Plantilla Modelo DPIA-FRIA

Índice

1. Descripción del proyecto en relación con el tratamiento de datos 4
1.1 Datos personales tratados 4
1.2 Procesos de tratamiento 5
1.3 Descripción y análisis del sistema de IA 7
1.4 Actores que intervienen en el tratamiento 12
2. Necesidad de llevar a cabo una EIPD y un FRIA 13
2.1 Necesidad de llevar a cabo una EIPD 13
2.2 Necesidad de llevar a cabo un FRIA 18
3. Evaluación de impacto en protección de datos 20
3.1 Necesidad y proporcionalidad 20
3.1.1 Finalidad del tratamiento 22
3.1.2 Principios de licitud 23
3.1.2.1 Base legal para el tratamiento 23
3.1.2.2 Tratamiento de datos de menores 24
3.1.2.3 Tratamiento de categorías especiales de datos 25
3.1.2.4 Tratamiento de datos penales 26
3.1.2.5 Validez del consentimiento 26
3.1.2.6 Transferencias de datos 27
3.1.2.7 Licitud del tratamiento para entrenar a la IA 28
3.1.3. Principio de lealtad del tratamiento 28
3.1.4 Principio de minimización 28
3.1.5 Principio de limitación del plazo de conservación 29
3.1.6 Principio de exactitud 30
3.1.7 Riesgos para las personas 30
3.1.8 Necesidad y proporcionalidad del tratamiento 32
3.1.9 Opinión de las personas interesadas 33
3.2 Controles para garantizar los derechos de las personas 35
3.2.1 Controles por el derecho a tener información transparente 35
3.2.2 Controles para el derecho de información 36
3.2.3 Controles para garantizar el derecho de acceso 38

3.2.4 Controles para garantizar el derecho de rectificación 39
3.2.5 Derecho de supresión 39
3.2.6 Derecho a limitar el tratamiento 40
3.2.7 Derecho a la portabilidad de los datos 41
3.2.8 Derecho de oposición 42
3.2.9 Derecho a no ser objeto de decisiones automatizadas 43
3.3. Riesgos en la seguridad de los datos 43
3.3.1 Impacto 44
3.3.2 Probabilidad inicial 46
3.3.3 Riesgo inicial 51
3.3.4 Controles de seguridad 51
3.3.5 Impacto residual 56
3.3.6 Probabilidad residual 58
3.3.7 Estimación del riesgo residual 62
4. Evaluación de impacto en los Derechos Fundamentales 63
4.1 Cuestionario de planificación y alcance 63
4.2 Matrices de riesgo 64
Tabla 1. Probabilidad 64
Tabla 2. Exposición 65
Tabla 3. Probabilidad de que se produzca un perjuicio (*likelihood*) 65
Tabla 4. Gravedad del perjuicio 65
Tabla 5. Esfuerzo para superar los perjuicios y revertir los efectos adversos 66
Tabla 6. Gravedad (*severity*) 66
Tabla 1A. Recogida de datos y análisis de riesgos 67
Tabla 7. Impacto general del riesgo 67
Tabla 2A. Gestión de riesgos (I) 67
Tabla 3A. Gestión de riesgos (II) 68

Esta plantilla de evaluación de impacto es un modelo que permite identificar y controlar los riesgos para los derechos y libertades de las personas, derivados del tratamiento de datos personales y del uso de la IA.

En algunos casos, una organización puede tener la obligación de realizar tanto la evaluación de impacto en la protección de datos (art. 35 RGPD) como también la evaluación de impacto en derechos fundamentales (art. 27 RIA). Para simplificar esta tarea, esta plantilla incluye unos apartados previos que son útiles para las dos evaluaciones: una descripción general del tratamiento, para determinar sus principales elementos; y las actividades que se van a desarrollar (identificadas de forma conjunta como «Proyecto»), incluido el uso de datos y de la IA que se ha previsto. El nivel de detalle debe ser suficiente para permitir evaluar los supuestos e indicadores de riesgo detallados.

Hay que tener en cuenta que el uso de la IA puede tener impacto en una o varias operaciones de tratamiento de datos de una actividad de tratamiento. Para poder evaluar correctamente los riesgos, es importante detectar los flujos y las interconexiones existentes en todo el ciclo de vida del tratamiento de los datos personales y, si procede, en el ciclo de vida del sistema de IA.

DESCRIPCIÓN GENERAL DEL PROYECTO

Descripción general del proyecto

¿Se utilizan datos personales?	☐ Sí ☐ No
¿Se utilizan datos recogidos con una finalidad distinta a la del tratamiento evaluado?	☐ Sí ☐ No
¿El tratamiento incorpora IA?	☐ Sí ☐ No

¿El proyecto utiliza prácticas prohibidas de IA establecidas en el artículo 5 del RIA?	☐ Sí ☐ No
Si se utiliza la IA, ¿a priori podría ese uso afectar a los derechos fundamentales de las personas afectadas o de terceros?	☐ Sí ☐ No
¿Es posible obtener los mismos resultados utilizando métodos menos intrusivos (por ejemplo, los datos sintéticos)?	☐ Sí ☐ No

¿En qué fase del ciclo de vida se encuentra el sistema de IA?	☐ Investigación ☐ Prueba de concepto ☐ Diseño ☐ Desarrollo ☐ Entrenamiento ☐ Validación ☐ Despliegue

1. Descripción del proyecto en relación con el tratamiento de datos

Es necesario realizar una descripción del tratamiento de datos personales y no personales lo más detallada posible, ya que será la base para evaluar la necesidad, la proporcionalidad y los riesgos del tratamiento.

Descripción detallada del tratamiento y del contexto

Finalidad del tratamiento

1.1 Datos personales tratados

Las características de los datos que se van a tratar son relevantes a la hora de determinar los riesgos de su tratamiento y el cumplimiento de algunas disposiciones del Reglamento.

Tipo de dato	
Fuente / Origen	
Plazo de conservación	

Tipo de dato	
¿Existen datos merecedores de especial protección? (económicos, violencia de género, subvenciones...)	☐ Sí ☐ No
¿Se utilizarán con un propósito distinto al de la recogida?	☐ Sí ☐ No
¿El tratamiento ofrece servicios de la sociedad de la información a niños y niñas y tiene como base el consentimiento?	☐ Sí ☐ No
¿Se tratan datos de categorías especiales o de colectivos vulnerables?	☐ Sí ☐ No
¿Se tratan datos relativos a condenas o infracciones penales?	☐ Sí ☐ No
Si se hace uso de IA, ¿el conjunto de datos de entrenamiento del modelo contiene datos personales o bien se han utilizado datos que se pueden considerar anónimos?	☐ Datos personales ☐ Anónimos
Si se utilizan datos personales, ¿el proveedor del sistema de IA ha llevado a cabo una EIPD?	☐ Sí ☐ No
[Proveedor de IA] En caso de usar un modelo entrenado a partir de un conjunto de datos que puede considerarse anónimo, ¿se ha evaluado el riesgo de reidentificación?	☐ Sí ☐ No
[Responsable del despliegue] En caso de uso de IA, ¿el conjunto de datos utilizado para contextualizar el funcionamiento del sistema (p. ej. afinamiento - *fine-tuning*) contiene datos personales (incluidos los obtenidos mediante raspado web - *web scraping*)?	☐ Sí ☐ No

1.2 Procesos de tratamiento

El objetivo de esta sección es identificar los distintos componentes del proceso cuando la IA se utilice en fases o funcionalidades distintas dentro de la misma finalidad general.

Proceso	
Descripción	
¿El proceso incorpora inteligencia artificial (sistema o componente)?	☐ Sí ☐ No

Proceso	
	(Consulte el apartado Descripción y análisis del sistema de IA)
Datos tratados	
Resultado del proceso	
Persona destinataria	
Lugar del tratamiento	

Proceso	
Descripción	
¿El proceso incorpora inteligencia artificial (sistema o componente)?	☐ Sí ☐ No (Consulte el apartado Descripción y análisis del sistema de IA)
Datos tratados	
Resultado del proceso	
Persona destinataria	
Lugar del tratamiento	

Proceso	
Descripción	
¿El proceso incorpora inteligencia artificial (sistema o componente)?	☐ Sí ☐ No (Consulte el apartado Descripción y análisis del sistema de IA)
Datos tratados	
Resultado del proceso	
Persona destinataria	
Lugar del tratamiento	

1.3 Descripción y análisis del sistema de IA

¿Qué tipo de sistema de IA es?	☐ Sistema de IA específico. Si se trata de una IA de propósito general, es necesario tener en cuenta el tipo de sistema desarrollado, así como las características y capacidades técnicamente viables ☐ Modelo de IA de propósito general (GPAI) (modelo que se puede utilizar para muchas tareas diferentes) ☐ Sistema basado en GPAI (aplicación construida a partir de un modelo de IA de propósito general) ☐ Sistema de IA generativa (IA capaz de generar contenido nuevo, como texto, imágenes, audio, vídeo, código, etc.) ☐ Sistema de IA agéntica (IA capaz de actuar de forma relativamente autónoma para alcanzar objetivos concretos) ☐ GPAI con riesgo sistémico (modelos de IA muy potentes, con impacto potencial amplio y con obligaciones adicionales según normativa) ☐ Otros. Especifique: _____

Tipología funcional	☐IA discriminativa o clasificadora (clasifica, categoriza o identifica patrones) ☐ IA predictiva (estima probabilidades, riesgos o eventos futuros) ☐ IA generativa (genera texto, imágenes, audio, vídeo, código u otros contenidos) ☐ IA agéntica (planifica, decide o ejecuta acciones con diferentes grados de autonomía) ☐ Sistema de recomendación o apoyo a la decisión (propone opciones, recomendaciones o decisiones) ☐ Sistema de detección de anomalías o fraude ☐ Sistema conversacional (chatbot, asistente virtual o copiloto) ☐ Sistema de visión artificial (procesa imágenes o vídeo) ☐ Sistema multimodal (combina texto, imagen, audio, vídeo u otras modalidades) ☐ Sistema robotizado o físico (robots, dispositivos inteligentes o vehículos autónomos) ☐ Otros. Especifique: _____
Grado de autonomía	☐ Asistencia al usuario (*human-in-the-loop*) ☐ Recomendación con validación humana obligatoria ☐ Ejecución semiautónoma ☐ Ejecución autónoma supervisada ☐ Ejecución autónoma sin intervención humana ☐ Otros. Especifique: _____

Arquitectura del sistema	☐ Modelo propio desarrollado o entrenado por la organización ☐ Modelo comercial de terceros ☐ Modelo de código abierto (*open source*) ☐ Sistema con ajuste (*fine-tuning*) ☐ Sistema basado en RAG (generación aumentada con recuperación de información) ☐ Sistema híbrido (combinación de varios modelos o tecnologías) ☐ Otros. Especifique: _____
Tecnologías de mejora de la privacidad (PETs)	☐ No se utilizan PET ☐ Anonimización ☐ Pseudonimización ☐ Privacidad diferencial ☐ Aprendizaje federado ☐ Cifrado homomórfico ☐ Computación multiparte segura (SMPC) ☐ Entornos de ejecución de confianza (TEE) ☐ Computación confidencial ☐ Datos sintéticos ☐ Pruebas de conocimiento cero (ZKP) ☐ Desaprendizaje automático (*machine unlearning*) ☐ Otros. Especifique: _____

