apdcat
Autoritat Catalana de Protecció de Dades

Plantilla de Evaluación de Impacto relativa a la Protección de Datos

Una evaluación de impacto relativa a la protección de datos (EIPD) es un procedimiento que busca identificar y controlar los riesgos por los derechos y las libertades de las personas que resultan de un tratamiento de datos personales.

Es necesaria una descripción del tratamiento para determinar si es necesaria una EIPD. Esta descripción debe tener un nivel de detalle que permita evaluar los supuestos e indicadores de riesgo que se detallan a continuación.

Descripción del tratamiento

No es necesario hacer una EIPD si aplica alguno de los supuestos siguientes:

Supuesto	
El tratamiento tiene naturaleza, alcance, contexto y finalidad parecida a otro tratamiento por el que ya se ha hecho 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 esta base jurídica.	

Justificación

Si ninguno de los supuestos anteriores aplica, hay que hacer una EIPD si el tratamiento puede comportar un riesgo grave por los derechos y las libertades de las personas. El Grupo de Trabajo del Artículo 29 (GT29) da la siguiente lista de características que pueden ser indicativas de riesgo alto.

Indicador de alto riesgo potencial	
Evaluación o puntuación, incluidas la elaboración de perfiles y predicciones.	
Toma de decisiones automatizada con efectos jurídicos o que afecta de manera similar y significativa a la persona física.	

Indicador de alto riesgo potencial	
Observación sistemática de un área de acceso público.	
Datos sensibles, relativos a condenas o infracciones penales, o datos que permitan determinar la situación financiera.	
Datos biométricos con el propósito de identificar de manera única a una persona física.	
Datos genéticos para cualquier fin.	
Tratamiento de datos a gran escala.	
Conjuntos de datos que se han enlazado o combinado.	
Datos relacionados con personas vulnerables	
Uso innovador de tecnologías.	
Tratamiento que en sí mismo impide el ejercicio de un derecho o el uso de un servicio o contrato.	

Según el GT29, hay que hacer una EIPD cuando el tratamiento presenta dos o más, aunque indica que puede ser conveniente hacer la EIPD incluso en algunos casos en los que solo presenta una. Si hay otros o más y se considera que no hay que hacer una EIPD, hay que justificarlo.

Hay que hacer la EIPD? ¿Por qué?

Si se ha nombrado un DPD, hay que considerar su opinión respecto de la necesidad de hacer una EIPD.

Opinión del DPD respecto de la necesidad de hacer una EIPD

1. Descripción del tratamiento

Hay que hacer una descripción del tratamiento que sea lo más detallada posible, ya que esta será la base para evaluar la necesidad, la proporcionalidad y los riesgos del tratamiento.

Descripción detallada del tratamiento

Finalidad del tratamiento

1.1 Datos personales tratados

Las características de los datos a tratar son relevantes a la hora de determinar los riesgos del tratamiento y el cumplimiento de algunas disposiciones del reglamento.

Tipo de dato.	
Fuente.	
Plazo de conservación.	
¿Dato especialmente sensible?	
¿Uso con propósito diferente a de recolección?	

Tipo de dato.	
Fuente.	
Plazo de conservación.	
¿Dato especialmente sensible?	
¿Uso con propósito diferente a de recolección?	

1.2 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.

Nombre.	
Procesos en que interviene.	
Descripción.	

Nombre.	
Procesos en que interviene.	
Descripción.	

1.3 Procesos de tratamiento

El objetivo de esta sección es dividir el tratamiento en partes más pequeñas. De manera que sean más coherentes y más fáciles de explicar.

Proceso.	
Descripción.	
Datos tratados.	
Resultado del proceso.	
Persona destinataria.	
Lugar del tratamiento.	

Proceso.	
Descripción.	
Datos tratados.	
Resultado del proceso.	
Persona destinataria.	
Lugar del tratamiento.	

1.4 Transferencias de datos

Compartir datos con agentes externos puede incrementar los riesgos del tratamiento; especialmente si se hacen en terceros países donde el RGPD no aplica.

Se comparten datos? Describe qué datos se comparten, la persona destinataria (física o ɹrídica) y el motivo/finalidad.

