Directrices para un Plan Integrado para la DPIA-FRIA

Octubre 2026

DPD en xarxa

Índice

Presentación 4

1. Principales bloques de la EIPD y su integración con el FRIA 5
   1.1 La descripción sistemática 5
   1.2 La evaluación 6
   1.3 Medidas de mitigación 9
2. Flujo de trabajo integrado de AIPD-FRIA y diseño del modelo 10

Coordinadores:

Alessandro Mantelero y Joana Marí

Participantes:

Aida Mariscal (Centro de Telecomunicaciones y Tecnologías de la Información)

Albert Portugal (Consorcio de Servicios Universitarios de Catalunya)

Albert Serra (Autoridad Catalana de Protección de Datos)

Alessandro Mantelero (Universidad Politécnica de Turín)

Cristina Guzmán (Universidad Politécnica de Catalunya – BarcelonaTech (UPC))

Carles Garcia (Autoritat Catalana de Protecció de Dades)

Carlos López (Autoritat Catalana de Protecció de Dades)

Esther Garcia (CaixaBank, SA)

Irma Choy (Consorci AOC)

Joana Judas (Autoridad Catalana de Protección de Datos)

Joana Marí (Autoridad Catalana de Protección de Datos)

M. Ascensión Moro (Ayuntamiento de Sant Feliu de Llobregat)

M. Ester Santiago (Ayuntamiento de Barcelona)

María José Campo (Fundación TIC Salud y Social)

María José Candial (Ayuntamiento de Barcelona)

Mariona Perramon (Consorcio de Servicios Universitarios de Catalunya)

Mireia Bosch (Departamento de Justicia y Calidad Democrática - Generalitat de Catalunya)

Patricia Lozano (Universitat Oberta de Catalunya)

Rosa Parrilla (Departamento de la Presidencia - Generalitat de Catalunya)

Roser Bellido (Departamento de Derechos Sociales e Inclusión -Generalitat de Catalunya)

Ruben Ortiz (Universidad de Barcelona)

Sara Hernández (Fundación TIC Salud y Social)



Barcelona, 2026

El contenido de este documento es propiedad de la Autoridad Catalana de Protección de Datos y está sujeto a la licencia Creative Commons BY-NC-ND,
https://creativecommons.org/licenses/by-nc-nd/4.0/deed.es.

La autoría de la obra debe reconocerse mediante la inclusión de la mención siguiente:
Obra titularidad de la Autoridad Catalana de Protección de Datos.
Con licencia bajo la licencia CC BY-NC-ND.

Aviso: cuando se reutilice o distribuya la obra, deberán indicarse claramente los términos de la licencia.

Aviso legal: Las opiniones expresadas en este documento son responsabilidad de sus autores y no reflejan necesariamente la opinión oficial de la APDCAT. La Autoridad Catalana de Protección de Datos, y los autores y miembros del grupo de trabajo no asumen ninguna responsabilidad por las posibles consecuencias de las acciones de personas físicas o jurídicas derivadas de cualquier información contenida en este documento.

Presentación

En este año 2026 hemos celebrado el décimo aniversario del Reglamento general de protección de datos. Poco puede destacarse que no se haya dicho con anterioridad, pero es evidente que fue una norma determinante para consolidar el derecho fundamental a la protección de datos, tanto en el ámbito europeo como internacional.

De hecho, es la base sobre la que se ha construido toda la estrategia europea de los datos. Así, el Reglamento de inteligencia artificial, de 2024 y modificado en 2026, lo menciona en diversas ocasiones a lo largo de su articulado: por una parte, afirma que no lo desplaza (considerando los artículos 10 y 2.7); por otra, refuerza el papel de las autoridades de control de protección de datos, en artículos como el 5, el 57, el 74 o, una vez designadas las autoridades de protección de los derechos fundamentales, el 77. Y, finalmente, quiero destacar el artículo 27.

Este artículo regula las evaluaciones del impacto sobre los derechos fundamentales en los sistemas de inteligencia artificial (EIDF) y establece la relación entre esa evaluación y la de la protección de datos del RGPD y de la Directiva (UE) 2016/680 (EIPD). Y en la redacción de 2026, a causa de la reforma ómnibus aprobada por la Unión Europea, prevé que en las dos evaluaciones se puedan incluir o referencias cruzadas o las partes pertinentes de la EIPD en la EIDF. Por lo tanto, ambos reglamentos son complementarios.

Pero de la norma a la práctica, hay un trecho. Por ello, desde la Autoridad Catalana de Protección de Datos nos propusimos llenar dos vacíos: el primero, cómo hacer una evaluación de impacto sobre los derechos fundamentales; el segundo, cómo integrar de forma efectiva las dos evaluaciones.