Modalidades de datos procesados	☐ Texto ☐ Imágenes ☐ Audio ☐ Vídeo ☐ Documentos ☐ Datos estructurados (bases de datos, archivos, hojas de cálculo) ☐ Datos biométricos ☐ Datos de geolocalización ☐ Otros. Especifique: _____
Origen de los datos personales tratados por el sistema de IA	☐ Datos internos de la organización ☐ Datos facilitados por los usuarios ☐ Datos procedentes de otras administraciones o entidades ☐ Datos *abiertos (open data)* ☐ Raspado web (*web scraping*) ☐ Datos adquiridos a terceros ☐ Datos sintéticos ☐ Otros. Especifique: _____

¿Cuáles son las finalidades (objetivos específicos) del sistema de IA?	☐ Apoyo a la toma de decisiones humanas ☐ Generación de contenido o recomendaciones ☐ Clasificación o perfilado de personas ☐ Automatización de decisiones ☐ Automatización de procesos operativos ☐ Otros. Especifique: _____
[Proveedor de IA] ¿Las herramientas de IA utilizadas para el tratamiento de datos (por ejemplo, redes neuronales convolucionales profundas, máquinas de vectores de soporte, etc.) utilizan la menor cantidad posible de datos personales para el fin previsto?	☐ Sí ☐ No
[Proveedor de IA] ¿Se ha documentado, si procede, la necesidad de utilizar el aprendizaje automático, en particular el aprendizaje profundo?	☐ Sí ☐ No

[Proveedor de IA] ¿Se pueden tener en cuenta opciones de diseño de IA de cara a la protección de datos desde el diseño (aprendizaje federado, computación multipartita segura, cifrado homomórfico, etc.)?	☐ Sí ☐ No En caso afirmativo, ¿cuáles?
¿Cuáles son las principales características del sistema?	
Enumere los procesos del tratamiento con los que opera la IA (enlazar con el punto 1.2 Procesos de tratamiento)	
¿En qué países se ofrecerá?	
Identificación de los posibles titulares de derechos: ¿quiénes son los individuos o grupos que pueden verse afectados por los sistemas de IA? ¿Incluyen individuos o grupos vulnerables?	

1.4 Actores que intervienen en el tratamiento

Los actores que intervienen en el tratamiento, su función y los datos que tratan son importantes a la hora de determinar los riesgos del tratamiento.

		Rol a efectos del RIA	Rol a efectos del RGPD
Nombre		☐ Proveedor ☐ Responsable del despliegue	☐ Responsable ☐ Encargado
Procesos en los que interviene			
Descripción			

Nombre		☐ Proveedor ☐ Responsable del despliegue	☐ Responsable ☐ Encargado
Procesos en los que interviene			
Descripción			

Nombre		☐ Proveedor ☐ Responsable del despliegue	☐ Responsable ☐ Encargado
Procesos en los que interviene			
Descripción			

Nombre		☐ Proveedor ☐ Responsable del despliegue	☐ Responsable ☐ Encargado
Procesos en los que interviene			
Descripción			

Nombre		☐ Proveedor	☐ Responsable
Procesos en los que interviene		☐ Responsable del despliegue	☐ Encargado
Descripción			

2. Necesidad de llevar a cabo una EIPD y un FRIA

No es necesario realizar una EIPD (art. 35 RGPD), si es de aplicación alguno de los supuestos siguientes:

Supuesto	
El tratamiento tiene naturaleza, alcance, contexto y finalidad similar a otro tratamiento para el que ya se ha realizado una EIPD.	
El tratamiento tiene una base jurídica en el derecho de la UE o de un estado miembro, y ya se ha realizado una EIPD en el momento de adoptar esa base jurídica.	

Justificación

Si no se aplica ninguno de los supuestos anteriores pero el tratamiento puede comportar un riesgo grave para los derechos y libertades de las personas, es necesario realizar una EIPD.

2.1 Necesidad de llevar a cabo una EIPD

Ficha técnica de la EIPD	
Versión actual y registro de versiones (con la explicación del historial de los cambios realizados en la información contenida en la plantilla EIPD para este tratamiento, si los hubiere)	
El equipo implicado en esta EIPD (proporcionando detalles de sus roles, tareas, responsabilidades, etc.)	

Ficha técnica de la EIPD

Directrices, estándares, códigos de conducta y otros materiales de referencia utilizados para realizar esta EIPD.			
Razones para llevar a cabo la EIPD (se puede marcar más de una casilla de selección)	1. Nueva actividad de tratamiento, la EIPD probablemente será necesaria debido al alto riesgo (obligación según el artículo 35.3 RGPD):	Evaluación sistemática y extensa de los aspectos personales relacionados con las personas físicas basada en el tratamiento automatizado, incluido el perfilado, y en el que se basan decisiones que producen efectos legales sobre la persona física o que le afectan significativamente.	☐ Sí ☐ No
		Tratamiento a gran escala de categorías especiales de datos mencionadas en el artículo 9.1 RGPD o de datos personales relacionados con condenas penales y delitos mencionados en el artículo 10.	☐ Sí ☐ No
		Monitorización sistemática de un área de acceso público a gran escala.	☐ Sí ☐ No
	2. Nueva actividad de tratamiento, EIPD posiblemente requerida a causa de un probable alto riesgo (obligación legal, según la legislación nacional)	Justificación:	
	3. Nueva actividad de tratamiento, posiblemente requerida debido al probable alto riesgo (siguiendo al CEPD y las directrices nacionales):	Evaluación o puntuación, incluido perfilado y predicción, especialmente de los aspectos relacionados con el rendimiento laboral del sujeto, situación económica, salud, preferencias o intereses personales, fiabilidad o	☐ Sí ☐ No

		comportamiento, ubicación o movimientos.	
		Toma de decisiones automatizada con efecto legal o significativo similar: tratamiento que tiene como objetivo tomar decisiones sobre sujetos de datos que producen «efectos legales sobre la persona física» o que «afectan de forma similar a la persona física».	☐ Sí ☐ No
		Monitorización sistemática: tratamiento utilizado para observar, monitorear o controlar sujetos de datos, incluidos datos recogidos a través de redes o «una monitorización sistemática de un área accesible públicamente».	☐ Sí ☐ No
		Datos sensibles o datos de carácter altamente personal: esto incluye categorías especiales de datos personales, tal y como se definen en el artículo 9 (por ejemplo, información sobre las opiniones políticas de los individuos). También datos personales relacionados con condenas penales o delitos según la definición del artículo 10 RGPD.	☐ Sí ☐ No
		Datos tratados a gran escala, considerando el número de sujetos implicados, ya sea como un número específico o como una proporción de la población relevante: el volumen de datos y/o la gama de distintos elementos de datos que se están tratando; la duración, o permanencia, de la actividad de tratamiento	☐ Sí ☐ No

		de datos; la extensión geográfica de la actividad de tratamiento.	
		Comparación o combinación de conjuntos de datos.	☐ Sí ☐ No
		Datos sobre sujetos vulnerables (debido al desnivel de poder creciente entre los sujetos y el responsable de la información de datos, lo que significa que las personas quizá no puedan consentir fácilmente, oponerse al tratamiento de sus datos o ejercer sus derechos).	☐ Sí ☐ No
		Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas.	☐ Sí ☐ No
		Cuando el tratamiento en sí mismo «impide que los sujetos ejerzan un derecho o utilicen un servicio o un contrato».	☐ Sí ☐ No
		Otros (por ejemplo, lista nacional sobre las operaciones de tratamiento sujetas a los requisitos de una evaluación de impacto de protección de datos)	Indique cuáles:
	4. Nueva actividad de tratamiento, EIPD necesaria o beneficiosa	Opinión o recomendación del DPD	☐ Sí ☐ No
		Opinión o recomendación de los sujetos de datos (o de sus representantes).	☐ Sí ☐ No

Ficha técnica de la EIPD

		Exigida por un código de conducta, estándar, buenas prácticas, etc.	☐ Sí ☐ No
		Otros (por ejemplo, gestionar riesgos o demostrar responsabilidad y construir confianza).	Indique cuáles:
	5. Actividades de tratamiento de alto riesgo existentes, para las que ha habido un cambio en los riesgos:	El tratamiento de datos ha cambiado.	☐ Sí ☐ No
		El contexto organizativo o social de la actividad de tratamiento ha cambiado.	☐ Sí ☐ No
		¿Cómo?	
Alcance de esta EIPD (qué se ha considerado y qué se ha dejado fuera de la evaluación, y por qué).			
Fecha de finalización			
Fecha de validación formal (aprobación como completa y terminada por un funcionario responsable de la EIPD)			
¿La EIPD (o partes de ésta) está pensada para ser publicada o compartida externamente?	☐ No	☐ Sí, se publicará. ¿Cómo?	☐ Sí, se compartirá externamente. ¿Cómo?

¿Es necesario hacer la EIPD? ☐ Sí ☐ No

Justificación:

Si se ha nombrado un DPD, debe considerarse su opinión respecto a la necesidad de hacer una EIPD.

Opinión del DPD respecto a la necesidad de realizar una EIPD

2.2 Necesidad de llevar a cabo un FRIA

A continuación, se indican los requisitos de necesidad a efectos del artículo 27 RIA. Sin embargo, la evaluación del impacto sobre los derechos fundamentales también forma parte del sistema de gestión de riesgos que se indica en el artículo 9 y que los proveedores de IA deben adoptar, para lo que se puede utilizar el modelo FRIA.

Ámbito objetivo	¿El sistema está clasificado como alto riesgo según el artículo 6.2 RIA? (art. 27.1)	☐ Sí ☐ No
	¿No es un sistema de IA destinado a utilizarse como componente de seguridad en la gestión y funcionamiento de infraestructuras digitales críticas, tráfico de vehículos o suministro de agua, gas, calefacción o electricidad?	☐ Sí ☐ No
	¿El sistema está incluido en alguno de los ámbitos enumerados en los puntos 1 y del 3 al 8 del anexo III?	☐ Sí ☐ No
		¿Cuál?

Ámbito subjetivo	El responsable del despliegue de sistemas de IA de alto riesgo es un organismo de derecho público:	☐ Sí ☐ No	
	El responsable del despliegue de sistemas de IA de alto riesgo es una entidad privada que presta servicios públicos:	☐ Sí ☐ No	
	El responsable del despliegue es alguno de los que se mencionan en el anexo III, punto 5, letras *b* y *c*.	☐ Sí ☐ No	
		¿Cuál?	
Cuestiones generales	¿Es el primer uso del sistema de IA?	☐ Sí ☐ No	
	¿Existe un FRIA previo para el mismo sistema o uno similar?	☐ Sí ☐ No	
	¿El proveedor ha facilitado una evaluación de impacto FRIA reutilizable?	☐ Sí ☐ No	
	En caso afirmativo, qué elemento ha cambiado o ha dejado de estar actualizado que justifique la necesidad de rehacer el FRIA	La finalidad	☐ Sí ☐ No
		El contexto de uso	☐ Sí ☐ No
		Los procesos	☐ Sí ☐ No
		Las categorías de personas afectadas / colectivos	☐ Sí ☐ No
		La frecuencia o intensidad de uso	☐ Sí ☐ No
		Los riesgos potenciales	☐ Sí ☐ No

		La supervisión humana	☐ Sí ☐ No

Si hay respuestas afirmativas (sí) a las preguntas relativas al ámbito objetivo y/o al ámbito subjetivo, hay que efectuar un FRIA.