2. Necesidad y proporcionalidad

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

2.1 Finalidad del tratamiento

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

¿Se utilizan datos recogidos con una finalidad diferente a la de este tratamiento?	☐ Sí ☐ No

En caso afirmativo

Las siguientes condiciones permiten el tratamiento de los datos con una finalidad diferente a la de recogida.	
Se ha obtenido el consentimiento de las personas interesadas para el tratamiento con la nueva finalidad.	
El tratamiento está basado en el derecho de la Unión o de los estados miembros que constituye una medida para salvaguardar:	
La seguridad nacional.	
La defensa.	
La seguridad pública.	
Prevención, investigación, detección y procesamiento de delitos penales.	
Otros objetivos importantes de interés público.	

En caso afirmativo

Protección de la independencia judicial y de los procedimientos judiciales.	
La prevención, la investigación, la detección y el procesamiento de infracciones en normas deontológicas.	

Si no 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.	

Si no 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.	

2.2 Principios de licitud y la lealtad

2.2.1 Base legal para el tratamiento

Un tratamiento es lícito si aplica alguna de las bases legales. Marcar lo que corresponda.

La persona interesada ha dado su consentimiento para el tratamiento de sus datos personales, por una o varias finalidades específicas.	
El tratamiento es necesario para ejecutar un contrato en el que la persona interesada es parte o para aplicar medidas precontractuales.	
El tratamiento es necesario para cumplir una obligación legal aplicable al responsable del tratamiento.	
El tratamiento es necesario para proteger intereses vitales de la persona interesada o de otra persona física.	
El tratamiento es necesario para cumplir una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.	
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 (en particular, cuando es un menor).	

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.

2.2.2 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 conlleva.

¿El tratamiento ofrece servicios de la sociedad de la información a niños niñas y tiene como base el consentimiento?	☐ Sí ☐ No
En caso afirmativo, ¿se ha tenido en cuenta la edad mínima de consentimiento?	☐ Sí ☐ No

2.2.3 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 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.	
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.	
El tratamiento es necesario para proteger intereses vitales de la persona interesada o de otra persona física, en el supuesto que el interesado no esté capacitado para dar el consentimiento.	
El tratamiento es legítimo y con garantías, hecho por una asociación sin ánimo de lucro de carácter político, filosófico, religioso o sindical, siempre que el tratamiento afecte a personas con las que mantienen contactos en relación con estas finalidades y los datos no se comuniquen a terceros sin el consentimiento de las personas interesadas.	
El tratamiento hace referencia a datos que el interesado ha hecho públicos.	
El tratamiento es necesario para formular, ejercer o defender reclamaciones, o cuando los tribunales actúan en su función judicial.	
El tratamiento es necesario por razones de interés público esencial.	
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.	
El tratamiento es necesario por razones de interés público en el ámbito de la salud pública.	
El tratamiento es necesario con la finalidad de archivo con interés público, investigación científica o histórica, o con finalidad estadística.	

Justificación de la licitud del tratamiento de datos de categorías especiales

2.2.4 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 puede llevarse 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

2.2.5 Validez del consentimiento

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

El responsable debe poder demostrar que lo ha recogido.	
La solicitud de consentimiento es inteligible, de fácil acceso y en un lenguaje claro.	
La ejecución de un contrato no puede supeditarse a recibir el consentimiento respecto de datos personales no necesarios para ejecutar el contrato.	
Se ha informado a las personas interesadas de la posibilidad de retirar el consentimiento en cualquier momento.	

2.2.6 Transferencias de datos

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

¿Se hacen 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 nivel adecuado de protección, si se han establecido las garantías suficientes según el artículo 46 o si aplica alguna de las excepciones del artículo 49.

Datos transferidos.	
País.	
Condición que permite la transferencia.	

Datos transferidos.	
País.	
Condición que permite la transferencia.	

2.2.7 Lealtad del tratamiento

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

Justificación del tratamiento leal

2.3 Principio de minimización

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

Tipos de datos.	

Justificación de la adecuación, relevancia y necesidad

2.4 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. Hay que 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 borradas? ¿Cuánto tiempo y cómo se garantiza que no se tratan? etc.).

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.

2.5 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 las que sean inexactas se actualicen o se borren sin dilación.

Controles de la calidad de los datos

Medidas para corregir los datos

2.6 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 está diseñado. Es decir, no consideramos los casos en que falla la seguridad del sistema (sea este 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 les personas interesadas y del delegado de protección de datos.

