SocInfo Digital

IA en Acción dentro de un Ámbito Ético y Responsable

29 de octubre de 2025

David de Francisco Marcos
Subdirector General de Fomento y Regulación de la Inteligencia Artificial (SEDIA)

GOBIERNO DE ESPAÑA

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

GovTechLab: Casos de Uso en la Administración del Estado

Laboratorio de experimentación con IA Generativa en la AGE

Más de 300 propuestas, 23 casos de uso transversales a toda la AGE en desarrollo

Ministerio de Derechos Sociales, Consumo y Agenda 2030	• Chatbot inteligente para la verificación documental en solicitudes de juegos y rifas ocasionales
Ministerio de Inclusión, Seguridad Social y Migraciones	• Marco de referencia para la creación de chatbots de ayuda para consultas ciudadanas
Ministerio de Industria y Turismo	• Agente inteligente para la valoración y comparación de legislación con otros países
Ministerio de Política Territorial y Memoria Democrática	• Sistema centralizador y de búsqueda en bases de conocimiento jurídico
Ministerio de Transformación Digital y para la Función Pública	• Sistema de asistencia para el proceso de gestión y evaluación de convocatorias de ayudas • Agente Soberano de IA para el uso interno de la Administración
Ministerio de Trabajo y Economía Social	• Chatbot de atención al ciudadano para el portal web del INSST • Asistente de generación y distribución de informes para las inspecciones provinciales de trabajo
Agencia Estatal de Meteorología	• Automatización de la redacción de reportes meteorológicos
Ministerio de Ciencia, Innovación y Universidades	• Asistente para la aceleración de la homologación de títulos universitarios extranjeros
Ministerio de Economía, Comercio y Empresa	• Sistema de consulta de conocimiento jurídico para servicios de inspección aduanera
Presidencia del Gobierno	• Asistente de búsqueda y síntesis de evidencia científica

El Origen de la Regulación de IA

Caso Compass

Sistema de IA usado en el sistema judicial de USA, que calculaba el riesgo de reincidencia delictiva. En 2016 un estudio demostró **sesgo racista**, otorgaba mucho más riesgo de delinquir a ciudadanos de raza negra ante expedientes muy similares

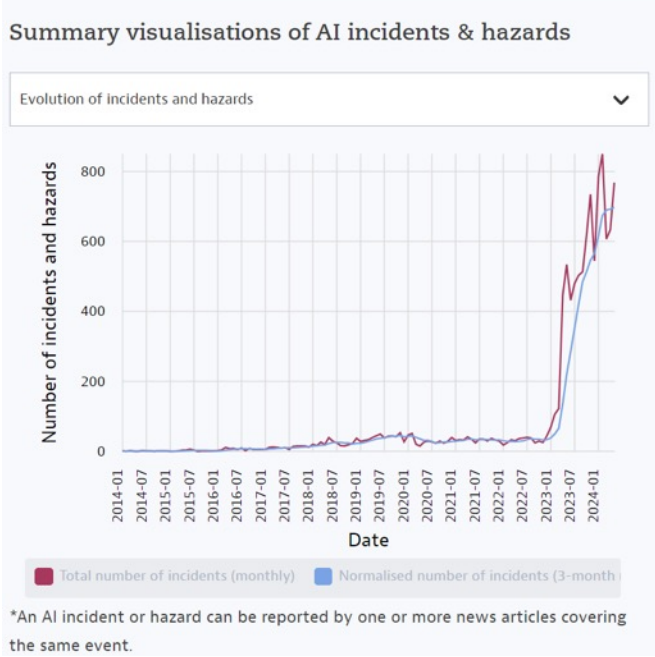
Dutch scandal serves as a warning for Europe over risks of using algorithms

The Dutch tax authority ruined thousands of lives after using an algorithm to spot suspected benefits fraud – and critics say there is little stopping it from happening again.

Authorities penalized families over a mere suspicion of fraud based on the system's risk indicators. Tens of thousands of families — often with lower incomes or belonging to ethnic minorities — were pushed into poverty because of exorbitant debts to the tax agency. Some victims committed suicide. More than a thousand children were taken into foster care.

