Organiza

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Foro GRC
Privacidad · IA · Ciberseguridad

II Insight IA 2025

Foro GRC

Presentación: Primera Certificación Profesional Gobierno, Riesgo y Cumplimiento en Inteligencia Artificial (CP-GRC-IA)

Ponencia de *Alessandro Mantelero*: “Evaluación de Impacto en Derechos Fundamentales en Inteligencia Artificial”

Jueves 18 septiembre - 16:30 - streaming

Partners Estratégicos

Telefónica Tech

GOVERTIS
Part of Telefónica Tech

CANAL AEC

"Presentación de la certificación CP-GRC-IA de la AEC"

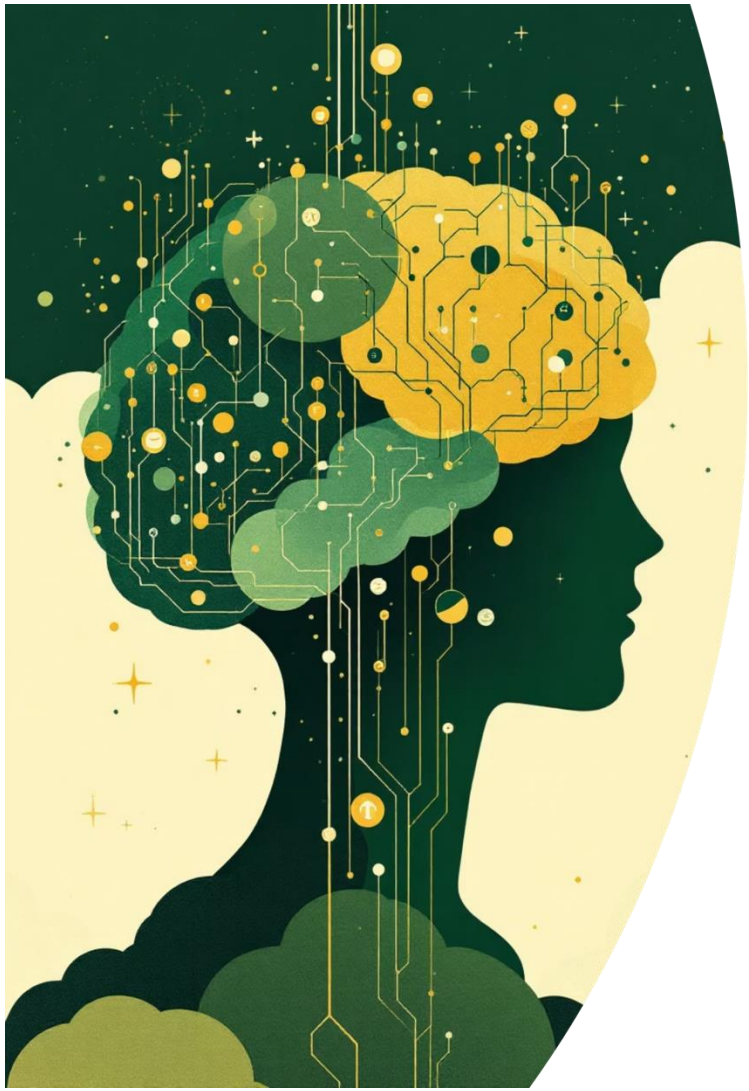
Alberto González

Director de Operaciones y TI, AEC

https://www.linkedin.com/in/albertogonzalezmerino/

Certificación Profesional GRC-IA

El futuro de la gobernanza responsable en inteligencia artificial



Organiza:
AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Partners Estratégicos:
Telefónica Tech
GOVERTIS
Part of Telefónica Tech

La era de la IA: Oportunidades y Desafíos

Transformación Sin Precedentes

La IA está revolucionando la Sociedad y las empresas a un ritmo acelerado.

Riesgos Emergentes

Sesgos, falta de transparencia, amenazas a la privacidad y la ciberseguridad.

Nueva Necesidad

Surge la figura del Profesional GRC-IA para abordar estos desafíos críticos.