Si (i) ya se ha efectuado un FRIA previamente o (ii) existe un FRIA del proveedor que ya cubre todos los riesgos relevantes, no es necesario efectuar un nuevo FRIA. Esto es así siempre y cuando todos los riesgos se hayan analizado en relación al contexto de uso y no haya habido cambios.

En relación con la EIPD (art. 27.3 RIA)	¿Existe una EIPD conforme al artículo 35 RGPD relacionada con el sistema?	☐ Sí ☐ No
	¿Qué partes es necesario complementar con un FRIA?	

3. Evaluación de impacto en protección de datos

3.1 Necesidad y proporcionalidad

La evaluación de la necesidad y la proporcionalidad del tratamiento se realiza en relación con la finalidad del tratamiento, que se ha descrito en la sección anterior.

Necesidad y proporcionalidad desde la perspectiva del SIA	Necesidad social o de política pública	¿El sistema aporta algún beneficio directo a «la humanidad»? (considerando 27)	☐ Sí ☐ No
		¿Contribuye a objetivos públicos (equidad, transparencia, accesibilidad, eficiencia)?	☐ Sí ☐ No
		¿Responde a problemas estructurales (saturación de servicios, falta de personal, etc.)?	☐ Sí ☐ No
		¿El sistema es socialmente aceptable y comprensible para los usuarios afectados?	☐ Sí ☐ No
	Evaluación inspirada en políticas públicas	¿Qué problema o necesidad concreta quiere resolverse con este sistema de IA?	
		¿Por qué ese problema es relevante o crítico para la organización?	
		¿Qué soluciones no algorítmicas o tradicionales existen actualmente?	
		¿Justifica por qué el “no hacer nada” (o mantener la situación actual) no es una opción y qué beneficios específicos aporta la IA (eficiencia, precisión, escalabilidad)?	
	Necesidad de utilizar el tipo concreto de IA seleccionado	¿Existen alternativas igual de efectivas con menor impacto en derechos?	☐ Sí ☐ No
		En caso afirmativo, ¿por qué no sería suficiente una IA de bajo riesgo o un sistema más simple, o bien por qué se ha descartado la alternativa tecnológica «más simple»?	Justificación

		¿El nivel de automatización es realmente necesario para lograr la finalidad?	☐ Sí ☐ No

3.1.1 Finalidad del tratamiento

En principio, los datos recogidos se utilizan para lograr la finalidad del tratamiento que motivó la recogida. Ahora bien, en algunos casos el Reglamento permite el tratamiento de datos que se han recogido con una finalidad distinta.

¿Se utilizan datos recogidos con una finalidad distinta a la del tratamiento original?	☐ Sí ☐ No

En caso afirmativo

Las condiciones siguientes permiten el tratamiento de los datos con una finalidad distinta a la de la recogida.	
Se ha obtenido el consentimiento de las personas interesadas para el tratamiento con la nueva finalidad.	☐ Sí ☐ No
El tratamiento se basa en el derecho de la Unión o de los Estados miembros que constituye una medida para salvaguardar:	
La seguridad nacional.	☐ Sí ☐ No
La defensa.	☐ Sí ☐ No
La seguridad pública.	☐ Sí ☐ No
La prevención, la investigación, la detección y el tratamiento de delitos penales.	☐ Sí ☐ No
Otros objetivos importantes de interés público.	☐ Sí ☐ No
La protección de la independencia judicial y de los procedimientos judiciales.	☐ Sí ☐ No

En caso afirmativo

La prevención, la investigación, la detección y el tratamiento de infracciones en normas deontológicas.	☐ Sí ☐ No
La protección de la persona interesada o de los derechos y libertades de terceros.	☐ Sí ☐ No
La ejecución de demandas civiles.	☐ Sí ☐ No

Si no se aplica ninguna de las condiciones anteriores, es necesario que la nueva finalidad sea compatible con la finalidad que motivó la recogida de los datos.

Finalidad inicial.	
Datos.	
Nueva finalidad.	
Justificación de la compatibilidad.	

Finalidad inicial.	
Datos.	
Nueva finalidad.	
Justificación de la compatibilidad.	

3.1.2 Principios de licitud

3.1.2.1 Base legal para el tratamiento

Un tratamiento es lícito si se aplica alguna de las bases legales siguientes:

La persona interesada ha dado su consentimiento para el tratamiento de sus datos personales, para una o varias finalidades específicas.	☐ Sí ☐ No
El tratamiento es necesario para ejecutar un contrato en el que la persona interesada es parte o para aplicar medidas precontractuales.	☐ Sí ☐ No

La persona interesada ha dado su consentimiento para el tratamiento de sus datos personales, para una o varias finalidades específicas.	☐ Sí ☐ No
El tratamiento es necesario para cumplir con una obligación legal aplicable al responsable del tratamiento.	☐ Sí ☐ No
El tratamiento es necesario para proteger intereses vitales de la persona interesada o de otra persona física.	☐ Sí ☐ No
El tratamiento es necesario para cumplir una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.	☐ Sí ☐ No
El tratamiento es necesario para satisfacer los intereses legítimos del responsable del tratamiento o de un tercero, siempre que no prevalezcan los intereses o derechos y libertades fundamentales de la persona interesada (especialmente, cuando es un menor).	☐ Sí ☐ No

Justificación de la licitud del tratamiento.

Además, es necesario que el tratamiento no incurra en ningún ilícito en un sentido más amplio. Por ejemplo, infringir el copyright o acuerdos contractuales.

Confirma que el tratamiento no incurre en ningún tipo de ilícito.

3.1.2.2 Tratamiento de datos de menores

Los menores necesitan una protección especial en el tratamiento de sus datos, porque pueden no ser conscientes de los riesgos que comporta .

¿El tratamiento ofrece servicios de la sociedad de la información a niños y niñas y tiene como base el consentimiento?	☐ Sí ☐ No
En caso afirmativo, ¿se ha tenido en cuenta la edad mínima de consentimiento?	☐ Sí ☐ No
¿Se utilizan los datos del menor para elaborar perfiles y/o para tomar decisiones total o parcialmente automatizadas a partir de ellos?	☐ Sí ☐ No

¿El tratamiento ofrece servicios de la sociedad de la información a niños y niñas y tiene como base el consentimiento?	☐ Sí ☐ No

3.1.2.3 Tratamiento de categorías especiales de datos

¿Se tratan datos de categorías especiales?	☐ Sí ☐ No

En caso afirmativo

El tratamiento de categorías especiales de datos está prohibido, salvo que se aplique alguno de los supuestos siguientes.	
La persona interesada ha dado su consentimiento explícito para el tratamiento con una finalidad específica, salvo que el derecho de la UE o del Estado miembro no lo permita.	☐ Sí ☐ No
El tratamiento es necesario para cumplir obligaciones o para ejercer derechos en el ámbito del derecho laboral y de la seguridad y la protección social.	☐ Sí ☐ No
El tratamiento es necesario para proteger intereses vitales de la persona interesada o de otra persona física, en el supuesto de que la persona interesada no esté capacitada para dar el consentimiento.	☐ Sí ☐ No
El tratamiento es legítimo y con garantías, realizado por una asociación sin ánimo de lucro de carácter político, filosófico, religioso o sindical, siempre que el tratamiento afecte a personas con quienes mantienen contactos en relación con esas finalidades y que los datos no se comuniquen a terceros sin el consentimiento de las personas interesadas.	☐ Sí ☐ No
El tratamiento hace referencia a datos que la persona interesada ha hecho manifiestamente públicos.	☐ Sí ☐ No
El tratamiento es necesario para formular, ejercer o defender reclamaciones, o cuando los tribunales actúan en su función judicial.	☐ Sí ☐ No
El tratamiento es necesario por razones de interés público esencial.	☐ Sí ☐ No
El tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social.	☐ Sí ☐ No
El tratamiento es necesario por razones de interés público en el ámbito de la salud pública.	☐ Sí ☐ No

En caso afirmativo

El tratamiento es necesario para finalidades de archivo con interés público, investigación científica o histórica, o con finalidad estadística.	☐ Sí ☐ No
[Proveedor de IA] ¿ El tratamiento es necesario para detectar y corregir los sesgos asociados a los sistema de IA de alto riesgo, de acuerdo con el artículo 10.5 RIA?	☐ Sí ☐ No
[Responsable del despliegue / Proveedor de IA] En caso afirmativo, ¿se han establecido medidas para evitar la recuperación de los datos personales utilizados en el momento de usar el sistema de IA?	☐ Sí ☐ No

Justificación de la licitud del tratamiento de datos de categorías especiales

3.1.2.4 Tratamiento de datos penales

¿Se tratan datos relativos a condenas o infracciones penales?	☐ Sí ☐ No

En caso afirmativo

Aunque los datos relativos a condenas o infracciones penales no son categorías especiales de datos, existe un requisito adicional para tratarlos: el tratamiento sólo se puede llevar a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el derecho de la Unión o del estado miembro.

Justificación de la licitud del tratamiento de datos penales

3.1.2.5 Validez del consentimiento

Si un tratamiento tiene como base legal el consentimiento, es necesario que se cumplan las condiciones siguientes para que éste sea válido:

El responsable puede demostrar que lo ha recogido.	☐ Sí ☐ No
La solicitud de consentimiento es inteligible, de fácil acceso y en lenguaje claro.	☐ Sí ☐ No
La ejecución de un contrato no puede supeditarse a recibir el consentimiento respecto de datos personales no necesarios para ejecutar el contrato.	☐ Sí ☐ No
Se ha informado a las personas interesadas de la posibilidad de retirar el consentimiento en cualquier momento.	☐ Sí ☐ No
Si la persona interesada no quiere consentir, se le ofrece una opción alternativa que no le perjudica ni implica trato desfavorable.	☐ Sí ☐ No

3.1.2.6 Transferencias de datos

Para evitar que las personas interesadas vean reducidos sus derechos, el RGPD es especialmente restrictivo con las transferencias de datos a países donde el RGPD no se aplica.

¿Se realizan transferencias a terceros países o a organizaciones internacionales?	☐ Sí ☐ No

En caso afirmativo

Estas transferencias están permitidas si la Comisión Europea considera que el país u organización ofrece un adecuado nivel de protección, si se han establecido las garantías suficientes según el artículo 46 o si se aplica alguna de las excepciones del artículo 49.

Datos transferidos.	
País.	
Condición que permite la transferencia.	

Datos transferidos.	
País.	
Condición que permite la transferencia.	

3.1.2.7 Licitud del tratamiento para entrenar a la IA

[Proveedor de IA] Si se reutilizan datos disponibles públicamente o datos obtenidos de un tercero (por ejemplo, un proveedor de datos) para entrenar a la IA, ¿se comprueba que no se esté reutilizando un conjunto de datos que se haya creado claramente de forma ilícita?	☐ Sí ☐ No
¿La fuente de los datos está claramente identificada y documentada?	☐ Sí ☐ No
¿El conjunto de datos es el resultado de un delito o una infracción (filtración, robo, etc.) o ha sido objeto de una condena o sanción pública por parte de una autoridad competente y, como consecuencia, se ha tenido que retirar o prohibido su uso?	☐ Sí ☐ No
¿Las condiciones en las que se recogieron los datos están suficientemente documentadas?	☐ Sí ☐ No
¿El conjunto de datos contiene información sensible o que infrinja derechos? Si es así, ¿se hacen comprobaciones exhaustivas para garantizar que el tratamiento es lícito?	☐ Sí ☐ No

3.1.3. Principio de lealtad del tratamiento

Un tratamiento es leal si hace un uso de los datos previsible por parte de las personas interesadas, y si del tratamiento no se derivan consecuencias adversas para las personas interesadas que no sean justificables.