Potenciales efectos negativos del tratamiento sobre las personas

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

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

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

Amenazas	Probabilidad	Riesgo

Riesgo estimado

Efecto sobre las personas:

Impacto:

Amenazas	Probabilidad	Riesgo

Riesgo estimado

Efecto sobre las personas:

A menos que el riesgo sea bajo, hay que 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 comenzar el tratamiento hay que consultar 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, habrá que revisar y actualizar las secciones anteriores de la EIPD.

2.7 Necesidad y proporcionalidad del tratamiento

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

Justificación de la eficacia e idoneidad del tratamiento por el propósito que se busca

Justificación de la necesidad del tratamiento

Justificación de que el tratamiento es proporcional

2.8 Opinión de las personas interesadas

El RGPD establece que, si es posible, hay que recoger la opinión de les personas interesadas del tratamiento.

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

En caso de que no se considera apropiado recoger la opinión de las personas interesadas, hay que justificarlo.

¿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 al apartado 2.7 y se pretende llevar adelante el tratamiento, hay que justificar el porqué.

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

3. Controles para garantizar los derechos de las personas

3.1 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 se debe hacer esta comunicación.

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

El responsable debe responder a las peticiones de ejercicio de 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, se puede extender el periodo en dos meses. En este caso hay que informar de las razones dentro del primer mes.	☐ Sí ☐ No

Si el responsable no tiene que 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 llevar a cabo la petición (por ejemplo, la petición es repetitiva o el responsable no puede identificar 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 Controles por 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.

Los artículos 13 y 14, especifican que hay que informar a las personas interesadas de los puntos 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 los hay).	☐ Sí ☐ No
La finalidad del tratamiento.	☐ Sí ☐ No
La base legal del tratamiento.	☐ Sí ☐ No
El interés legítimo del responsable, si esta 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 utilizado para determinarlo.	☐ Sí ☐ No
La intención de transmitir los datos fuera de la UE, si procede.	☐ Sí ☐ No
La decisión de la Comisión Europea respecto de la suficiencia de la seguridad que ofrece el país u 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
La existencia del derecho a revocar el consentimiento (si esta es la base legal del tratamiento).	☐ Sí ☐ No
La existencia del derecho a presentar una 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 diferente 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

Hay 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 hay que informarla si se da alguna de las siguientes condiciones: l[1]a persona interesada ya dispone de esta información, la comunicación es imposible o supone un esfuerzo desproporcionado, así está regulado por 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, hay que justificarlo.

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

Si aplica alguna exención al derecho de información, hay que decir cuál, a qué datos y justificar el porqué.

Si se informa a las personas interesadas, el Reglamento determina cuándo hay que hacerlo[2].

Si los datos se recogen directamente de las personas interesadas, en el momento de recogerlos.	☐ Sí ☐ No

Si los datos se recogen indirectamente, hay que 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, como muy tarde en el momento de la primera comunicación.	☐ Sí ☐ No
Si se quieren comunicar los datos a terceros, antes de comunicarlos.	☐ Sí ☐ No

[1] RGPD, artículo 14.5.

[2] GDPR art 13(1) y 14(3),

3.3 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 este caso, el derecho de acceso a los datos personales y a la siguiente información:

La finalidad del tratamiento.	☐ Sí ☐ No
Las categorías de datos tratadas.	☐ Sí ☐ No
Las personas destinatarias de los datos.	☐ Sí ☐ No
El plazo de conservación de los datos.	☐ Sí ☐ No
Los derechos a rectificar y suprimir los datos.	☐ Sí ☐ No
Los derechos a 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, si procede.	☐ Sí ☐ No

Aparte de conocer qué información se debe transmitir a las personas interesadas, hay que 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

3.4 Controles para garantizar el derecho de rectificación

Las personas tienen el derecho a que se rectifiquen sus datos, si estos 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, es necesario que informe a las personas destinatarias sobre la rectificación.

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

3.5 Derecho de supresión

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

- Los datos ya no son necesarios en relación con la finalidad por la que se recogieron.
- La persona interesada su consentimiento y no hay otra base legal para el tratamiento.
- La persona interesada se opone al tratamiento y no hay otro factor superior que lo legitime.
- Los datos se han tratado sin una base legal.
- Los datos deben borrarse de acuerdo con una obligación legal que afecta al responsable.
- Los datos se utilizan para ofrecer servicios de la sociedad de la información a niños.
- En cambio, el derecho de supresión no aplica en los siguientes casos:
- 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 estas finalidades se viera afectado por la supresión de los datos).
- Para presentar, ejercer o defender reclamaciones legales.