El Profesional GRC-IA

Un pilar estratégico para la gestión responsible de la inteligencia artificial

Definición del Perfil

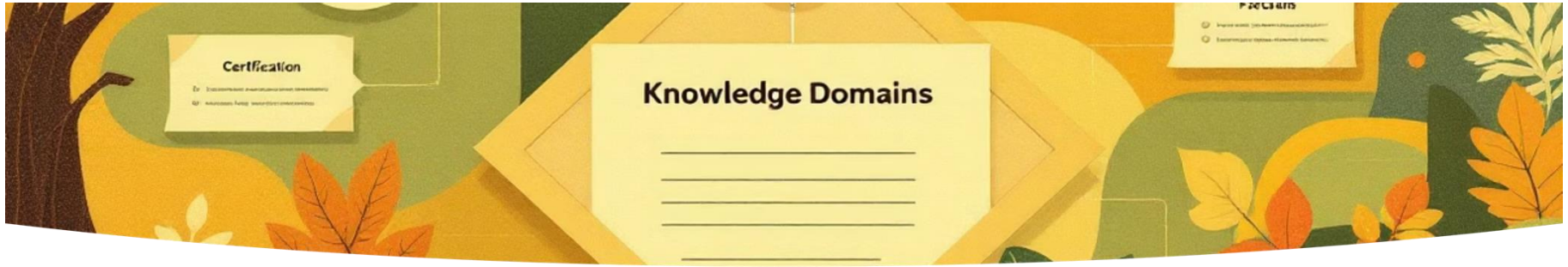
- ✓ Gestiona de forma integrada el Gobierno, Riesgo y Cumplimiento de la IA. Diseña, supervisa y garantiza sistemas éticos, seguros y alineados con marcos regulatorios.
- ✓ Su función es asegurar que la IA sea transparente, justa, segura y alineada con las regulaciones vigentes, con un sólido entendimiento del impacto y los riesgos tecnológicos y las nociones adecuadas sobre la tecnología que soporta este nuevo paradigma

Rol Multidisciplinar

- ✓ Puente esencial entre equipos técnicos, directivos y organismos reguladores. Conector entre áreas legal, tecnológica y de negocio.

¿Para quién es esta Certificación?

- Profesionales GRC. Especialistas en cumplimiento que buscan adaptarse a la era de la IA.
- Consultores y Auditores
- Directores de innovación, IT y cualquier profesional que desee especializarse.
- Representantes RIA, DPDs, CISOs y profesionales de ciberseguridad.
- Estudiantes universitarios que buscan especializarse en esta área emergente y estratégica.



Dominios de conocimiento CP-GRC-IA

PARTE GENERAL: Fundamentos GRC

D1	Fundamentos Inteligencia Artificial
D2	Fundamentos Protección de Datos
D3	Fundamentos Seguridad de la Información
D4	Fundamentos Sistemas de Gestión

PARTE ESPECÍFICA: GRC aplicado a la IA

D1	Fundamentos avanzados de la Inteligencia Artificial
D2	Cumplimiento Legal y Normativo de la IA
D3	Marco Organizativo y Gobierno Corporativo de la IA
D4	Gestión de Riesgos de IA y Evaluación de Impacto

Proceso de Certificación

01

Prerrequisitos

- Cumplimiento de prerrequisitos basados en experiencia o formación.
- Obtención de la certificáción vía méritos excepcionales (*temporalmente*).

02

Examen Online

80 preguntas tipo test. Puntuación mínima: 70% global y 50% por cada parte. Dos oportunidades .

03

Registro y publicación

04

Mantenimiento

Validez de 3 años. Renovación con 30 horas de formación continua (*mínimo 10h formación específica IA*).

Más información

Proceso de Certificación. Prerrequisitos.

- **Opción 1: Experiencia**: 3 años de experiencia profesional acreditable, en al menos 2 de los dominios recogidos en la PARTE GENERAL: Fundamentos GRC.
- **Opción 2: Formación:** 140 horas formación, en al menos 2 de los dominios recogidos en la PARTE GENERAL: Fundamentos GRC.
- **Opción 3: Formación especializada GRC IA:** «Programa Experto en GRC IA» de la AEC
- **Opción 4:** Excepcional y temporal (hasta marzo de 2026) obtención de la certificación con acreditación de méritos extraordinarios

Más información

Proceso de Certificación. Convocatorias examen.

- **25 de noviembre de 2025**
- **16 de diciembre de 2025**
- **29 de enero de 2026**

Ventajas de la Certificación

Reconocimiento Profesional

Te posiciona como referente en gestión ética y responsable de la IA.

Empleabilidad

Altamente valorado en mercado emergente, incrementando oportunidades laborales.

Red de Contactos

Integración en comunidad de expertos para compartir experiencias.

Impacto Organizacional

Aportas valor estratégico, mitigando riesgos y asegurando cumplimiento.

La AEC: Experiencia y Rigor

CERPER: Centro de Registro y Certificación de Personas

- ✓ Certificando personas desde 1997
- ✓ Agente en España de la **European Organization for Quality** (EOQ)
- ✓ Más de 13.000 certificados emitidos, en 15 ámbitos diferentes.
- ✓ Único organismo acreditado por ENAC en España para la certificación de personas en los ámbitos de **gestión de la calidad, gestión ambiental y, recientemente, innovación**
- ✓ **Certificadora Líder en Protección de Datos**
- ✓ **Ahora hemos creado esta nueva certificación, con esquema propiedad de la AEC.**

Profesional CERPER Certificado

La AEC: Experiencia y Rigor

¿Por qué AEC Formación?