Justificación del tratamiento leal

3.1.4 Principio de minimización

Los datos deben ser adecuados, relevantes y limitados a lo estrictamente necesario para cumplir la finalidad del tratamiento.

Tipo de datos.	

Justificación de la adecuación, la relevancia y la necesidad

Tipo de datos.	
Tipo de datos.	

Justificación de la adecuación, la relevancia y la necesidad

3.1.5 Principio de limitación del plazo de conservación

Los datos personales no deben conservarse más tiempo del estrictamente necesario para cumplir con la finalidad del tratamiento. En la descripción del tratamiento, se especificó el plazo de conservación de los datos. Es necesario justificar que los plazos dados cumplen el principio de limitación del plazo de conservación.

Justificación de que los plazos de conservación dados cumplen con la limitación del plazo de conservación

¿Es necesario que los mecanismos establecidos para borrar los datos sean efectivos (es automático o debe activarse manualmente? ¿Permanecen los datos en las copias de seguridad del sistema una vez borrados? ¿Cuánto tiempo y cómo se garantiza que no se tratan?

Describe los mecanismos establecidos para borrar los datos

Los datos pueden conservarse indefinidamente con finalidad de archivo en interés público, con finalidad de investigación científica o histórica, o con finalidad estadística.

Se conservan datos con finalidad de archivo en interés público, con finalidad de investigación científica o histórica, o con finalidad estadística.	

En caso afirmativo, qué medidas se han implantado para garantizar el principio de minimización

Se conservan datos con finalidad de archivo en interés público, con finalidad de investigación científica o histórica, o con finalidad estadística.	

3.1.6 Principio de exactitud

El tratamiento de datos inexactos puede afectar negativamente a las personas. El principio de exactitud pide que los datos sean exactos y que se tomen las medidas adecuadas para garantizar que los que sean inexactos se actualicen o borren sin dilación.

Controles de la calidad de los datos[1]

Medidas para corregir los datos

3.1.7 Riesgos para las personas

El objetivo de este punto es identificar los posibles efectos negativos sobre las personas, cuantificarlos y, si es necesario, proponer medidas para mitigarlos.

En esta sección evaluaremos el tratamiento tal y como se ha diseñado. Es decir, no consideramos los casos en los que falla la seguridad del sistema (sea ese fallo accidental o intencionado).

En la identificación de los potenciales efectos negativos del tratamiento sobre las personas conviene tener en cuenta el punto de vista de las personas interesadas y del delegado de protección de datos.

[1] Incluye la fase de entrenamiento de los modelos de IA

Potenciales efectos negativos del tratamiento sobre las personas

Por cada uno de los efectos negativos identificados, es necesario estimar el nivel de riesgo asociado. El riesgo depende de dos factores: el impacto que tiene sobre las personas (bajo, medio, alto o muy alto) y la probabilidad de que se materialice (baja, media, alta). El impacto se estima directamente a partir de los efectos potenciales. Para determinar la probabilidad, es necesario analizar qué circunstancias hacen que los efectos negativos se materialicen (las amenazas) y estimar su probabilidad.

El riesgo se determina, en función del impacto y de la probabilidad, conforme a la tabla siguiente:

	Impacto			
Probabilidad	Bajo	Medio	Alto	Muy alto
Baja	Riesgo bajo	Riesgo bajo	Riesgo medio	Riesgo alto
Media	Riesgo bajo	Riesgo medio	Riesgo alto	Riesgo alto
Alta	Riesgo medio	Riesgo alto	Riesgo alto	Riesgo alto

Primero se estimará el riesgo asociado a cada amenaza. El riesgo global será el máximo de los riesgos de las amenazas.

Efecto sobre las personas

Impacto:

Amenaza	Probabilidad	Riesgo

Riesgo estimado

Efecto sobre las personas		
Impacto:		
Amenaza	Probabilidad	Riesgo

Riesgo estimado:

Salvo que el riesgo sea bajo, será necesario buscar medidas para reducirlo. Esto es especialmente necesario en los casos de riesgo alto o muy alto. Si no es posible reducir un riesgo alto, antes de empezar el tratamiento se debe consultar a la autoridad de protección de datos competente sobre la idoneidad del tratamiento.

En caso de que se haya alterado el tratamiento inicial para hacerlo menos lesivo para las personas, será necesario revisar y actualizar las secciones anteriores de la EIPD.

Derechos/libertades afectados	Probabilidad	Gravedad	Impacto global	Medidas para prevenir/mitigar el impacto

3.1.8 Necesidad y proporcionalidad del tratamiento

Con la información recogida en esta sección, es necesario justificar que el tratamiento es necesario (el propósito buscado no se puede alcanzar con ninguna otra medida más moderada) y proporcional (no provoca más daños que beneficios).

Justificación de la idoneidad del tratamiento para el propósito que se busca

Justificación de la necesidad del tratamiento

Justificación de que el tratamiento es proporcional

3.1.9 Opinión de las personas interesadas

El RGPD establece que, si es posible, es necesario recoger la opinión de las personas interesadas sobre el tratamiento.

Opinión de las personas interesadas sobre la necesidad y la proporcionalidad del tratamiento

En el caso de que no se considere apropiado recoger la opinión de las personas interesadas, debe justificarse.

¿Por qué no se ha recogido la opinión de las personas interesadas?

Si la opinión de las personas interesadas respecto al tratamiento difiere de la visión que el responsable ha dado en el apartado 2.7 y se pretende llevar adelante el tratamiento, debe justificarse el porqué.

¿Por qué se lleva adelante el tratamiento a pesar de las discrepancias de las personas interesadas?

3.2 Controles para garantizar los derechos de las personas

3.2.1 Controles por el derecho a tener información transparente

La transparencia es transversal y debe estar presente en todas las comunicaciones con las personas interesadas.

Toda comunicación con las personas interesadas debe ser concisa, inteligible, de fácil acceso y debe hacer uso de un lenguaje claro y sencillo.	☐ Sí ☐ No

El reglamento regula cómo debe hacerse esta comunicación.

La información se dará por escrito (incluyendo medios electrónicos).	☐ Sí ☐ No
En caso de peticiones hechas con medios electrónicos, la información se dará preferentemente de forma electrónica.	☐ Sí ☐ No
Si la persona interesada lo solicita, la información se dará oralmente.	☐ Sí ☐ No

El responsable debe responder a las peticiones de ejercicio de los derechos de una persona interesada dentro de unos plazos establecidos:

Sin demora indebida y no más allá de un mes.	☐ Sí ☐ No
Si la complejidad o el número de peticiones lo justifica, puede extenderse el período en dos meses. En ese caso, es necesario informar de las razones dentro del primer mes.	☐ Sí ☐ No

Si el responsable no debe responder a la petición de ejercicio de derechos de una persona interesada, es necesario:

Avisar a la persona interesada de este hecho sin demora indebida y como máximo en un mes.	☐ Sí ☐ No
Explicar las razones para no realizar la petición (por ejemplo, la petición es repetitiva o el responsable no puede identificar a la persona interesada).	☐ Sí ☐ No
Informar de la posibilidad de recurrir la decisión ante una autoridad supervisora o un juzgado.	☐ Sí ☐ No

Sólo si la petición es excesiva (por ejemplo, por repetitiva), se podrá cobrar un cargo para cubrir los costes de tramitarla.	☐ Sí ☐ No

3.2.2 Controles para el derecho de información

A la hora de recoger datos personales, el responsable del tratamiento debe informar a las personas interesadas de diferentes aspectos del tratamiento.

[Responsable del despliegue] ¿El proveedor del sistema de IA ha facilitado la información necesaria para cumplir el deber de informar a las personas interesadas de manera adecuada?[2]	☐ Sí ☐ No

Los artículos 13 y 14 especifican que es necesario informar a las personas interesadas de los puntos que se detallan en la tabla siguiente:

La identidad y los datos de contacto del responsable.	☐ Sí ☐ No
Los datos de contacto del delegado de protección de datos (si hay).	☐ Sí ☐ No
La finalidad del tratamiento.	☐ Sí ☐ No
La base legal del tratamiento.	☐ Sí ☐ No
El interés legítimo del responsable, si esa es la base legal del tratamiento.	☐ Sí ☐ No
Los destinatarios o categorías de destinatarios de los datos.	☐ Sí ☐ No
El plazo de conservación de los datos o el criterio empleado para determinarlo.	☐ Sí ☐ No
La intención de transmitir los datos fuera de la UE, en su caso.	☐ Sí ☐ No
La decisión de la Comisión Europea respecto a la suficiencia de la seguridad que ofrece el país o la organización destinataria.	☐ Sí ☐ No
La existencia del derecho de acceso a los datos.	☐ Sí ☐ No
La existencia del derecho de rectificación y supresión.	☐ Sí ☐ No
La existencia del derecho de limitación del tratamiento.	☐ Sí ☐ No
La existencia del derecho de oposición al tratamiento.	☐ Sí ☐ No
La existencia del derecho de portabilidad de datos.	☐ Sí ☐ No

[2] Este punto cobra especial relevancia para cumplir correctamente con las obligaciones establecidas en el artículo 86 del RIA.

La identidad y los datos de contacto del responsable.	☐ Sí ☐ No
La existencia del derecho a revocar el consentimiento (si esa es la base legal del tratamiento).	☐ Sí ☐ No
La existencia del derecho a presentar reclamación ante una autoridad de control.	☐ Sí ☐ No
Que la comunicación de los datos es un requisito legal o contractual, si procede.	☐ Sí ☐ No
La existencia de decisiones automatizadas.	☐ Sí ☐ No
El propósito de utilizar datos con una finalidad distinta a la que motivó la recogida, en su caso.	☐ Sí ☐ No
La procedencia de los datos, si no se han obtenido directamente de la persona interesada.	☐ Sí ☐ No

Existen algunas exenciones a la obligatoriedad de informar, que dependen de la forma en que se han recogido los datos.

- Si los datos se han obtenido directamente de la persona interesada, no existe la obligación de informarla si ya dispone de la información.
- Si los datos no se han obtenido directamente de la persona interesada, no es necesario informarle si se da alguna de las condiciones siguientes: la persona interesada ya dispone de esta información; la comunicación es imposible o supone un esfuerzo desproporcionado; está regulado así en una norma de la UE o de los estados miembros; o la información tiene carácter confidencial sobre la base del secreto profesional.

Si no se informa, debe justificarse.

¿Se aplica el derecho de información a todos los datos tratados?	

Si se aplica alguna exención al derecho de información, es necesario decir cuál, en qué datos y justificar el porqué

Si se informa a las personas interesadas, el Reglamento determina cuándo hay que hacerlo[3].