Dimos respuesta al primer vacío en el año 2025, con la presentación del modelo catalán FRIA (por sus siglas en inglés de Fundamental Rights Impact Assessment): una metodología pionera y probada con diversos casos de uso. Fue fruto del esfuerzo de un grupo de trabajo liderado por el profesor Alessandro Mantelero, de la Universidad Politécnica de Turín, en el marco de 'DPD en Red', la comunidad de aprendizaje impulsada por la APDCAT. Este modelo fue uno de los primeros que adoptó la Agencia de Derechos Fundamentales de la Unión Europea. Para este modelo FRIA el 7 de octubre de 2026 se presentó la aplicación FRIA, que permite llevar a cabo la evaluación de impacto de forma automatizada y ágil.

El segundo vacío lo llenamos con estas orientaciones, que son el resultado del esfuerzo del mismo grupo de trabajo, que no se detuvo y ha seguido trabajando para proporcionar a los DPD y a las organizaciones un nuevo recurso que facilitará el cumplimiento normativo.

Desde la APDCAT, seguimos comprometidos con la garantía del derecho a la protección de datos y los demás derechos fundamentales. Continuaremos trabajando en ello junto con los grandes profesionales de los que disponemos en Cataluña.

Meritxell Borràs i Solé
Directora
Autoridad Catalana de Protección de Datos

1. Principales bloques de la EIPD y su integración con el FRIA

En las secciones siguientes se examinan los elementos principales de la EIPD tal como se establecen en el artículo 35 del RGPD. Se describe el contenido de la EIPD a partir de la práctica internacional y de la experiencia del sector público en Cataluña. Con la plantilla de la EIPD de la APDCAT, se proporcionarán directrices para identificar los elementos clave que deben incluirse en cada fase, con el objetivo de crear una EIPD que pueda complementar fácilmente el FRIA exigido por el RIA.

El modelo resultante no pretende sustituir la plantilla de la EIPD de la APDCAT ni las plantillas existentes desarrolladas por diversas instituciones, sino solo presentar un modelo ágil que pueda integrarse fácilmente con la plantilla de FRIA adoptada por la APDCAT. De este modelo FRIA, el 7 de octubre de 2026 se presentó la aplicación FRIA, que permite realizar la evaluación de impacto de forma automatizada y ágil.

La nueva plantilla permite a los usuarios ampliar la sección de la EIPD para incluir una evaluación más amplia del cumplimiento de las disposiciones del RGPD en general y, en especial, cuando se incorpora IA al tratamiento de datos personales.

Este ejercicio de simplificación ha sido necesario atendiendo a lo que establece el artículo 27.4 del RIA, donde se indica que:

> «4. Si ya se cumplen cualesquiera de las obligaciones establecidas en el presente artículo mediante la evaluación de impacto relativa a la protección de datos realizada en virtud del artículo 35 del Reglamento (UE) 2016/679 o del artículo 27 de la Directiva (UE) 2016/680, el responsable del despliegue podrá, al llevar a cabo la evaluación de impacto relativa a los derechos fundamentales a que se refiere el apartado 1 del presente artículo, incluir referencias cruzadas a las secciones pertinentes de dicha evaluación de impacto relativa a la protección de datos o incluir las partes pertinentes de esta en la evaluación de impacto relativa a los derechos fundamentales».

La metodología se estructura a partir de **dos partes comunes a ambas evaluaciones** que, en un modelo integrado, pueden examinarse una sola vez y cuyos resultados pueden utilizarse tanto para la EIPD como para el FRIA. Este análisis es crucial para evitar repetir dos veces la evaluación de los mismos elementos (por ejemplo, el contexto de uso) y para crear un flujo de información coherente entre las dos evaluaciones.

1.1 La descripción sistemática

Esta es la primera parte tanto de la EIPD como del FRIA. Consiste en hacer un análisis de las necesidades y describir las soluciones previstas que se desarrollarán, con referencia a su contexto de uso. Debe proporcionarse información general preliminar a los usuarios de la herramienta de evaluación de impacto, sobre la naturaleza y el propósito de la evaluación y sobre los conceptos generales de evaluación basada en el riesgo, que están presentes tanto en el RGPD como en el RIA.

En lo que respecta a la descripción de las soluciones previstas, los proyectos que impliquen el uso de datos personales, así como los que impliquen IA, deben describir cómo se utilizan tanto los datos como la IA. Para ello, es necesario proporcionar información detallada sobre la

naturaleza de los datos y su tratamiento, que se integrará con la información sobre el sistema de IA utilizado. De la misma manera, se necesita información sobre las personas directamente implicadas en el desarrollo del proyecto y su función en virtud del RGPD (responsable del tratamiento, corresponsable del tratamiento, encargado del tratamiento, subencargado del tratamiento) y del RIA (proveedor, responsables del despliegue), las posibles categorías de titulares de derechos afectados y los contextos de uso.