El mejor aliado: confianza y experiencia

+ 60 años formando profesionales
+ 70.000 alumnos nos han elegido

Más allá del conocimiento: competencias y habilidades

Compartir conocimientos y experiencias reales
Aplicación inmediata del valor aprendido en las organizaciones

Metodologías adaptadas a la realidad de las organizaciones

+ 350 programas formativos al año
Directo/Presencial, Online, Mixta e Incompany

Profesorado referente

Especialistas en sus sectores, con experiencia real en las empresas
100% en activo. Experiencia pedagógica y fuerte vocación eductiva

Opciones de Formación AEC

Curso de Preparación

- ✓ Online a tu ritmo, temario descargable y más de 240 preguntas de simulación para el examen.
- ✓ Recomendado para la opción 1 y 2 de los prerequisitos de acceso.

Programa Experto GRC IA

- ✓ Formación completa de 110 horas con tutorías y clases en directo.
- ✓ Acceso directo a la certificación.
- ✓ Formación bonificable.

Profesores y entidades colaboradoras de Formación AEC GRC-IA

Con la colaboración de:

ODISEIA

Organiza:

QAEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Partners Estratégicos:

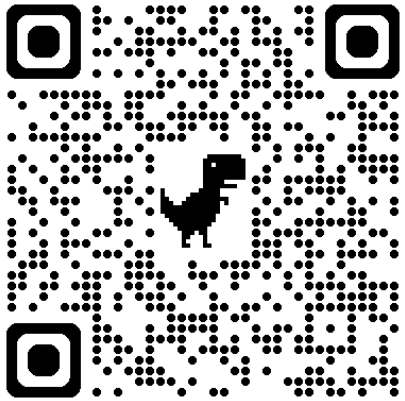
Telefónica Tech

GOVERTIS
Part of Telefónica Tech

¡GRACIAS!

¡Súmate al Foro GRC!

https://www.aec.es/espacios-de-relacion/comunidades



Organiza

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Foro GRC
Privacidad · IA · Ciberseguridad

II Insight IA 2025

Foro GRC

Presentación: Primera Certificación Profesional Gobierno, Riesgo y Cumplimiento en Inteligencia Artificial (CP-GRC-IA)

Ponencia de *Alessandro Mantelero*: “Evaluación de Impacto en Derechos Fundamentales en Inteligencia Artificial”

Jueves 18 septiembre - 16:30 - streaming

Partners Estratégicos

Telefónica Tech

GOVERTIS
Part of Telefónica Tech

CANAL AEC

Metodología de evaluación del impacto sobre los derechos fundamentales en IA

18 de septiembre de 2025

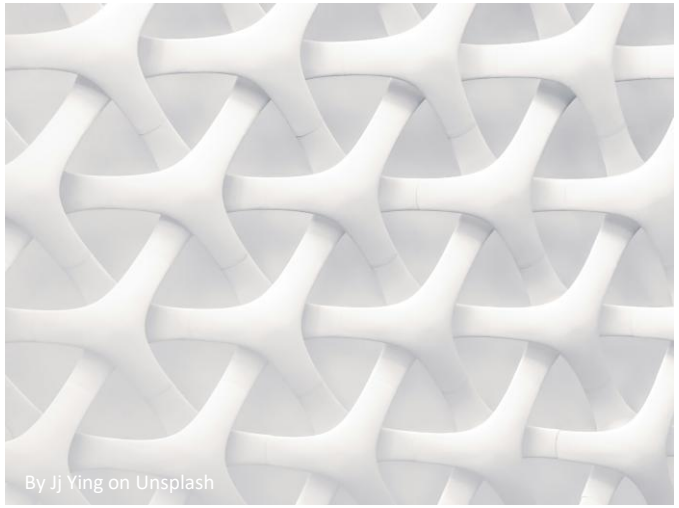
Alessandro Mantelero
Catedra Jean Monnet de Sociedades digitales mediterráneas y derecho| Univeridad Politécnica de Turín

I. Las raíces del FRIA


By Florian Schmid on Unsplash

- Las raíces del FRIA en los Principios Rectores sobre Empresas y Derechos Humanos de Naciones Unidas
- Diferencia entre directrices, metodologías y modelos
- Diferencia entre el análisis de impacto algorítmico (AIA), la evaluación ética y la evaluación de estrategias para el desarrollo de la IA
- Diferencias entre los modelos
    - Modelos de concienciación y modelos de evaluación del riesgo
    - Modelos lineales con diseño Why-What-How y modelos de evaluación de riesgo circulares
    - Modelos matemáticos y enfoque jurídico de la FRIA