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

Es recomendable establecer un canal estándar para que las personas interesadas puedan pedir hacer efectivo el derecho de supresión. Ahora bien, hay que 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

3.6 Derecho a limitar el tratamiento

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

- 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 aplica el derecho a limitar el tratamiento?	☐ Sí ☐ No

Hay que asegurarse de que el personal está 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, hay que tener en cuenta las diferentes formas que éste 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, hay que 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

3.7 Derecho a la portabilidad de los datos

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

- Si el tratamiento está basado en el consentimiento, o es necesario para ejecutar un contrato o para aplicar medidas precontractuales.
- El tratamiento se hace con 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 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, hay que 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), hay que 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 las libertades de las demás personas?	☐ Sí ☐ No

Hay que asegurarse de que el personal está 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 hacerse la portabilidad.

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

3.8 Derecho de oposición

Las personas tienen el derecho a oponerse al tratamiento de su información cuando este tratamiento se hace 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 este caso, el responsable cesará en el tratamiento, salvo que acredite motivos legítimos que prevalezcan sobre los derechos del interesado.

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

Hay que asegurarse de que el personal está 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 se debe actuar al recibir una petición de oposición al tratamiento en varios casos.

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

3.9 Derecho a no ser objeto de decisiones automatizadas

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

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 hacer uso de 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 que lo permite?	
La persona interesada ha dado su consentimiento explícito.	
El tratamiento se hace para proteger los intereses vitales de la persona interesada o de otra persona.	

4. Riesgos en la seguridad de los datos

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

4.1 Impacto

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

Para fijar el impacto sobre las personas de la pérdida de la seguridad de los datos, hay que tener en cuenta las características del tratamiento. Entre otros:

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

- Ejemplos de casos de pérdida de la integridad:
- 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 tráfico.
- 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 los datos tiene sobre las personas.

Ejemplos de casos de pérdida de la disponibilidad:

- Un fichero es corrompe o se borra y no hay una copia de seguridad.
- Se pierde un expediente del que sólo había 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

4.2 Probabilidad inicial

La tabla siguiente muestra 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 se cumplen.

Hardware y software

Q1. ¿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. Pudiendo ser la información capturada o modificada maliciosamente mientras está en tráfico. Eso se produce, por ejemplo, cuando se han contratado servicios en la nube, teletrabajando se realizan conexiones a los sistemas de la organización, o se permiten accesos a través de internet a la red interna para conectarse a bases de datos corporativas, entre otros motivos.	☐ Sí ☐ No

Hardware y software

Q2. ¿Alguna parte del tratamiento se hace 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 y 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 tratamientos que hacen uso del correo electrónico, aquellos en que el mantenimiento o la supervisión se hace a través de internet o bien el uso de servicios en la nube como son Google Drive, Microsoft OneDrive, Amazon Web Services, Microsoft Azure, entre otros.	☐ Sí ☐ No
Q3. ¿Falta de seguimiento de un documento de buenas prácticas relevante en el diseño o 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 hay multitud de guías de buenas prácticas en seguridad con diferentes temáticas como pueden ser para diseño de una red local, cortafuegos, segmentación de la red, redes privadas virtuales (VPN), configuración del sistema operativo, antivirus, uso de contraseñas seguras, factores múltiples de autenticación (MFA), etc. Disponer de un documento de buenas prácticas ayuda a dimensionar el sistema de tratamiento de datos 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 se pueden gestionar en este entorno, entre otras actuaciones.	☐ Sí ☐ No

Hardware y software

Q4. Falta de seguimiento de un documento de buenas prácticas relevante en 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, monitorización y un plan de respuesta a incidentes del sistema adecuados. El mantenimiento debe realizarse tanto de los dispositivos y hardware como del software. La monitorización permite analizar un incidente una vez se ha producido y ayuda a detectar comportamientos sospechosos a fin de 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 importantes tareas 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
Q5. ¿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 impida 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 de seguridad o cuando se realiza otros supuestos.	☐ Sí ☐ No

Uso del sistema de tratamiento

Q6. ¿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 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 a otra organización o persona, entre otras.	☐ Sí ☐ No