[3] RGPD art. 13(1) y 14(3),

Si los datos se recogen directamente de las personas interesadas, en el momento de recogerlos.	☐ Sí ☐ No
Si los datos se recogen indirectamente, es necesario cumplir las condiciones siguientes:	
En un período razonable de tiempo y no superior a un mes.	☐ Sí ☐ No
Si nos comunicamos con las personas interesadas, a más tardar en el momento de la primera comunicación.	☐ Sí ☐ No
Si se desea comunicar los datos a terceros, antes de comunicarlos.	☐ Sí ☐ No

3.2.3 Controles para garantizar el derecho de acceso

La persona interesada tiene el derecho de obtener del responsable del tratamiento la confirmación de que se están tratando sus datos y, en ese caso, el derecho de acceso a los datos personales y a la información siguiente:

La finalidad del tratamiento.	☐ Sí ☐ No
Las categorías de datos tratados.	☐ Sí ☐ No
Las personas destinatarias de los datos.	☐ Sí ☐ No
El plazo de conservación de los datos.	☐ Sí ☐ No
Los derechos de rectificar y suprimir los datos.	☐ Sí ☐ No
Los derechos de limitar y oponerse al tratamiento.	☐ Sí ☐ No
El derecho a reclamar ante una autoridad de control.	☐ Sí ☐ No
Si los datos no se han obtenido de la persona interesada, el origen de los datos.	☐ Sí ☐ No
La existencia de decisiones automatizadas, en su caso.	☐ Sí ☐ No
Garantías en la transferencia de datos fuera de la UE, en su caso.	☐ Sí ☐ No

Aparte de saber qué información debe transmitirse a las personas interesadas, es necesario asegurarse de que se dan las condiciones para hacer efectivo el derecho de acceso.

¿Se ha establecido un procedimiento estándar para la gestión de solicitudes de acceso?	☐ Sí ☐ No
¿El personal que trata con las personas interesadas tiene la formación necesaria para reconocer las solicitudes de acceso?	☐ Sí ☐ No

3.2.4 Controles para garantizar el derecho de rectificación

Las personas tienen derecho a que se rectifiquen sus datos si no son exactos.

¿Se ha establecido un procedimiento para la gestión de solicitudes de rectificación?	☐ Sí ☐ No
¿El personal que trata con las personas interesadas tiene la formación necesaria para reconocer las solicitudes de rectificación?	☐ Sí ☐ No

Si el responsable ha compartido los datos, debe informar a las personas destinatarias sobre la rectificación.

¿Se ha establecido un procedimiento para notificar la rectificación a las personas destinatarias?	☐ Sí ☐ No

3.2.5 Derecho de supresión

Las personas tienen derecho a que se borre su información cuando se da alguno de los casos siguientes:

- Los datos ya no son necesarios en relación con la finalidad para la que se recogieron.
- La persona interesada retira su consentimiento y no existe otra base legal para el tratamiento.
- La persona interesada se opone al tratamiento y no existe otro factor superior que lo legitime.
- Los datos se han tratado sin una base legal.
- Los datos deben borrarse conforme a una obligación legal que afecta al responsable.
- Los datos se utilizan para ofrecer servicios de la sociedad de la información a niños y niñas.

En cambio, el derecho de supresión no se aplica en los casos siguientes:

- Para ejercer el derecho a la libertad de expresión y de información.
- Para cumplir una obligación legal o en el interés público.

- Con la finalidad de archivo en interés público, con finalidad de investigación científica o histórica y con finalidad estadística (si el cumplimiento de estos fines se viera afectado por la supresión de los datos).
- Para presentar, ejercer o defender reclamaciones legales.

¿El personal tiene capacidad para decidir si se aplica el derecho de supresión?	☐ Sí ☐ No

Es recomendable establecer un canal estándar para que las personas interesadas puedan pedir hacer efectivo el derecho de supresión. Ahora bien, es necesario asegurarse de que el personal está capacitado para detectar las solicitudes que se hagan por otros medios.

¿Se ha establecido un procedimiento para la gestión de solicitudes de supresión?	☐ Sí ☐ No
¿El personal que trata con las personas interesadas tiene la formación necesaria para reconocer las solicitudes de supresión?	☐ Sí ☐ No

Si el responsable del tratamiento comparte los datos, debe tomar las medidas apropiadas (teniendo en cuenta los costes y la tecnología disponible) para notificar a las personas destinatarias sobre la petición de supresión.

¿Se ha establecido un procedimiento para notificar la petición de supresión a las personas destinatarias?	☐ Sí ☐ No

3.2.6 Derecho a limitar el tratamiento

El artículo 18 otorga a las personas el derecho a limitar el tratamiento de sus datos, en los casos siguientes:

- La persona interesada ha pedido la rectificación de sus datos y el responsable está verificando si son exactos.
- Los datos se han tratado sin una base legal.
- La persona interesada necesita que el responsable guarde los datos para iniciar, ejercer o defender una reclamación.
- La persona interesada se ha opuesto al tratamiento y el responsable está evaluando si los motivos legítimos del responsable prevalecen sobre los de la persona interesada.

¿El personal está capacitado para decidir si se aplica el derecho a limitar el tratamiento?	☐ Sí ☐ No

Hay que asegurarse de que el personal esté capacitado para detectar las solicitudes de limitación del tratamiento.

¿Se ha establecido un procedimiento para la gestión de solicitudes de limitación del tratamiento?	☐ Sí ☐ No
¿El personal que trata con las personas interesadas tiene la formación necesaria para reconocer las solicitudes de limitación del tratamiento?	☐ Sí ☐ No

A la hora de limitar el tratamiento, es necesario tener en cuenta las diferentes formas que puede tener: recogida de datos, análisis de datos, diseminación de resultados, etc.

¿Se tienen en cuenta todas las posibles formas de tratamiento a la hora de limitarlo?	☐ Sí ☐ No

Si se han compartido datos, es necesario informar a las personas destinatarias de las peticiones de limitación del tratamiento.

¿Se ha establecido un procedimiento para notificar la petición de limitación del tratamiento a las personas destinatarias?	☐ Sí ☐ No

3.2.7 Derecho a la portabilidad de los datos

Las personas tienen derecho a pedir los datos que han facilitado al responsable del tratamiento en los casos siguientes:

- Si el tratamiento se basa en el consentimiento, o es necesario para ejecutar un contrato o aplicar medidas precontractuales.
- El tratamiento se realiza mediante medios automatizados.

El derecho a la portabilidad de datos no se limita a los datos que las personas han dado de forma explícita; también afecta a los datos que se han recogido de la observación de las personas.

¿El personal está capacitado para decidir si se aplica el derecho a la portabilidad de datos?	☐ Sí ☐ No

El derecho a la portabilidad de datos no debe afectar negativamente a otras personas. En particular:

- Si los datos personales contienen información de una tercera persona, es necesario evaluar si esta última puede ver afectados sus derechos y libertades.
- Si los datos están asociados a varias personas (por ejemplo, una cuenta bancaria compartida), es necesario buscar el consenso de todas las personas interesadas.

¿El procedimiento para hacer efectivo el derecho a la portabilidad de datos tiene en cuenta el efecto sobre los derechos y libertades de las demás personas?	☐ Sí ☐ No

Debe asegurarse de que el personal esté capacitado para detectar las solicitudes de portabilidad de datos.

¿Se ha establecido un procedimiento para la gestión de solicitudes de portabilidad de datos?	☐ Sí ☐ No
¿El personal que trata con las personas interesadas tiene la formación necesaria para reconocer las solicitudes de portabilidad de datos?	☐ Sí ☐ No

El reglamento determina la forma en la que debe realizarse la portabilidad.

¿Se usa un formato estructurado, de uso común y que sea de fácil lectura mecánica?	☐ Sí ☐ No

3.2.8 Derecho de oposición

Las personas tienen derecho a oponerse al tratamiento de su información cuando este tratamiento se realiza sobre la base de:

- El interés público o el ejercicio de poderes públicos conferidos al responsable del tratamiento.
- El interés legítimo del responsable del tratamiento.

En tal caso, el responsable cesará en el tratamiento, salvo que acredite motivos legítimos que prevalezcan sobre los derechos de la persona interesada.

¿El personal está capacitado para decidir si se aplica el derecho de oposición?	☐ Sí ☐ No

Debe asegurarse de que el personal esté capacitado para detectar las solicitudes de oposición.

¿Se ha establecido un procedimiento para la gestión de solicitudes de oposición al tratamiento?	☐ Sí ☐ No
¿El personal que trata con las personas interesadas tiene la formación necesaria para reconocer las solicitudes de oposición al tratamiento?	☐ Sí ☐ No

El reglamento especifica cómo hay que actuar al recibir una petición de oposición al tratamiento en diversos casos.

Si la petición se opone al tratamiento con fines de marketing, debe aceptarse sin excepción.	☐ Sí ☐ No
Si la petición se opone al tratamiento con finalidad de investigación científica o histórica, o con finalidad estadística, será aceptada salvo que el tratamiento se realice en el interés público.	☐ Sí ☐ No

3.2.9 Derecho a no ser objeto de decisiones automatizadas

¿Se realiza un tratamiento automatizado que tiene efectos jurídicos u otros efectos significativos para las personas?	☐ Sí ☐ No
En caso afirmativo, ¿qué base legal lo permite?	
Es necesario para la ejecución de un contrato entre la persona interesada y el responsable.	☐ Sí ☐ No
Está autorizado por el derecho de la Unión o de un Estado miembro.	☐ Sí ☐ No
La persona interesada ha dado su consentimiento explícito.	☐ Sí ☐ No

La persona interesada siempre tiene derecho a obtener intervención humana, a expresar su punto de vista y a impugnar la decisión.

¿Existe un procedimiento para que las personas puedan pedir intervención humana, expresar su punto de vista e impugnar la decisión?	☐ Sí ☐ No
¿Hay personal en la organización con la capacidad de revisar las decisiones y cambiarlas?	☐ Sí ☐ No

Las decisiones automatizadas sólo pueden usar categorías especiales de datos si existe el consentimiento explícito de la persona interesada, o si el tratamiento se hace para proteger los intereses vitales de la persona interesada o de otra persona.

¿Se hace uso de categorías especiales de datos en el tratamiento automático?	☐ Sí ☐ No
En caso afirmativo, ¿qué base legal lo permite?	
La persona interesada ha dado su consentimiento explícito.	☐ Sí ☐ No
El tratamiento se realiza para proteger los intereses vitales de la persona interesada o de otra persona.	☐ Sí ☐ No

3.3. Riesgos en la seguridad de los datos

De acuerdo con el RGPD, las medidas utilizadas para proteger la información deben ser apropiadas al riesgo para los derechos y libertades de las personas. En esta sección seguimos una metodología sencilla para analizar los riesgos relacionados con la seguridad de los datos. Es decir, los riesgos asociados a la pérdida de la confidencialidad, la integridad y la disponibilidad de los datos.

3.3.1 Impacto

Evaluamos el impacto que la pérdida de la confidencialidad, la integridad y la disponibilidad de los datos personales tiene sobre la persona interesada.

Para fijar el impacto sobre las personas de la pérdida de la seguridad de los datos, es necesario tener en cuenta las características del tratamiento. Entre otras:

- El tratamiento de datos de categorías especiales u otros datos especialmente sensibles (información financiera, localizaciones, etc.).
- La monitorización de personas.
- El tratamiento de datos de grupos con necesidades especiales (menores, autoridades, etc.).
- El tratamiento de gran cantidad de datos de cada persona.

Con el objetivo de contextualizar el cálculo del impacto, se plantean diferentes escenarios en los que se pierde alguna de estas propiedades.

Impacto que la pérdida de la confidencialidad de los datos (es decir, de un acceso no autorizado a los datos) tiene sobre las personas.

Ejemplos de casos de pérdida de confidencialidad:

- Pérdida o robo de un ordenador que contiene datos personales.
- Envío por error de datos personales a personas no autorizadas.
- Posibilidad de acceder de forma no autorizada a la cuenta de una persona.
- Un error de configuración en una web expone los datos personales de sus usuarios.
- Robo de información de las instalaciones del responsable o del encargado del tratamiento.
- Un empleado de un centro médico consulta de forma no autorizada el expediente de un paciente.