II. Errores de método: matematizar el FRIA o utilizar la lógica formal



Combinaciones matemáticas de elementos heterogéneos, incluidos los derechos fundamentales (por ejemplo, Bertaina et al. 2025)

- Media del riesgo total, que incluye características heterogéneas (tipología del algoritmo, propiedad y control, proceso de toma de decisiones y supervisión humana, datos de entrada, rendimiento, transparencia, explicabilidad, equidad, seguimiento y mantenimiento)
- Impacto conjunto en los derechos fundamentales
- Ponderación arbitraria de los riesgos generales (30 %) y del impacto conjunto en los derechos fundamentales (70 %)

Table 8
The list of possible values for class severity, class effort and duration and class probability of occurrence, together with an explanation of the value meaning..[13]

Value	Class Severity	Class Effort and Duration	Class Probability of Occurrence
Neutral (-)	no impact at all is expected for the considered FR, and thus the Severity/Effort and Duration of Classes is not even evaluated		
Irrelevant (0)	the Severity/Effort and Duration is evaluated, and the result is that no impact or an irrelevant impact is expected		Probability of Occurrence < 1%.
Low (1)	a low impact is expected		1% < Probability of Occurrence < 35%.[7]
Medium (2)	a medium impact is expected		35% < Probability of Occurrence < 70%.[7]
High (3)	a high impact is expected		Probability of Occurrence > 70%.[7]

- Dependencia de series históricas en lugar de un enfoque basado en rangos (definición arbitraria de series relevantes)
- Combinaciones opacas de parámetros clave (tablas 8 y 9)

Table 9
The mapping table that defines the value for class risk score given a combination of class severity, class effort and duration and class probability of occurrence.

Class Risk Score	Corresponding combinations of: Class severity – class effort and duration – class probability of occurrence
0	1–0-1; 0–3-1; 0–2-1; 0–1-1; 0–0-1; 0–3-2; 0–2-2; 0–1-2; 0–0-2; 0–3-3; 0–2-3; 0–1-3; 0–0-3; 3–3-0; 3–2-0; 3–1-0; 3–0-0; 2–3-0; 2–2-0; 2–1-0; 2–0-0; 1–3-0; 1–2-0; 1–1-0; 1–0-0; 0–0-0
1	3–0-1; 2–1-1; 2–0-1; 2–0-2; 1–2-1; 1–1-1; 1–1-2; 1–0-2; 1–0-3
2	3–3-1; 3–2-1; 3–1-1; 3–1-2; 3–0-2; 3–0-3; 2–3-1; 2–2-1; 2–2-2; 2–1-2; 2–1-3; 2–0-3; 1–3-1; 1–3-2; 1–2-2; 1–2-3; 1–1-3
3	3–3-2; 3–2-2; 3–3-3; 3–2-3; 3–1-3; 2–3-2; 2–3-3; 2–2-3; 1–3-3
-	Whenever Class Severity is Neutral (and as a consequence Class Effort and Duration is Neutral), independently of Class Probability of Occurrence

Politecnico di Torino

Uso de la lógica formal abstracta (por ejemplo, García-Godínez, Miguel. 2025, https://doi.org/10.1007/s43681-025-00761-1)

S1. AIA and EU Fundamental Rights

Let $\mathcal{W}_1$ be the initial set of empirical information consisting of $\{R(a), I(a), B(a), S(a), N(a)\}$. Where $R(a)$ represents the premise that the AI is intended to be used for recruitment; $I(a)$ that the AI is designed for conducting interviews; $B(a)$ that the AI uses biometrics; $S(a)$ that the AI is used for screening application materials and online activity; and $N(a)$ that the AI employs NLP.[30]

And let $\mathcal{D}_1$ be the initial set of defaults consisting of $\{\delta_1, \delta_2, \delta_3, \delta_4\}$ (with no priority relation between them, i.e., $<= \emptyset$). Where $\delta_1 = \{R(x) \rightarrow HR(x)\}$ (the default that if the AI is intended for recruitment purposes, then it is a high-risk system)[31]; $\delta_2 = \{HR(x) \rightarrow FRIA(x)\}$ (the default that if the AI is classified as high-risk, then a FRIA must be implemented before deployment)[32]; $\delta_3 = \{APP(y) \rightarrow ND(y)\}($ the default that anyone applying for a job has the right to non-discrimination)[33]; and $\delta_4 = \{APP(y) \rightarrow PR(y)\}($ the default that anyone applying for a job has the right to privacy).[34]

In this scenario, given that $\delta_1 - \delta_4$ are all binding, Cybercruitment is rationally committed to accepting, on the one hand, that since the AI system is intended to be used for recruitment purposes, then it is high-risk ($HR(a)$) and so a FRIA must be conducted prior to deployment ($FRIA(a)$); and on the other, that if someone b submits a job application, their fundamental rights of non-discrimination ($ND(b)$) and privacy ($PR(b)$) must be protected throughout the implementation of the AI system.