Uso del sistema de tratamiento

Q7. ¿Hay 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
Q8. ¿Puede el personal conectar dispositivos externos al sistema? La conexión de dispositivos externos (teléfono móvil, memoria USB, etc.) al 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
Q9. ¿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). Esto compromete la capacidad de detectar, analizar y responder a posibles amenazas. Por tanto, es necesario disponer de un registro adecuado que permita conocer quién accede a los sistemas de información y asegurar que las actividades registradas sean monitorizadas de manera efectiva.	☐ Sí ☐ No

Personas que intervienen en el tratamiento

Q10. ¿El personal recibe permisos que no son necesarios para cumplir las tareas que tiene encomendadas? Cuanto mayor sea la cantidad de personas que tienen acceso a unos datos, mayor es la probabilidad de que se produzca un abuso. Para evitar esto, es esencial que el sistema controle el acceso al sistema del personal y autorice sólo los accesos que son estrictamente necesarios para cumplir las tareas que tiene encomendadas.	☐ Sí ☐ No

Personas que intervienen en el tratamiento

Q11. ¿Se ha externalidad 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
Q12. ¿Existe una falta de conocimiento del personal respecto del uso adecuado del sistema, de aspectos de seguridad de los datos o de las limitaciones de uso que impone el RGPD? Una falta de conocimientos sobre el uso que se espera del sistema, sobre 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, a la hora de guardar documentos, no ser consciente de garantizar su seguridad, entre otras situaciones.	☐ Sí ☐ No

Otras características

Q13. ¿Ha sufrido la empresa u otras empresas del sector ataques últimamente? La existencia de ataques anteriores debe servir como lección para identificar vulnerabilidades y reforzar la seguridad, así como advertencia de potenciales ataques futuros.	☐ Sí ☐ No
Q14. ¿Se han recibido quejas de alguna persona respecto de la estabilidad o la seguridad del sistema de tratamiento últimamente? La presencia de errores en el sistema de tratamiento incrementa la probabilidad de sufrir un ataque. Del mismo modo, las alertas o advertencias respecto potenciales fallos en la seguridad del sistema también pueden indicar una probabilidad más alta de sufrir ataques.	☐ Sí ☐ No
Q15. ¿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 extra para los posibles atacantes.	☐ Sí ☐ No

Calculamos la probabilidad inicial de en función del número de respuestas afirmativas de acuerdo con la siguiente tabla:

Respuestas Afirmativas	Probabilidad inicial
0 - 4	Baja
5 – 9	Media
10 - 15	Alta

Número de respuestas afirmativas	
Probabilidad inicial estimada	

4.3 Riesgo inicial

Una vez estimado el impacto y la probabilidad inicial, aplicaremos la tabla de la Sección 2.6 para calcular el riesgo inicial (sin los controles de seguridad).

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

4.4 Controles de seguridad

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

Existen varias listas de controles de seguridad. Aquí hacemos uso de los controles del Esquema Nacional de Seguridad ENS (RD311/2022). En la guía sobre EIPD hay más detalles sobre los controles e indicaciones para determinar cuáles aplicar.

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

Bajo	Medio	Alto	Control	Aplicado
Sí	Sí	Sí	Configuración de seguridad [op.exp.2] (sistema)	
Sí	Sí	Sí	Gestión de la configuración de la seguridad [op.exp.3] (sistema)	
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 suministros [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)	

Bajo	Medio	Alto	Control	Aplicado
No	No	Sí	Pruebas periódicas [op.cont.3] (D)	
No	No	No	Medios alternativos [op.cont.] (D)	
				Monitorización del sistema
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 de 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				

Bajo	Medio	Alto	Control	Aplicado
Sí	Sí	Sí	Puesto de trabajo vaciado [mp.eq.1] (sistema)	
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 la 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

Bajo	Medio	Alto	Control	Aplicado
No	Sí	Sí	Calificación de la información [mp.info.2] (C)	
Sí	No	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 de navegación web [mp.s.3] (sistema)	
No	Sí	Sí	Protección contra la denegación de servicio [mp.s.4] (D) (impacto, probabilidad)	

4.5 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 la 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 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 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

4.6 Probabilidad residual

Para reducir la probabilidad hay que eliminar la casuística que hace que las preguntas de la sección 4.2 tengan respuesta afirmativa. Por ejemplo, si permitir el tratamiento a través de internet no es esencial, podemos desactivarlo para hacer negativa la respuesta a la pregunta Q2.