1.2 La evaluación

Respecto a la fase de evaluación, cabe señalar que la EIPD y el FRIA son obligaciones legales con un alcance limitado, definido respectivamente por el artículo 35 del RGPD y el artículo 27 del RIA. Asimismo, en el ámbito de la protección de datos, al igual que en el de la IA, la evaluación previa de riesgos tiene un alcance que va más allá de las evaluaciones de impacto reguladas.

En virtud del RGPD, los riesgos deben tenerse en cuenta al aplicar el Reglamento, incluso si no suponen un riesgo elevado para los derechos y libertades de las personas físicas. También en estos casos sigue siendo necesario aplicar adecuadamente todos los principios establecidos en el artículo 5 del RGPD y en las disposiciones pertinentes del Reglamento, con el fin de minimizar cualquier impacto, incluso los de menor alcance, sobre el derecho a la protección de datos y otros derechos fundamentales. Por lo tanto, una evaluación general de riesgos es inherente a todas las actividades de tratamiento, mientras que una EIPD formal solo es obligatoria en casos de alto riesgo.[1]

Lo mismo se aplica al FRIA. A pesar de limitarse a determinadas categorías de responsables del despliegue y determinadas situaciones, la protección garantizada de los derechos fundamentales exige el deber de proteger activamente estos derechos y un FRIA es una herramienta útil para lograr este objetivo. Además, el FRIA, en términos de metodología para evaluar el impacto sobre los derechos fundamentales, también la **pueden utilizar los proveedores de IA** para cumplir con el artículo 9 en lo que respecta a los riesgos que plantean para los derechos fundamentales y, en términos generales, para cualquier entidad que incorpore sistemas de IA en su organización, dado que en el contexto de la Unión Europea la garantía y protección de los derechos fundamentales, recogidos en la Carta de los Derechos Fundamentales de la Unión Europea, es común a cualquier actuación.

En lo que respecta al cumplimiento estricto del RGPD y el Reglamento de IA, un modelo que integre la EIPD y el FRIA requiere un análisis previo de los requisitos legales establecidos por estas dos normativas a fin de determinar los supuestos en que ambos son obligatorios. Esta evaluación se realiza en la sección 2 del modelo de evaluación (Necesidad de realizar una EIPD y un FRIA).

En cuanto a la evaluación de riesgos para los «derechos y libertades de las personas físicas» (artículo 35 del RGPD) y «el impacto en los derechos fundamentales» (artículo 27 de la Ley de IA), hay diferencias porque el Reglamento europeo de IA, en su artículo 1, se refiere a la «protección de [...] los derechos fundamentales consagrados en la Carta». No obstante, más

[1] Véase también el artículo 29 del Grupo de trabajo de protección de datos-Data Protection Working Party (nota 2), 8 («En los casos en que no esté claro si se requiere una EIPD, el WP29 recomienda que se realice una EIPD de todos modos, ya que una EIPD es una herramienta útil para ayudar a los responsables a cumplir con la legislación de protección de datos»).

allá de la calificación jurídica de estos derechos, el enfoque metodológico es el mismo: se centra en el riesgo en términos de perjuicio a estos derechos, teniendo en cuenta la probabilidad de que se produzca un daño y la gravedad de dicho daño.[2]

Como se puede observar en las tablas siguientes, extraídas de la plantilla de evaluación de impacto en protección de datos de la CNIL[3] y el FRIA de la APDCAT[4], la metodología de evaluación de riesgos está alineada de la misma manera en ambos instrumentos.

[2] Consulte el artículo 3, apartado 2, de la Ley de IA; el artículo 25, apartado 1, y el Considerando 75 del RGPD. Según el considerando 76 del RGPD, «La probabilidad y gravedad del riesgo para los derechos y libertades del interesado debe determinarse de acuerdo con la naturaleza, el alcance, el contexto y los fines del tratamiento de datos»
[3] Véase CNIL (nota 7), 20.
[4] Véase Autoridad Catalana de Protección de Datos (nota 6), 19.