Now, in order to determine whether the AI poses any serious risk to these fundamental rights, Cybercruitment can move then to the next scenario.

S2. Risk Identification

Let $\mathcal{W}_2 = \{\mathcal{W}_1\}$, $\mathcal{D}_2 = \{\mathcal{D}_1 \cup (\delta_5, \delta_6)\}$, and $< = \emptyset$. Where $\{\mathcal{W}_1\}$ and $\{\mathcal{D}_1\}$ are as before, and $\delta_5 = \{B(x) \rightarrow \neg ND(y)\}($ if the AI uses inferential biometric technology, then it undermines the right to non-discrimination) and $\delta_6 = \{N(x) \rightarrow \neg PR(y)\}($ if the AI uses NLP to score application materials, then it affects right to privacy).

The rationale behind δ_5 is that biometric systems may disproportionately disadvantage certain demographic groups due to biases in data and algorithmic design [56]. And the justification behind δ_6 is that NLP may expose individuals to invasive and potentially prejudiced assessments [57]. So, in the specific situation where b is evaluated through the AI, the proper scenario would then yield both $\neg ND(b)$ and $\neg PR(b)$.

However, this result conflicts with the consequence that obtains from $\mathcal{S}1$. In particular, with the normative conclusions that follow from δ_3 and δ_4, viz., that the applicant's right to non-discrimination and privacy must be protected (i.e., $ND(b)$ and $PR(b)$). To solve this conflicting situation, Cybercruitment can move next to the risk mitigation scenario.

III. Los elementos de la FRIA

- Fase de planificación y delimitación del alcance (cuestionario de evaluación)
  - Centrarse en las principales características del producto/servicio y en el contexto en el que se utilizará
- Fase de recopilación de datos y análisis de riesgos
  - Identificar los riesgos potenciales y estimar los posibles impactos en los derechos fundamentales
- Fase de gestión de riesgos
  - Adoptar las medidas adecuadas para prevenir o mitigar los riesgos identificados, comprobar la eficacia de estas medidas y realizar un seguimiento continuo cuando sea necesario

- **El cuestionario de evaluación**
  - Contextualizar el sistema de IA y su uso
  - Identificar las categorías que podrían verse afectadas
  - La FRIA no consiste en marcar casillas, sino que es una herramienta de diseño.

Sección A Descripción y análisis del sistema de IA, incluidos los flujos de datos relacionados	¿Cuáles son los principales objetivos del sistema de IA? ¿Cuáles son las principales características del sistema? ¿En qué países se ofrecerá? ¿Qué tipos de datos se tratan (personales, no personales, categorías especiales)? Identificación de los posibles titulares de derechos: ¿quiénes son los individuos o grupos que pueden verse afectados por los sistemas de IA? ¿Se incluyen entre ellos individuos o grupos vulnerables? Identificación de los responsables: ¿qué personas/entidades están implicadas en el diseño, desarrollo y despliegue de los sistemas de IA? ¿Cuál es su papel?

- Las secciones del cuestionario
  - Sección A - Descripción y análisis del sistema de IA, incluidos los flujos de datos relacionados
  - Sección B - Contexto de derechos fundamentales
  - Sección C - Controles implementados
  - Sección D - Intervención de las partes interesadas y diligencia debida

Análisis y gestión de riesgos

- Evaluación del impacto
  - Uso de escalas (nivel mínimo/máximo de impacto)
  - Uso de variables ordinales (por ejemplo, bajo, medio, etc.)
  - Las escalas y las variables facilitan la evaluación comparativa, la transparencia y la rendición de cuentas
- Adopción de medidas adecuadas de prevención y mitigación de riesgos
- Aplicación de dichas medidas
- Seguimiento

- Componentes de riesgo (índice de riesgo) para cada derecho que pueda verse afectado
  - Probabilidad de impacto adverso (basada tanto en casos anteriores, analizando situaciones comparables, como en el uso de técnicas analíticas y de simulación, basadas en posibles escenarios de uso)
    - Probabilidad de impactos perjudiciales
    - Exposición

Tabla 1. Probabilidad

Bajo	El riesgo de perjuicio es improbable o altamente improbable
Medio	El riesgo puede producirse
Alto	Existe una alta probabilidad de que se produzca el riesgo
Muy alto	Es muy probable que se produzca el riesgo

Tabla 2. Exposición

Bajo	Pocos o muy pocos de la población identificada de titulares de derechos están potencialmente afectados
Medio	Parte de la población identificada está potencialmente afectada
Alto	La mayoría de la población identificada está potencialmente afectada
Muy alto	Casi toda la población identificada está potencialmente afectada

		Probabilidad			
		Baja	Media	Alta	Muy alta
Exposición	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