Impacto			
Bajo	Medio	Alto	Muy alto
Justificación			

Impacto

Impacto que la pérdida de la integridad de los datos (es decir, de la modificación no autorizada de los datos) tiene sobre las personas.

- Un empleado o empleada modifica por error los datos de un cliente.
- Un error en la red de comunicaciones altera los datos mientras están en tránsito.
- Por motivos operacionales, una empresa mantiene varias copias de los datos, pero un cambio en alguna de las copias no se propaga a las demás.
- Pérdida de parte de un expediente, como consecuencia de un fallo en el sistema de tratamiento.

Impacto

Bajo	Medio	Alto	Muy alto

Justificación

Impacto que la pérdida de la disponibilidad de datos tiene sobre las personas.

Ejemplos de casos de pérdida de disponibilidad:

- Un archivo es corrompe o se borra y no hay ninguna copia de seguridad.
- Se pierde un expediente del que sólo existía una copia en papel.
- Un servicio de consulta de datos deja de estar disponible (por ejemplo, el servicio para acceder a los registros electrónicos de salud).

Impacto

Bajo	Medio	Alto	Muy alto

Justificación

El impacto del sistema será el máximo de los tres.

Impacto			
Bajo	Medio	Alto	Muy alto

Justificación

3.3.2 Probabilidad inicial

En la tabla siguiente se muestran las características del tratamiento que incrementan los riesgos de seguridad de los datos. Estimaremos la probabilidad de fallo en la seguridad en función del número de características que se cumplen.

Hardware y software	
P1. ¿El sistema de tratamiento está conectado a sistemas externos a la organización? La conexión con sistemas externos a la organización incrementa la exposición a amenazas, ya que la información puede ser capturada o modificada maliciosamente mientras está en tránsito. Esto se produce, por ejemplo, cuando se han contratado servicios en la nube, se realizan conexiones en modalidad de teletrabajo a los sistemas de la organización o se permiten accesos a través de Internet a la red interna para conectarse a las bases de datos corporativas, entre otros supuestos.	☐ Sí ☐ No
P2. ¿Alguna parte del tratamiento se realiza a través de Internet? La interacción con las personas interesadas a través de Internet expone el sistema de tratamiento a amenazas externas, como *phishing*, *SQL injection, man-in-the-middle attacks, DoS i XSS*. Estas amenazas pueden comprometer el sistema de tratamiento y afectar a las propiedades de seguridad de los datos (confidencialidad, integridad y disponibilidad). Permitir que el personal acceda al sistema de tratamiento a través de Internet también incrementa la exposición a ataques externos y, además, incrementa la posibilidad de que el personal haga un mal uso de la información (accidental o intencionado). Algunos ejemplos de este tipo de tratamiento pueden ser los que utilizan el correo electrónico, aquellos en los que el mantenimiento o la supervisión se realiza a través de Internet o bien el uso de servicios en la nube, como Google Drive, Microsoft One Drive, Amazon Web Services (AWS), Microsoft Azure, entre otros.	☐ Sí ☐ No

Hardware y software

P3. ¿Falta un documento de buenas prácticas relevante en el diseño o en la configuración del sistema de tratamiento? Si el sistema de tratamiento no está bien diseñado o los elementos que lo componen no están configurados adecuadamente, los riesgos para la seguridad de los datos se incrementan. Para garantizar un buen diseño y una buena configuración del sistema de tratamiento, existen multitud de guías de seguridad con diferente temática que se pueden adoptar para seguirlas como, por ejemplo, diseño de la red local, cortafuegos, segmentación de red, redes privadas virtuales (VPN), configuración del sistema operativo, antivirus, uso de contraseñas seguras, múltiple factor de autenticación (MFA), etc. Disponer de un documento de buenas prácticas ayuda a dimensionar el sistema de tratamiento teniendo en cuenta las necesidades computacionales, de comunicación, de seguridad y de almacenamiento. También permite configurar correctamente el software, aplicar una metodología de desarrollo que priorice la seguridad de los datos durante todo el ciclo de vida de la aplicación, utilizar aplicaciones seguras en la nube o establecer criterios sobre el uso y la tipología de datos que pueden gestionarse en ese entorno, entre otras actuaciones.	☐ Sí ☐ No
P4. ¿Falta un documento de buenas prácticas relevante sobre el mantenimiento, la monitorización y la respuesta a incidentes del sistema de tratamiento? Disponer de un documento de buenas prácticas que recoja estos aspectos es esencial para garantizar el mantenimiento, la monitorización y un plan de respuesta a incidentes del sistema adecuados. El mantenimiento debe hacerse tanto para los dispositivos y el hardware como para el software. La monitorización permite analizar un incidente una vez se ha producido y ayuda a detectar comportamientos sospechosos para evitar que el incidente ocurra o para reducir su impacto. El plan de respuesta a incidentes permite contar con un enfoque sistemático para abordar y gestionar los incidentes de seguridad. Este documento de buenas prácticas puede recoger las tareas importantes, como la aplicación de actualizaciones de seguridad del sistema operativo, la realización de copias de seguridad regulares, el uso de sistemas automáticos de detección o correlación de eventos de seguridad, así como la realización periódica de auditorías para la revisión de vulnerabilidades y la seguridad general, entre otros.	☐ Sí ☐ No

Hardware y software

P5. ¿Existe una falta de seguridad física en las instalaciones donde tiene lugar el tratamiento? La seguridad física de las instalaciones de tratamiento es esencial. Sin embargo, no se puede garantizar la seguridad del sistema de tratamiento (ya sea electrónico o no). Esto puede darse, por ejemplo, cuando el CPD no está debidamente protegido con un sistema que impide el acceso a las personas no autorizadas o no está protegido contra accidentes naturales e industriales (fallos eléctricos, inundaciones, etc.), cuando el archivo se ha distribuido en diferentes áreas de forma que no se pueda garantizar la seguridad o cuando se utilizan servicios en la nube sin tener garantías de que las instalaciones del proveedor están debidamente protegidas, entre otros supuestos.	☐ Sí ☐ No

Uso del sistema de tratamiento

P6. ¿Existe una falta de claridad en la definición de los roles y las responsabilidades del personal? Una falta de claridad en la definición de los roles y las responsabilidades puede dar lugar a un uso descontrolado de los datos (ya sea accidental o intencionado). Por ejemplo, un trabajador sólo debería consultar los datos que le son necesarios para realizar sus tareas. También debe ser responsable de destruir la información cuando ya no sea necesaria, así como de garantizar su seguridad cuando se comunica con otra organización o persona, entre otros.	☐ Sí ☐ No
P7. ¿Existe falta de claridad en la definición de los usos aceptables de los sistemas de tratamiento? Cuando los usos aceptables de los sistemas de tratamiento no están claramente definidos, se incrementa el riesgo de hacer un mal uso y de introducir vulnerabilidades en el sistema. Por ejemplo, la instalación de un software de compartición de archivos podría comportar la compartición involuntaria de información, o acceder a páginas web maliciosas podría facilitar la entrada de software malicioso y de robo de datos, entre otros riesgos.	☐ Sí ☐ No
P8. ¿Puede el personal conectar dispositivos externos al sistema? La conexión de dispositivos externos (teléfono móvil, memoria USB, etc.) en el sistema de tratamiento puede representar un riesgo de seguridad, dado que puede facilitar la entrada de software malicioso, la introducción de vulnerabilidades y la extracción no autorizada de información. Por ello, es imprescindible establecer una política clara que regule el uso de dispositivos externos por parte del personal de la organización.	☐ Sí ☐ No

Uso del sistema de tratamiento

P9. ¿Falta un procedimiento adecuado de registro y supervisión de las actividades relacionadas con el tratamiento? La falta de un registro de las actividades (*log file*) puede favorecer las malas prácticas del personal y dificultar la investigación de incidentes una vez se han producido, dada la falta de trazabilidad, tal y como establece el Esquema Nacional de Seguridad (ENS). Esta carencia compromete la capacidad de detectar, analizar y responder a posibles amenazas. Por lo tanto, es necesario disponer de un registro adecuado que permita conocer quién accede a los sistemas de información y asegurar que las actividades registradas se monitoricen de manera efectiva.	☐ Sí ☐ No

Personas que intervienen en el tratamiento

P10. ¿El personal recibe permisos que no son necesarios para cumplir las tareas que tiene encomendadas? Cuanto mayor sea el número de personas que tienen acceso a unos datos, mayor es la probabilidad de que se produzca un abuso. Para evitarlo, es esencial que el sistema controle el acceso del personal y autorice sólo los accesos que son estrictamente necesarios para cumplir con las tareas que se les encomienden.	☐ Sí ☐ No
P11. ¿Se ha externalizado alguna parte del tratamiento a un encargado? El encargado es la persona física o jurídica, autoridad pública, servicio u organismo que presta al responsable un servicio que comporta el tratamiento de datos personales por cuenta de éste. Por ejemplo, una empresa o entidad pública que ofrece un servicio de alojamiento de información en sus servidores o el gestor de un servicio público municipal, entre otros supuestos. La externalización del tratamiento o parte del tratamiento a un encargado supone una pérdida de control sobre los datos. Es necesario escoger un encargado que ofrezca garantías suficientes respecto de la implantación y el mantenimiento de las medidas de seguridad apropiadas, y definir claramente sus responsabilidades.	☐ Sí ☐ No

Personas que intervienen en el tratamiento

P12. ¿Existe una falta de conocimientos del personal respecto al uso adecuado del sistema, de aspectos de seguridad de los datos o de las limitaciones de uso que impone el RGPD? Una carencia de conocimientos sobre el uso que se espera del sistema, sobre la seguridad de la información o sobre las obligaciones y limitaciones que impone el RGPD puede dar lugar a malas prácticas. Así, por ejemplo, el personal podría ser más propenso a seguir las instrucciones de un correo de phishing o, en el momento de guardar documentos, no ser consciente de garantizar su seguridad, entre otras situaciones.	☐ Sí ☐ No
P.13. ¿Existe algún mecanismo de supervisión humana (IA)?	☐ Sí ☐ No

Otras características

P14. ¿La empresa u otras empresas del sector han sufrido ataques últimamente? La existencia de ataques anteriores debe servir como lección para identificar vulnerabilidades y reforzar la seguridad, además de servir de advertencia sobre potenciales ataques futuros.	☐ Sí ☐ No
P15. ¿Se han recibido últimamente quejas de alguna persona respecto a la estabilidad o seguridad del sistema de tratamiento? La presencia de errores en el sistema de tratamiento incrementa la probabilidad de sufrir un ataque. Del mismo modo, las alertas o advertencias respecto a potenciales fallos en la seguridad del sistema también pueden indicar una mayor probabilidad de sufrir ataques.	☐ Sí ☐ No
P16. ¿Se tratan datos de especial interés o datos de un número muy grande de personas usuarias? La presencia masiva de datos y la presencia de datos de especial interés son una motivación adicional para los posibles atacantes.	☐ Sí ☐ No

Calculamos la probabilidad inicial en función del número de respuestas afirmativas conforme a la tabla siguiente:

Respuestas afirmativas	Probabilidad inicial
0 – 4	Baja

Respuestas afirmativas	Probabilidad inicial
5 – 9	Media
10 – 15	Alta

Número de respuestas afirmativas	
Probabilidad inicial estimada	

3.3.3 Riesgo inicial

Una vez estimado el impacto y la probabilidad inicial, aplicaremos la tabla de la Sección 3.1.7 para calcular el riesgo inicial (sin controles de seguridad).