Incidentes (OCDE)

Ya se predecía por parte de la OCDE un **número creciente de incidentes graves** por uso irresponsable de la IA en 2022



Base Jurídica del Reglamento (UE) 2024/1689 (Reglamento IA)

1) Protección uniforme del interés público y de los derechos de las personas en todo el mercado interior **(art 114 TFUE)**

2) Protección de las personas físicas en tratamiento de datos personales relativos: restricciones de uso de IA para la identificación biométrica remota **(art 16 TFUE)**

Reglamento (UE) 2019/1020
Vigilancia del mercado y la conformidad de los productos

Reglamento (UE) 2016/679
Protección de datos personales

Reglamento (UE) 2024/1689
Reglamento de IA

Legislación horizontal sobre seguridad de los productos

- **Coherencia** con el acervo de la UE en materia de seguridad de los productos

Neutralidad tecnológica

- No hay regulación de la tecnología, sino de los **casos de uso**
- Se cubren los riesgos para **la salud, la seguridad y los derechos fundamentales**

Alcance

- **Introducción** en el mercado, **puesta en servicio o utilización** de sistemas de IA
- Introducción en el mercado de **modelos de IA** de uso general

Fuera del Alcance

- Investigación **científica y desarrollo**
- **Código abierto** (bajo condiciones específicas)
- IA para uso **militar, defensa** y **seguridad nacional**

Clasificación de Sistemas según su Riesgo

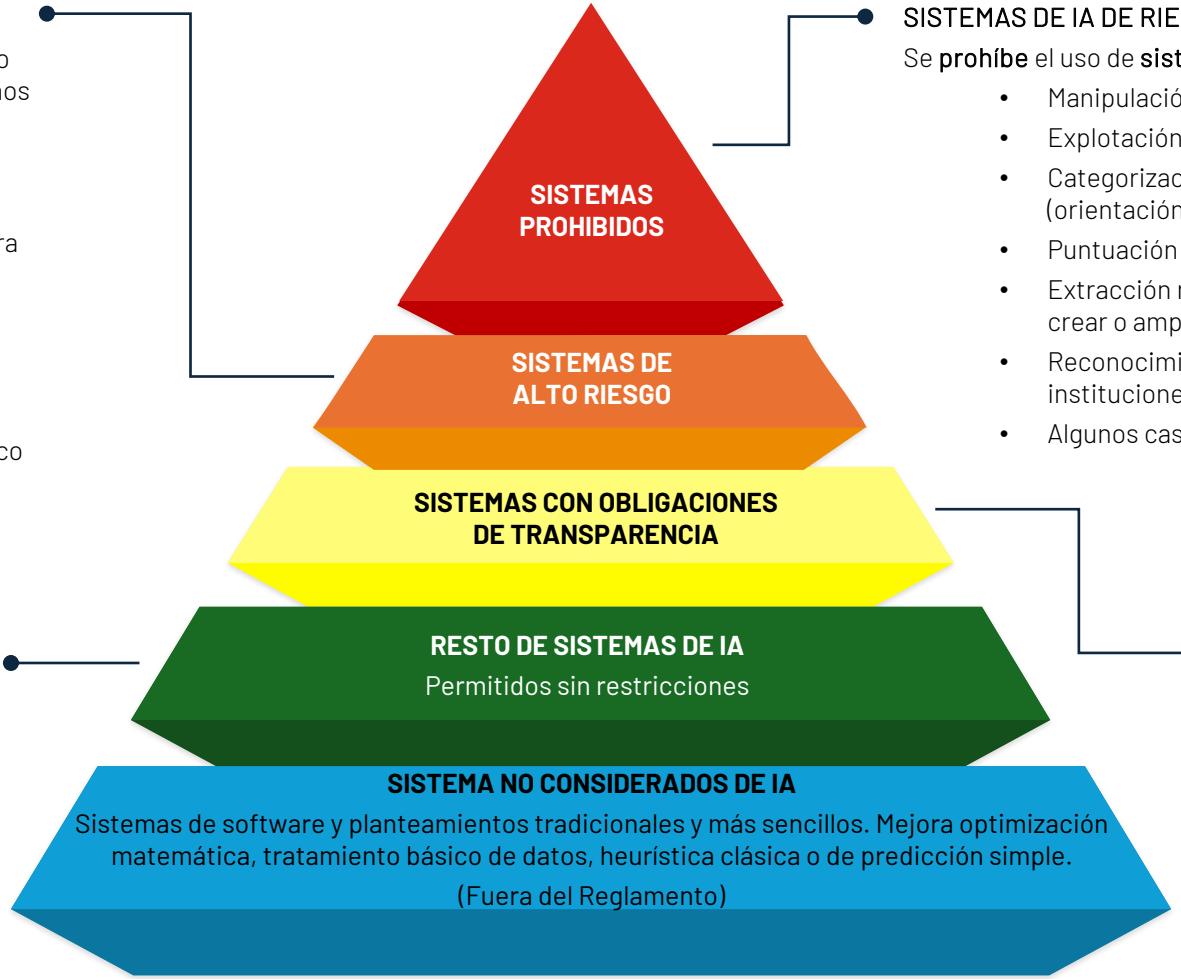
SISTEMAS DE IA DE ALTO RIESGO (HRAIS, ART.6)