Bajo	Medio	Alto	Muy alto

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

- Gravedad (mayor énfasis en el análisis jurídico relativo a la gravedad del perjuicio: jurisprudencia sobre derechos humanos/fundamentales, marco jurídico)
  - Gravedad: gravedad del perjuicio en el ejercicio de los derechos y libertades (gravedad), teniendo en cuenta el impacto específico en determinados grupos, la vulnerabilidad y las situaciones de dependencia
  - Esfuerzo: el esfuerzo por superar y revertir los efectos adversos (esto también pone de relieve la dimensión contextual y las interacciones)

- No existe un índice compuesto que combine todos los impactos potenciales sobre los derechos
- Factores que pueden excluir el riesgo (por ejemplo, el carácter obligatorio de determinadas características con impacto)
- El desarrollo de la IA centrado en el ser humano exige rendición de cuentas y transparencia
- Las herramientas utilizadas: escalas de riesgo y matrices (legibilidad, comprensibilidad y comparabilidad)
- El uso de matrices para construir índices de riesgo
    - Relativamente fácil de usar y explicar
    - Transparencia y rendición de cuentas

- Gestión de riesgos
  - Identificar las medidas adecuadas y evaluar el riesgo residual
  - Si bien deben mitigarse todos los impactos, los diferentes niveles de impacto sobre los distintos derechos pueden ayudarnos a comprender dónde intervenir primero y dónde es necesario revisar más a fondo el diseño de la IA
  - Una evaluación dinámica y circular

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

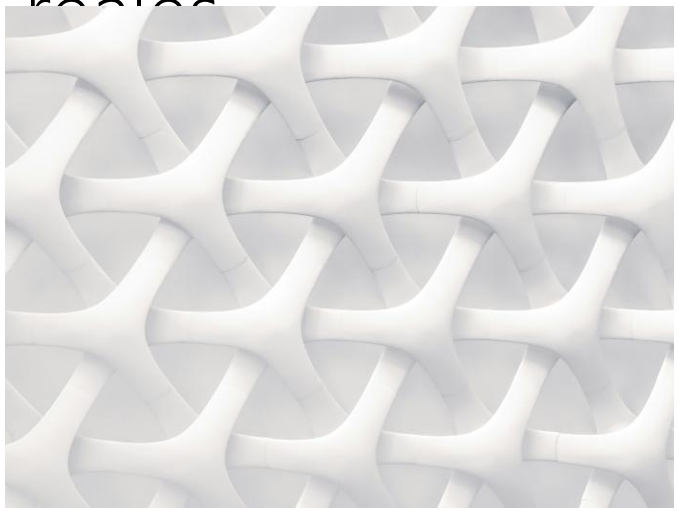
Tabla 2A. Gestión de riesgos (I)

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

Tabla 3A. Gestión de riesgos (II)

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

IV. Un modelo científicamente validado y probado en aplicaciones reales



- Mantelero, A. 2024. The Fundamental Rights Impact Assessment (FRIA) in the AI Act: roots, legal obligations and key elements for a model template. Computer Law & Security Review. 54, https://doi.org/10.1016/j.clsr.2024.106020 (open access)

- Mantelero, A. and Esposito, M.S. 2021. An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems. Computer Law & Security Rev. 41, https://doi.org/10.1016/j.clsr.2021.105561 (open access)

- Desde los modelos teóricos hasta su validación concreta
  - Una plataforma de analítica avanzada del aprendizaje
  - Una herramienta para la gestión de los recursos humanos
  - Una herramienta de imágenes médicas impulsada por IA para la detección del cáncer
  - ATENEA, IA al servicio de las personas mayores

Una herramienta de imagen médica basada en IA para la detección del cáncer

- Primera fase: desarrollo de un sistema de IA basado en imágenes médicas (5000 pacientes de diez países europeos)
- Segunda fase: validación del sistema de IA en ocho centros sanitarios de todo el mundo fuera de Europa (un centro sanitario en Asia, uno en África y uno en Sudamérica)
- Evaluación

Planificación y alcance

Sección A Descripción y análisis del sistema de IA, incluidos los flujos de datos relacionados	**¿Cuáles son los principales objetivos del sistema de IA?**	Mejorar el tratamiento de los pacientes con cáncer X mediante la predicción de: a) Respuesta del paciente al tratamiento. b) Efectos secundarios (toxicidad y sensibilidad). c) Previsiones para los próximos cinco años.
	¿Cuáles son las principales características del sistema?	Reconocimiento de imágenes basado en la IA. Uso de imágenes médicas para predecir la respuesta de un paciente a un determinado tratamiento y para ayudar a los profesionales sanitarios a determinar su aplicación en casos concretos, así como el nivel de uso una vez que se aplique.
	¿En qué países se ofrecerá?	Distribución mundial.
	¿Qué tipos de datos se tratan (personales, no personales, categorías especiales)?	• Datos demográficos (sexo, edad y país). • Características del cáncer (tipo de cáncer y zona afectada). • Estadio del cáncer y subtipo molecular. • Información relativa al tratamiento previo. • Régimen de tratamiento (esquema y duración). • Informe de patología (post-tratamiento).
	Identificación de los posibles titulares de derechos: ¿quiénes son los individuos o grupos	Personas entre 18 y 85 años.