Impacto sobre la confidencialidad	
Impacto sobre la integridad	
Impacto sobre la disponibilidad	
Máximo de los impactos	
Probabilidad	
Riesgo inicial	

3.3.4 Controles de seguridad

Una vez calculado el riesgo inicial, es necesario determinar qué controles (medidas para mejorar la seguridad) deben aplicarse.

Existen muchas listas de controles. Aquí utilizamos los controles del Esquema Nacional de Seguridad-ENS (RD 311/2024). Los controles del ENS son bastante complejos. En la Guía sobre la EIPD encontrará indicaciones y criterios para determinar cuáles hay que aplicar.

Bajo	Medio	Alto	Control	Aplicado
Marco organizativo				
Sí	Sí	Sí	Política de seguridad [org.1] (sistema)	

Bajo	Medio	Alto	Control	Aplicado
Sí	Sí	Sí	Normativa de seguridad [org.2] (sistema)	
Sí	Sí	Sí	Procedimientos de seguridad [org.3] (sistema)	
Sí	Sí	Sí	Proceso de autorización [org.4] (sistema)	

Marco operacional

				Planificación
Sí	Sí	Sí	Arquitectura de seguridad [op.pl.2] (sistema)	
Sí	Sí	Sí	Adquisición de nuevos componentes [op.pl.3] (sistema)	
Sí	Sí	Sí	Dimensionamiento [op.pl.4] (D)	
No	Sí	Sí	Componentes certificados [op.pl.5] (sistema)	
				Control de acceso
Sí	Sí	Sí	Identificación [op.acc.1] (sistema)	
Sí	Sí	Sí	Requerimientos de acceso [op.acc.2] (ICAT)	
No	Sí	Sí	Segregación de funciones y tareas [op.acc.3] (ICAT)	
Sí	Sí	Sí	Proceso de gestión de derechos de acceso [op.acc.4] (ICAT)	
Sí	Sí	Sí	Mecanismo de autenticación para usuarios externos [op.acc.5] (ICAT)	
Sí	Sí	Sí	Mecanismo de autenticación para usuarios internos [op.acc.6] (ICAT)	
				Explotación
Sí	Sí	Sí	Inventario de activos [op.exp.1] (sistema)	
Sí	Sí	Sí	Configuración de seguridad [op.exp.2] (sistema)	
Sí	Sí	Sí	Gestión de la configuración de la seguridad [op.exp.3] (sistema)	

Bajo	Medio	Alto	Control	Aplicado
Sí	Sí	Sí	Mantenimiento y actualizaciones de seguridad [op.exp.4] (sistema)	
No	Sí	Sí	Gestión de cambios [op.exp.5] (sistema)	
Sí	Sí	Sí	Protección contra código malicioso [op.exp.6] (sistema)	
Sí	Sí	Sí	Gestión de incidencias [op.exp.7] (sistema)	
Sí	Sí	Sí	Registro de la actividad de las personas usuarias [op.exp.8] (sistema)	
Sí	Sí	Sí	Registro de la gestión de incidencias [op.exp.9] (sistema)	
Sí	Sí	Sí	Protección de claves criptográficas [op.exp.10] (sistema)	
				Servicios externos
No	Sí	Sí	Contratación y acuerdos de nivel de servicio [op.ext.1] (sistema)	
No	Sí	Sí	Gestión diaria [op.ext.2] (sistema)	
No	No	Sí	Protección de la cadena de suministro [op.ext.3] (sistema)	
No	Sí	Sí	Interconexión de sistemas [op.ext.4] (sistema)	
				Servicios en la nube
Sí	Sí	Sí	Protección de los servicios en la nube [op.nub.1] (sistema)	
				Continuidad del servicio
No	Sí	Sí	Análisis de impacto [op.cont.1] (D)	
No	No	Sí	Plan de continuidad [op.cont.2] (D)	
No	No	Sí	Pruebas periódicas [op.cont.3] (D)	
No	No	Sí	Medios alternativos [op.cont.4] (D)	
				Monitorización del sistema

Bajo	Medio	Alto	Control	Aplicado
Sí	Sí	Sí	Detección de intrusiones [op.mon.1] (sistema)	
Sí	Sí	Sí	Sistema de métricas [op.mon.2] (sistema)	
Sí	Sí	Sí	Vigilancia [op.mon.3] (sistema)	
Medidas de protección				
				Protección de las instalaciones y las infraestructuras
Sí	Sí	Sí	Áreas separadas y control de acceso [mp.if.1] (sistema)	
Sí	Sí	Sí	Identificación de las personas [mp.if.2] (sistema)	
Sí	Sí	Sí	Acondicionamiento de los locales [mp.if.3] (sistema)	
Sí	Sí	Sí	Energía eléctrica [mp.if.4] (D)	
Sí	Sí	Sí	Protección contra incendios [mp.if.5] (D)	
No	Sí	Sí	Protección contra inundaciones [mp.if.6] (D)	
Sí	Sí	Sí	Registro de entrada y salida de equipamiento [mp.if.7] (sistema)	
				Gestión del personal
No	Sí	Sí	Caracterización del puesto de trabajo [mp.per.1] (sistema)	
Sí	Sí	Sí	Deberes y obligaciones [mp.per.2] (sistema)	
Sí	Sí	Sí	Concienciación [mp.per.3] (sistema)	
Sí	Sí	Sí	Formación [mp.per.4] (sistema)	
Protección de los equipos				
Sí	Sí	Sí	Puesto de trabajo vaciado [mp.eq.1] (sistema)	

Bajo	Medio	Alto	Control	Aplicado
No	Sí	Sí	Bloqueo del puesto de trabajo [mp.eq.2] (sistema)	
Sí	Sí	Sí	Protección de portátiles [mp.eq.3] (sistema)	
Sí	Sí	Sí	Otros dispositivos conectados a la red [mp.eq.4] (C)	
				Protección de las comunicaciones
Sí	Sí	Sí	Perímetro seguro [mp.com.1] (sistema)	
Sí	Sí	Sí	Protección de la confidencialidad [mp.com.2] (C)	
Sí	Sí	Sí	Protección de la autenticidad y de la integridad [mp.com.3] (IA)	
No	Sí	Sí	Segregación de flujos de información [mp.com.4] (sistema)	
				Protección de los soportes de la información
Sí	Sí	Sí	Etiquetado [mp.si.1] (C)	
No	Sí	Sí	Criptografía [mp.si.2] (IC)	
Sí	Sí	Sí	Custodia [mp.si.3] (sistema)	
Sí	Sí	Sí	Transporte [mp.si.4] (sistema)	
Sí	Sí	Sí	Borrado y destrucción [mp.si.5] (C)	
				Protección de las aplicaciones informáticas
No	Sí	Sí	Desarrollo de aplicaciones [mp.sw.1] (sistema)	
Sí	Sí	Sí	Aceptación y puesta en servicio [mp.sw.1] (sistema)	
				Protección de la información
No	Sí	Sí	Calificación de la información [mp.info.2] (C)	

Bajo	Medio	Alto	Control	Aplicado
Sí	Sí	Sí	Firma electrónica [mp.info.3] (IA)	
No	No	Sí	Sellos temporales [mp.info.4] (T)	
Sí	Sí	Sí	Limpieza de documentos [mp.info.5] (C)	
Sí	Sí	Sí	Copias de seguridad [mp.info.6] (D)	
				Protección de los servicios
Sí	Sí	Sí	Protección del correo electrónico [mp.s.1] (sistema)	
Sí	Sí	Sí	Protección de servicios y aplicaciones web [mp.s.2] (sistema)	
Sí	Sí	Sí	Protección navegación web [mp.s.3] (sistema)	
No	Sí	Sí	Protección contra la denegación de servicio [mp.s.4] (D) (impacto, probabilidad)	

3.3.5 Impacto residual

Los controles de seguridad pueden reducir el impacto de un incidente de seguridad. Por ejemplo, el cifrado de cierta información puede limitar la extensión de una pérdida de confidencialidad, una copia de seguridad puede limitar el impacto de una pérdida de la disponibilidad de la información y el uso de firma electrónica puede permitir la detección, y por tanto la reducción del impacto, de una pérdida de integridad.

Impacto que la pérdida de la confidencialidad de los datos (es decir, de un acceso no autorizado a los datos) tiene sobre las personas

Impacto

Bajo	Medio	Alto	Muy alto

Impacto residual

Bajo	Medio	Alto	Muy alto

Justificación

Impacto que la pérdida de la confidencialidad de los datos (es decir, de un acceso no autorizado a los datos) tiene sobre las personas

Impacto que la pérdida de la integridad de los datos (es decir, de la modificación no autorizada de los datos) tiene sobre las personas

Impacto

Bajo	Medio	Alto	Muy alto

Impacto residual

Bajo	Medio	Alto	Muy alto

Justificación

Impacto que la pérdida de la disponibilidad de los datos tiene sobre las personas

Impacto

Bajo	Medio	Alto	Muy alto

Impacto residual

Bajo	Medio	Alto	Muy alto

Justificación

Impacto que la pérdida de la disponibilidad de los datos tiene sobre las personas

Impacto

Bajo	Medio	Alto	Muy alto

Impacto que la pérdida de la disponibilidad de los datos tiene sobre las personas

Impacto residual

Bajo	Medio	Alto	Muy alto

Justificación

El impacto residual del sistema será el máximo de los tres anteriores.

Impacto residual del sistema

Bajo	Medio	Alto	Muy alto

3.3.6 Probabilidad residual

Para reducir la probabilidad es necesario eliminar la casuística que hace que las preguntas de la sección 3.2.2 tengan respuesta afirmativa.

En muchas ocasiones no es factible eliminar la casuística asociada a las preguntas de la sección 3.2.2. En este caso, para cambiar una respuesta afirmativa a negativa, es necesario justificar que, en el contexto del sistema de tratamiento, los controles implementados hacen que el objeto de la pregunta tenga un peso inapreciable en la aparición de incidentes de seguridad.

Es necesario revisar las respuestas dadas en el cálculo de la probabilidad inicial teniendo en cuenta los controles implementados.

Responder sólo en aquellas preguntas en las que se ha cambiado la respuesta en base a los controles que se hayan implementado. Se han puesto ejemplos de medidas de seguridad para justificar este cambio, sin perjuicio de que existan otros controles que también puedan reducir la probabilidad.

Hardware y software

P1	¿Está el sistema de tratamiento conectado a sistemas externos a la organización?	
	Controles implementados y justificación para reducir la probabilidad	

Hardware y software

	Cualquier medida relacionada con control de accesos, servicios externos, servicios en la nube, monitorización del sistema.	
P2	¿Alguna parte del tratamiento se realiza a través de Internet?	
	Controles implementados y justificación para reducir la probabilidad	
	Cualquier medida relacionada con control de accesos, servicios externos, servicios en la nube, monitorización del sistema.	
P3	¿Falta un documento de buenas prácticas relevante en el diseño o en la configuración del sistema de tratamiento?	
	Controles implementados y justificación para reducir la probabilidad	
	Cualquier medida de carácter organizativo y de formación de los trabajadores.	
P4	¿Falta un documento de buenas prácticas relevante sobre el mantenimiento, la monitorización y la respuesta a incidentes del sistema de tratamiento?	
	Controles implementados y justificación para reducir la probabilidad	
	Cualquier medida relacionada con formación de trabajadores y medidas relacionadas con monitorización o registros.	
P5	¿Existe una falta de seguridad física en las instalaciones donde tiene lugar el tratamiento?	
	Controles implementados y justificación para reducir la probabilidad	
	Cualquier medida relacionada con monitorización o registros.	