Muchas veces no es factible eliminar la casuística asociada a las preguntas de la sección 4.2. En este caso, para cambiar una respuesta afirmativa a negativa, hay que justificar que, en el contexto del sistema de tratamiento, los controles implementados hacen que el objeto de la pregunta tenga un peso negligible 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

Q1	¿Está el sistema de tratamiento conectado a sistemas externos a la organización?	
	Controles implementados y justificación para reducir probabilidad.	
	Cualquier medida relacionada con control de accesos, servicios externos, servicios en la nube, monitorización del sistema.	

Hardware y software

Q2	¿Alguna parte del tratamiento se hace a través de internet?	
	Controles implementados y justificación para reducir probabilidad.	
	Cualquier medida relacionada con control de accesos, servicios externos, servicios en la nube, monitorización del sistema.	
Q3	¿Falta de seguimiento de un documento de buenas prácticas relevante en el diseño o la configuración del sistema de tratamiento?	
	Controles implementados y justificación para reducir probabilidad.	
	Qualsevol mesura de caràcter organitzatiu i de formació dels treballadors.	
Q4	¿Falta de seguimiento de un documento de buenas prácticas relevante en el mantenimiento, la monitorización y la respuesta a incidentes del sistema de tratamiento?	
	Controles implementados y justificación para reducir probabilidad.	
	Cualquier medida relacionada con formación de trabajadores y medidas relacionadas con la monitorización o registros (logs).	
Q5	¿Existe una falta de seguridad física en las instalaciones donde tiene lugar el tratamiento?	
	Controles implementados y justificación para reducir probabilidad.	
	Cualquier medida relacionada con monitorización o registros (logs).	

Procedimientos relacionados con el tratamiento

Q6	¿Existe una falta de claridad en la definición de los roles y las responsabilidades de los trabajadores?	
	Controles implementados y justificación para reducir probabilidad.	
	Cualquier medida organizativa y/o relacionada con formación de trabajadores.	
Q7	¿Hay falta de claridad en la definición de los usos aceptables de los sistemas de tratamiento?	

Procedimientos relacionados con el tratamiento

	Controles implementados y justificación para reducir probabilidad.	
	Cualquier medida relacionada con formación de trabajadores.	
Q8	¿Puede el personal conectar dispositivos externos al sistema?	
	Controles implementados y justificación para reducir probabilidad.	
	Cualquier medida relacionada con control de accesos, servicios externos, servicios en la nube, monitorización del sistema.	
Q9	¿Falta un procedimiento adecuado de registro y supervisión de las actividades relacionadas con el tratamiento?	
	Controles implementados y justificación para reducir probabilidad.	
	Cualquier medida relacionada con control de accesos, servicios externos, servicios en la nube, monitorización del sistema.	

Personas que intervienen en el tratamiento

Q10	¿El personal recibe permisos que no son necesarios para cumplir las tareas que tiene encomendadas?	
	Controles implementados y justificación para reducir probabilidad.	
	Cualquier medida relacionada con el control de accesos y la formación a los usuarios.	
Q11	¿Se ha externalidad alguna parte del tratamiento a un encargado?	
	Controles implementados y justificación para reducir probabilidad.	
	Cualquier medida relacionada con control de accesos, servicios externos, servicios en la nube, monitorización del sistema.	
Q12	¿Existe una falta de conocimiento del personal respecto del 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 probabilidad.	
	Cualquier medida relacionada con formación de trabajadores	

Otras características

Q13	¿Ha sufrido la empresa u otras empresas del sector ataques últimamente?	
	Controles implementados y justificación para reducir 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.	
Q14	¿Se han recibido quejas de alguna persona respecto de la estabilidad o la seguridad del sistema de tratamiento últimamente?	
	Controles implementados y justificación para reducir probabilidad.	
	Por ejemplo, se han mejorado los procedimientos internos de seguridad, la gestión de configuración de la seguridad, o el sistema de métricas.	
Q15	¿Se tratan datos de especial interés o datos de un número muy grande de persones usuarias?	
	Controles implementados y justificación para reducir probabilidad.	
	Por ejemplo, se ha mejorado la gestión de configuración de la seguridad, o 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

4.7 Estimación del riesgo residual

Una vez estimado el impacto residual y la probabilidad residual, calculamos el riesgo residual siguiendo la tabla de la Sección 2.6.

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

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

Si el riesgo residual es alto, hay que proponer nuevos controles para reducirlo. Si no es posible reducirlo, antes de iniciar el tratamiento hay que consultar a la autoridad de protección de datos competente sobre su idoneidad.