	que pueden verse afectados por los sistemas de IA? ¿Se incluyen entre ellos individuos o grupos vulnerables?	Dado que todas las personas implicadas están afectadas por el cáncer, deben considerarse vulnerables, debido a sus condiciones de salud y a las relaciones entre estas condiciones y la finalidad del sistema de IA.
	Identificación de los responsables: ¿qué personas/entidades están implicadas en el diseño, desarrollo y despliegue de los sistemas de IA? ¿Cuál es su papel?	En el diseño participan hospitales y centros de investigación; estos últimos sólo en el diseño del sistema de IA y los primeros también en el tratamiento sanitario relacionado.
Sección B Contexto de derechos fundamentales	**¿Qué derechos fundamentales se ven potencialmente afectados por el uso del sistema de IA?**	☒ Derecho a la intimidad (incluida la protección de datos). ☒ Libertad frente a la discriminación. ☒ Derecho a un nivel de vida adecuado (incluido el derecho a la salud física y mental).
	¿Qué instrumentos jurídicos internacionales/regionales de protección de los derechos humanos/fundamentales se han aplicado a nivel operativo?	Declaración universal de los derechos humanos, Carta de derechos fundamentales de la UE, normativas de protección de datos aplicable.
	¿Cuáles son los tribunales u organismos más relevantes en materia de derechos fundamentales en el contexto?	Autoridades de protección de datos del país/región donde se desarrollen y utilicen los sistemas de IA, y órganos jurisdiccionales, Tribunal de Justicia de la Unión Europea y Tribunal Europeo de Derechos Humanos.

	¿Cuáles son las decisiones y disposiciones más relevantes en materia de derechos humanos/fundamentales?	No aplicable
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 previsto la constitución de un comité de ética específico para el proyecto.
	¿Se ha realizado, desarrollado y aplicado una evaluación de impacto en relación con cuestiones específicas (por ejemplo, protección de datos) o algunas características del sistema (por ejemplo, el uso de la biometría)?	Se debe realizar una evaluación de impacto sobre la protección de datos.
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?**	Pacientes con cáncer X [anonimizados].
	¿Qué partes interesadas, además de los individuos o grupos que puedan verse afectados por los sistemas de IA, deben participar (por ejemplo, la sociedad civil y las organizaciones internacionales, expertos, asociaciones industriales, periodistas)?	Asociaciones de pacientes con cáncer.
	¿Hay otros titulares de obligaciones que deban participar, aparte del proveedor y el responsable del despliegue de IA (por ejemplo, autoridades nacionales, organismos gubernamentales)?	Autoridad de protección de datos, Departamento de Sanidad local, comité ético de investigación científica, autoridad de supervisión de IA.

	¿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)?	No
	¿Ha llevado a cabo el proveedor de IA 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?**	N/A
	¿El proveedor y el responsable del despliegue de la IA han comunicado públicamente las posibles repercusiones del sistema de IA en los derechos fundamentales?	No
	¿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?	N/A

Politecnico di Torino

Tabla 1A. Recogida de datos y análisis de riesgos

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/H	MA

Probabilidad			
Baja	Media	Alta	Muy alta

Tabla 6. Gravedad (*severity*)

		Gravedad			
		Baja	**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			
Baja	Media	Alta	Muy alta

Derechos/libertades potencialmente afectados	**Descripción del impacto**	Probabilidad			Gravedad		
		Probabilidad de resultados adversos	Exposición	**Probabilidad**	Gravedad	Esfuerzo	**Gravedad**
Protección de datos/Privacidad	El desarrollo del sistema de IA se basa en el uso de categorías especiales de datos personales y otra información personal de los pacientes. Cualquier operación de tratamiento que no cumpla la normativa aplicable en materia de protección de datos personales podría afectar a este derecho.	[Baja] El proyecto está sujeto a evaluaciones específicas de impacto ético y de protección de datos.	[Muy alta] El impacto afecta potencialmente a todas las personas a las que se aplica el algoritmo.	**[Media]**	[Media] El tratamiento ilegal de datos sanitarios relacionados con el cáncer y el uso ilícito de esta información pueden ser invasivos y afectar a la intimidad de las personas.	[Medio] La recogida y el tratamiento ilícitos de datos pueden detectarse y detenerse, con la supresión de la información que se haya recogido ilegalmente.	**[Media]**
No discriminación	El algoritmo se entrenó con datos de centros sanitarios europeos, por lo que es posible que se produzcan	[Alta] La etnia puede provocar algunas diferencias en las imágenes médicas, que	[Muy alta] Todas las personas del grupo pertinente (grupo étnico)	**[Muy alta]**	[Muy alta] Impacto negativo en la igualdad de acceso a la asistencia sanitaria y en la	[Alto] Sería necesario adaptar o incluso volver a entrenar el	**[Muy alta]**