Procedimientos relacionados con el tratamiento

P6	¿Existe una falta de claridad en la definición de los roles y las responsabilidades de los trabajadores?	
	Controles implementados y justificación para reducir la probabilidad	
	Cualquier medida organizativa y/o relacionada con la formación de los trabajadores.	

Procedimientos relacionados con el tratamiento

P7	¿Existe falta de claridad en la definición de los usos aceptables de los sistemas de tratamiento?	
	Controles implementados y justificación para reducir la probabilidad	
	Cualquier medida relacionada con la formación de los trabajadores.	
P8	¿Puede el personal conectar dispositivos externos al sistema?	
	Controles implementados y justificación para reducir la probabilidad	
	Cualquier medida relacionada con control de accesos, servicios externos, servicios en la nube, monitorización del sistema.	
P9	¿Falta un procedimiento adecuado de registro y supervisión de las actividades relacionadas con el tratamiento?	
	Controles implementados y justificación para reducir la probabilidad	
	Cualquier medida relacionada con control de accesos, servicios externos, servicios en la nube, monitorización del sistema.	

Personas que intervienen en el tratamiento

P10	¿El personal recibe permisos que no son necesarios para cumplir las tareas que tiene encomendadas?	
	Controles implementados y justificación para reducir la probabilidad	
	Cualquier medida relacionada con el control de accesos y la formación a los usuarios.	
P11	¿Se ha externalizado alguna parte del tratamiento a un encargado?	
	Controles implementados y justificación para reducir la probabilidad	
	Cualquier medida relacionada con control de accesos, servicios externos, servicios en la nube, monitorización del sistema.	
P12	Existe una falta de conocimientos del personal respecto al uso adecuado del sistema, de aspectos de seguridad de los datos o de las limitaciones de uso que impone el RGPD.	
	Controles implementados y justificación para reducir la probabilidad	

Personas que intervienen en el tratamiento

	Cualquier medida relacionada con la formación de los trabajadores.

Otras características

P13	¿Ha sufrido la empresa u otras empresas del sector ataques últimamente?	
	Controles implementados y justificación para reducir la probabilidad	
	Por ejemplo, se han realizado mejoras en relación con la autenticación de los usuarios tanto internos como externos; se ha mejorado la gestión de incidentes; se ha mejorado la vigilancia y monitorización de los sistemas o la propia red corporativa.	
P14	¿Se han recibido últimamente quejas de alguna persona respecto a la estabilidad o seguridad del sistema de tratamiento?	
	Controles implementados y justificación para reducir la probabilidad	
	Por ejemplo, se han mejorado los procedimientos internos de seguridad, la gestión de configuración de la seguridad o el sistema de métricas.	
P15	¿Se tratan datos de especial interés o datos de un número muy grande de personas usuarias?	
	Controles implementados y justificación para reducir la probabilidad	
	Por ejemplo, se ha mejorado la gestión de configuración de la seguridad, o la existencia de sistemas redundantes o, en general, sistemas para mejorar la confidencialidad, la integridad o la autenticidad.	

La probabilidad residual se calcula contando el número de respuestas afirmativas.

Respuestas afirmativas	Probabilidad inicial
0 – 4	Baja
5 – 9	Media
10 – 14	Alta

3.3.7 Estimación del riesgo residual

Una vez estimado el impacto residual y la probabilidad residual, calculamos el riesgo residual siguiendo la tabla de la sección 3.1.7.

	Impacto			
Probabilidad	Bajo	Medio	Alto	Muy alto
Baja	Riesgo bajo	Riesgo bajo	Riesgo medio	Riesgo alto
Media	Riesgo bajo	Riesgo medio	Riesgo alto	Riesgo alto
Alta	Riesgo medio	Riesgo alto	Riesgo alto	Riesgo alto

Impacto residual sobre la confidencialidad Impacto residual sobre la integridad Impacto residual sobre la disponibilidad	
Máximo de los impactos residuales Probabilidad residual	
Riesgo residual	

Si el riesgo residual es alto, es necesario proponer nuevos controles para reducirlo. Si no es posible reducirlo, antes de iniciar el tratamiento es necesario realizar una consulta previa a la autoridad de protección de datos competente sobre su idoneidad.

4. Evaluación de impacto en los Derechos Fundamentales

En este apartado, se examinan los impactos sobre derechos y libertades fundamentales distintos del derecho a la protección de datos, que ya han sido objeto de la EIPD.

4.1 Cuestionario de planificación y alcance

Sección A[4] Descripción complementaria del sistema de IA, incluidos los flujos de datos relacionados	¿Cuáles son los principales objetivos del sistema de IA? ¿Qué tipos de datos se tratan (personales, no personales, categorías especiales)?
Sección B Contexto de derechos fundamentales	¿Qué derechos fundamentales se ven potencialmente afectados por el uso del sistema de IA? ¿Qué instrumentos jurídicos internacionales/regionales de protección de los derechos humanos/fundamentales se han aplicado a nivel operativo? ¿Cuáles son los tribunales u organismos más relevantes en materia de derechos fundamentales en su contexto de uso? ¿Cuáles son las decisiones y disposiciones más relevantes en materia de derechos humanos/fundamentales?
Sección C Controles implementados	¿Qué políticas y procedimientos se han implementado para evaluar el posible impacto sobre los derechos fundamentales, incluida la participación de las partes interesadas? Se ha efectuado, desarrollado y aplicado una evaluación de impacto en relación con cuestiones específicas (por ejemplo, protección de datos) o algunas características del sistema (por ejemplo, uso de biometría)?

[4] En la Sección A del modelo integrado, las cuestiones relativas a las principales características del sistema, los países donde se ofrecía y la identificación de las personas afectadas y de los responsables han pasado a la parte general de la evaluación (1.3 Descripción i análisis del sistema de IA).

Sección D Intervención de las partes interesadas y diligencia debida	¿Cuáles son los principales grupos o comunidades potencialmente afectados por el sistema de IA, incluido su desarrollo? ¿Qué partes interesadas, además de los individuos o grupos que pueden verse afectados por los sistemas de IA, deben participar (por ejemplo, la sociedad civil y las organizaciones internacionales, expertos, asociaciones industriales, periodistas)? ¿Existen otros titulares de obligaciones que deban participar, aparte del proveedor y el responsable del despliegue de la IA (por ejemplo, autoridades nacionales, organismos gubernamentales)? ¿Han participado en el proceso de evaluación los socios comerciales, incluidos los proveedores de servicios (por ejemplo, subcontratistas en sistemas de IA y conjuntos de datos)? ¿El proveedor de IA ha llevado a cabo una evaluación de su cadena de suministro para identificar si las actividades de los proveedores/contratistas que participan en el desarrollo de productos/servicios pueden afectar a los derechos fundamentales? ¿El proveedor ha promovido estándares o auditorías de derechos fundamentales para garantizar el respeto de los derechos fundamentales entre los proveedores? ¿El proveedor y el responsable del despliegue de la IA han comunicado públicamente las posibles repercusiones del sistema de IA en los derechos fundamentales? ¿El proveedor y el responsable del despliegue de la IA han proporcionado formación sobre estándares de derechos fundamentales al personal encargado de la gestión y la contratación relacionadas con el sistema de IA?

4.2 Matrices de riesgo

Tabla 1. Probabilidad

Baja	El riesgo de perjuicio es improbable o altamente improbable.
Media	El riesgo puede producirse.
Alta	Existe una alta probabilidad de que se produzca el riesgo.
Muy alta	Es muy probable que se produzca el riesgo.

Tabla 2. Exposición

Baja	Están potencialmente afectados pocos o muy pocos individuos de la población identificada de titulares de derechos.
Media	Parte de la población identificada está potencialmente afectada.
Alta	La mayoría de la población identificada está potencialmente afectada.
Muy alta	Casi toda la población identificada está potencialmente afectada.

Tabla 3. Probabilidad de que se produzca un perjuicio (*likelihood*)

		Probabilidad			
		Baja	**Media**	**Alta**	**Muy alta**
Exposición	**Baja**	B	B/M	B/A	B/MA
	Media	M/B	M	M/A	M/MA
	Alta	A/B	A/M	A	A / MA
	Muy alta	MA/B	MA/M	MA/A	MA

Probabilidad			
Baja	Media	Alta	Muy alta

Tabla 4. Gravedad del perjuicio

Baja	Los individuos y grupos afectados pueden encontrar sólo perjuicios menores en el ejercicio de sus derechos y libertades.
Media	Los individuos y grupos afectados pueden encontrarse con importantes prejuicios.
Alta	Los individuos y grupos afectados pueden enfrentarse a graves perjuicios.
Muy alta	Los individuos y grupos afectados pueden encontrarse con graves perjuicios e incluso irreversibles.

Tabla 5. Esfuerzo para superar los perjuicios y revertir los efectos adversos

Bajo	Los perjuicios sufridos pueden superarse sin problemas (por ejemplo, tiempo dedicado a modificar la información, molestias, irritaciones, etc.).
Medio	Los perjuicios sufridos pueden superarse a pesar de algunas dificultades (por ejemplo, costes adicionales, miedo, incomprensión, estrés, pequeñas dolencias físicas, etc.).
Alto	Los perjuicios sufridos pueden superarse aunque con serias dificultades (por ejemplo, pérdidas económicas, daños materiales, empeoramiento de la salud, etc.).
Muy alto	Los perjuicios sufridos pueden no superarse (por ejemplo, dolencias psicológicas o físicas de larga duración, muerte, etc.).

Tabla 6. Gravedad (*severity*)

		Gravedad			
		Bajo	**Media**	**Alta**	**Muy alta**
Esfuerzo	**Bajo**	B	B/M	B/A	B/MA
	Medio	M/B	M	M/A	M/MA
	Alto	A/B	A/M	A	A/MA
	Muy alto	MA/B	MA/M	MA/A	MA

Gravedad			
Bajo	Medio	Alto	Muy alto

Tabla 1A. Recogida de datos y análisis de riesgos

Derechos/ Libertades potencialmente afectados	Descripción del impacto	Probabilidad			Gravedad		
		Probabilidad de resultados adversos	Exposición	Probabilidad	Gravedad del impacto	Esfuerzo	Gravedad

Tabla 7. Impacto general del riesgo

		Gravedad			
		Baja	Media	Alta	Muy alta
Probabilidad	Baja				
	Media				
	Alta				
	Muy alta				

Riesgo global			
Bajo	Medio	Alto	Muy alto

Tabla 2A. Gestión de riesgos (I)

Derechos/libertades afectados	Probabilidad	Gravedad	Impacto global	Medidas para prevenir/mitigar los impactos

Tabla 3A. Gestión de riesgos (II)[5]

Derechos/libertades afectados	Probabilidad (residual)	Gravedad (residual)	Impacto residual

[5] En esta tabla deberá incorporarse una referencia al resultado final de la EIPD en cuanto a la probabilidad y la gravedad residual, que puede hacerse mediante una llamada a la página concreta de la EIPD donde se describen las medidas adoptadas.