer mecanismos de registro de acciones sobre los datos personales o logging así como herramientas fiables y flexibles de explotación de los ficheros de auditoría resultantes
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.DEP.06 - Datos especialmente protegidos: No registrar los accesos a las Historias Clínicas
Control	C.RGPD-APDCAT.OBGL.15 - El registro de actividades de tratamiento deberá mantenerse actualizado en todo momento
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.DEP.07 - Datos especialmente protegidos: Enviar información clínica, a través de redes de telecomunicaciones, sin cifrar
Control	C.RGPD.SAN.SEG.42 - Implementar mecanismos de trazabilidad que permitan, en este caso, tener controlados todos los accesos a

	esta información
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	20 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.DEP.07 - Datos especialmente protegidos: Enviar información clínica, a través de redes de telecomunicaciones, sin cifrar
Control	C.RGPD.SAN.SEG.43 - Implementar mecanismos de cifrado para el envío, a través de redes de telecomunicaciones, de información sensible
Responsable de Implementación	
Supervisor	
Fecha Límite	
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.DEP.09 - Datos especialmente protegidos: Existencia de errores técnicos u organizativos que propicien la falta de integridad de la información, permitiendo la existencia de registros duplicados o duplicidad de HC del mismo paciente, con informaciones diferentes o contradictorias, lo que puede derivar en la toma de decisiones erróneas Ej: que la aplicación que gestiona los datos de usuarios permita dar de alta dos usuarios con el mismo NIF
Control	C.MAN.CAL.01 - Control de Unicidad de Identidad: Implementar controles técnicos de unicidad en el nuevo SIHC de No problem S.L. para garantizar que no se pueden crear dos registros de paciente con el mismo NIF/Identificador Único, y realizar un proceso de depuración de duplicados en la fase de migración.
Responsable de Implementación	
Supervisor	

Fecha Límite	
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.DEP.10 - Datos especialmente protegidos: Falta de definición de los plazos de conservación de la distinta tipología de datos personales, en consonancia con el plazo de conservación de la HC
Control	C.RGPD-AEPD.CAL.8.a - Definir claramente los plazos de cancelación de todos los datos personales de los sistemas de información
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	27 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.DEP.10 - Datos especialmente protegidos: Falta de definición de los plazos de conservación de la distinta tipología de datos personales, en consonancia con el plazo de conservación de la HC
Control	C.RGPD-AEPD.CAL.8.b - Establecer controles automáticos dentro de los sistemas de información para avisar de la cercanía de los plazos de cancelación de la información
Responsable de Implementación	Alfred Pennyworth
Supervisor	Bruce Wayne
Fecha Límite	27 de diciembre de 2025
Completado (%)	0%

Escenario de Riesgo	RGPD.SAN.DEP.12 - Datos especialmente protegidos: No tener un procedimiento específico para la atención de las solicitudes de acceso a la Historia Clínica conforme a lo establecido en la Ley de Autonomía del Paciente y en la normativa autonómica
Control	C.RGPD.SAN.SEG.16 - Seguridad: Construir canales seguros y

	con verificación de identidad para la distribución de información de seguridad (códigos de usuario, contraseñas, etc.)
Responsable de Implementación	
Supervisor	
Fecha Límite	
Completado (%)	0%