	discriminaciones cuando se utilice en los tres centros sanitarios no pertenecientes a la UE.	pueden afectar a la precisión del diagnóstico.	a las que se aplica el algoritmo.		calidad del tratamiento oncológico recibido.	algoritmo con datos que eviten la discriminación.	
Derecho a la salud física y mental	El funcionamiento incorrecto del algoritmo puede dar lugar a un tratamiento sanitario ineficaz y perjudicial para el paciente, con el consiguiente perjuicio para el derecho a la salud.	[Media] Cuando se utiliza en pacientes europeos. [Alta] Cuando se utiliza en pacientes no europeos.	[Muy alta] El impacto afecta potencialmente a todas las personas a las que se aplica el algoritmo.	**[Alta]** **Cuando se utiliza en pacientes europeos.** **[Muy alta]** **Cuando se utiliza en pacientes no europeos.**	[Muy alta] El funcionamiento incorrecto del algoritmo puede dar lugar a un tratamiento sanitario ineficaz y perjudicial para el paciente.	[Medio] Patologías en las que un seguimiento posterior puede corregir el error del sistema. [Alto] Patología en la que el control posterior no puede corregir el error del sistema.	**[Alta]** **Cuando el control posterior del cáncer puede corregir el error del sistema** **[Muy alta]** **Cuando el control posterior del cáncer no puede corregir el error del sistema.**

Tabla 2A. Gestión de riesgos (I)

Derecho/libertad afectados	Probabilidad	Gravedad	Impacto global	Medidas para prevenir/mitigar los impactos
Protección de datos/Privacidad	[Media]	[Media]	**[Medio]**	• Publicar información sobre los procedimientos utilizados para obtener y procesar los datos originales utilizados para entrenar el sistema de IA.
No discriminación	[Muy alta]	[Muy alta]	**[Muy alto]**	• Ampliar el conjunto de datos de entrenamiento, evitando una baja representación de los grupos relevantes.
Derecho a la salud física y mental	[Alta] Cuando se utiliza en pacientes europeos. [Muy alta] Cuando se utiliza en pacientes no europeos.	[Alta] Cuando el control posterior del cáncer puede corregir el error del sistema [Muy alta] Cuando el control posterior del cáncer no puede corregir el error del sistema.	**[Alto]** Sólo cuando se utiliza en pacientes europeos y cuando la patología es tal que el seguimiento posterior puede corregir el error del sistema. **[Muy alto]** Para los otros tres escenarios.	• Informar a los profesionales sanitarios de las limitaciones de la herramienta. Por ejemplo, indicando el tipo de errores. • Diferenciar entre patologías con o sin evolución rápida. • Informar a los profesionales sanitarios de que debe tenerse en cuenta la tasa de error. del equipo de diagnóstico por imagen utilizado.

Tabla 3A. Gestión de riesgos (II)

Derecho/libertad afectados	Probabilidad (residual)	Gravedad (residual)	Impacto residual
Protección de datos/Privacidad	[Media]	[Baja] Ya que el esfuerzo se ha reducido a bajo.	**[Medio]**
No discriminación	[Media] Ya que la probabilidad se ha reducido a baja.	[Media] Ya que el esfuerzo se ha reducido a bajo.	**[Medio]**
Derecho a la salud física y mental	[Media] Cuando se utiliza en pacientes europeos, ya que la probabilidad se ha reducido a baja. [Alta] Cuando se utiliza en pacientes no europeos, ya que la probabilidad se ha reducido a media.	[Media] Si se trata de una patología en la que un seguimiento posterior puede corregir el error del sistema, ya que el esfuerzo se ha reducido a bajo. [Alta] Si se trata de una patología en la que el seguimiento posterior no puede corregir el error del sistema, ya que el esfuerzo se ha reducido a medio.	**[Medio]** Sólo cuando se utilice en pacientes europeos y cuando la patología sea tal que el seguimiento posterior pueda corregir el error del sistema. **[Alto]** Para los tres escenarios restantes.

Alessandro Mantelero
alessandro.mantelero@polito.it

https://www.dpdenxarxa.cat/pluginfile.php/2468/mod_folder/content/0/FRIA_es_2.pdf