Tabla 3. CNIL EIP

3.2 Risk assessment: potential privacy breaches

Analysis and assessment of risks

Risk	Main risk sources	Main threats	Main potential impacts	Main controls reducing the severity and likelihood	Severity	Likelihood
Illegitimate access to data						
Unwanted change of data						
Disappearance of data						

Assessment of the risks

Risks	Acceptable/can be improved on?	Corrective controls	Residual severity	Residual likelihood
Illegitimate access to data	[*The assessor must determine whether the existing or planned controls (already undertaken) sufficiently reduce this risk for it to be deemed acceptable.*]	[*Where applicable, he shall indicate here any additional controls that would prove necessary.*]		
Unwanted change of data	[*The assessor must determine whether the existing or planned controls (already undertaken) sufficiently reduce this risk for it to be deemed acceptable.*]	[*Where applicable, he shall indicate here any additional controls that would prove necessary.*]		

Tabla 4. APDCAT FRIA

Taula 2A. Gestió de riscos (I)

Drets/llibertats afectats	Probabilitat	Gravetat	Impacte global	Mesures per prevenir/mitigar els impactes

Taula 3A. Gestió de riscos (II)

Drets/llibertats afectats	Probabilitat (residual)	Gravetat (residual)	Impacte residual

De acuerdo con la metodología general de evaluación de riesgos**, se examina la probabilidad y la gravedad de los posibles daños** basándose en el diseño del proyecto, se prevén las posibles medidas de mitigación y se lleva a cabo una nueva evaluación, para definir así el impacto de estas medidas y los riesgos residuales. Este proceso iterativo es coherente con el enfoque basado en el riesgo, adoptado tanto por la EIPD como por el FRIA.

Mientras que la EIPD analiza los diversos riesgos de un derecho único, reflejando la naturaleza procedimental de la protección de datos en términos de posibles violaciones (por ejemplo, acceso no autorizado a los datos o cambios no deseados), el FRIA considera cada derecho afectado en toda su dimensión, sin identificar subconjuntos de riesgos para ningún tipo de perjuicio potencial. Esto también se debe a que la protección de los derechos fundamentales distintos al derecho a la protección de datos no tiene una naturaleza procedimental similar y, en sus respectivas normativas, se basa en la definición de un ámbito de protección concreto y en la prohibición de interferir en él, salvo que prevalezcan otros bienes e intereses jurídicos de acuerdo con la ley.

Por lo tanto, para alinear la EIPD y el FRIA, no es necesario revisar las matrices utilizadas en la EIPD para evaluar el nivel de riesgo en la protección de datos, ya que estas matrices siguen formando parte de la evaluación general del impacto sobre este derecho.

No obstante, las medidas de mitigación adoptadas en materia de protección de datos también pueden beneficiar a otros derechos, lo que debe tenerse en cuenta en cuanto a los controles establecidos y actualizar la sección C del cuestionario FRIA.

Además, debe tenerse en cuenta que el tratamiento de datos personales puede generar riesgos para otros derechos y libertades de las personas, más allá del propio derecho a la protección de los datos personales. Por lo tanto, la EIPD también puede ayudar a identificar impactos potenciales en otros derechos derivados del tratamiento realizado y, en especial, del uso que se haga de la IA.

1.3 Medidas de mitigación

El bloque final de la EIPD consiste en identificar las medidas de mitigación más adecuadas para reducir el impacto en la protección de datos.

De conformidad con el artículo 35, apartado 7, letra *d*, estas medidas son las «previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.»

Entre estas medidas de mitigación, se pueden incluir los elementos del cumplimiento del RGPD que pueden contribuir a reducir el riesgo. Además, estos elementos también son relevantes desde la perspectiva del FRIA, ya que pueden ayudar a reducir los efectos negativos sobre otros derechos y libertades.

La calidad de los datos, por ejemplo, puede reducir los sesgos y los efectos negativos sobre el derecho a la no discriminación, mientras que la supervisión humana[5] puede ser eficaz en la toma de decisiones basada en datos, no solo en términos de cumplimiento del RGPD, sino también como una intervención que mitiga el impacto sobre otros derechos afectados[6].

En relación con lo anterior, las diversas preguntas sobre estos diferentes aspectos incluidos en la EIPD deben replantearse dentro de la lógica de las posibles medidas que haya que adoptar para mitigar los riesgos, en lugar de como elementos de una verificación del cumplimiento.

2. Flujo de trabajo integrado de AIPD-FRIA y diseño del modelo

Conforme a las consideraciones expuestas en las secciones anteriores, el flujo de trabajo general de la plantilla del modelo DPIA-FRIA puede describirse como se muestra en el diagrama siguiente:



[5] Ver también el artículo 14 del RIA
[6]La misma consideración puede aplicarse a la transparencia, que es un factor que permite comprender las posibles consecuencias negativas del uso de los datos, también en el contexto de la IA, y que puede combinarse con las obligaciones de transparencia previstas en el RIA (ver también el artículo 13 del RIA). El correcto cumplimiento de estas obligaciones de transparencia por parte de los proveedores de sistemas de IA es esencial para el cumplimiento de las obligaciones del responsable del tratamiento, en términos del RGPD.


DPD
en xarxa