Los sistemas de IA que pueden conducir a un riesgo significativo para la salud, la seguridad o los derechos fundamentales, por ejemplo:

- Contratación, promoción, evaluación
- Acceso a créditos y seguros de vida y salud
- Identificación biométrica (a excepción de la mera identificación del usuario final y las prácticas prohibidas)
- Infraestructuras críticas según Directiva UE 2022/2557
- Otros productos ya regulados por normas armonizadas UE (productos médicos, diagnóstico in vitro, ascensores, vehículo autónomo, etc.)

RESTO DE SISTEMAS DE IA

Obligación de alfabetización en materia de IA (Art 4)
(Común a todos los sistemas de IA)



SISTEMAS DE IA DE RIESGO INACEPTABLE (ART. 5)

Se **prohíbe** el uso de **sistemas de IA como**:

- Manipulación cognitivo-conductual
- Explotación de vulnerabilidades de personas
- Categorización biométrica para inferir datos sensibles (orientación sexual, creencias, etc.)
- Puntuación y/o clasificación social
- Extracción no selectiva de imágenes faciales de Internet para crear o ampliar bases de datos de reconocimiento facial
- Reconocimiento de emociones en el lugar de trabajo y en las instituciones educativas
- Algunos casos de vigilancia policial predictiva para las personas

SISTEMAS DE IA CON OBLIGACIONES DE TRANSPARENCIA ESPECÍFICAS (ART.50)

Permitidos pero sujetos a una serie de obligaciones de transparencia, sistemas relacionados con:

- La interacción con humanos
- La generación de contenidos manipulados
- Control mitigante: Revelar que el contenido ha sido generado por IA

Ejemplos Relevantes de Uso de IA en las AAPP

Prácticas de IA Prohibidas

Prohibiciones relevantes para el sector público:

- Puntuación social
- Vigilancia predictiva individual
- Raspado no dirigido de imágenes faciales de internet para construir bases de datos biométricas
- Identificación biométrica remota en tiempo real
- Categorización biométrica para inferir rasgos de carácter sensibles

Sistemas de Alto Riesgo

Casos de uso de alto riesgo relevantes para el sector público:

- Herramientas de IA que utilizan datos biométricos
- Sistemas de IA que son componentes de seguridad en infraestructuras críticas, por ejemplo, gas, calefacción, electricidad, agua
- Cálculo basado en IA de beneficios y servicios públicos
- Evaluaciones de riesgo basadas en IA, polígrafo, evaluación de la fiabilidad de pruebas en la aplicación de la ley y migración
- Herramientas de IA para preparar fallos judiciales

Requisitos de los sistemas de IA de Alto Riesgo

El Reglamento establece una serie de requisitos a cumplir para la introducción en el mercado de HRAIS

Los requisitos para los sistemas de IA de alto riesgo los podemos clasificar en tres bloques: **gestión, interacción con los responsables del despliegue y técnicos.**

Evaluación de impacto sobre los derechos fundamentales (FRIA) antes de la introducción en el mercado de un HRAIS

Sistema de gestión de riesgos

- Foco en la gestión de los **riesgos que puedan afectar a la salud, seguridad o derechos fundamentales de las personas**
- **Proceso continuo** e iterativo

Datos y gobernanza de datos

- Conjuntos de datos **con buena calidad y gobierno del dato**
- Los **datos** deben ser **relevantes**, representativos, libres de error y completos
- Se deben **aplicar técnicas de Gobierno del Dato** apropiadas

Registros

- Se **guardan suficientes logs**
- Debe ser mantenida **documentación técnica suficiente** para poder verificar la conformidad con la Regulación
- **Explicabilidad**

Transparencia y comunicación a los responsables del despliegue

- Los responsables del despliegue deben poder **entender y controlar** el HRAIS
- Incluye **información concisa, clara, no técnica, accesible y entendible** por el responsable del despliegue
- Lista de lo **que debe incluir la documentación**

Vigilancia humana

- Límite en la delegación
- **Se pueda decidir no usar el HRAIS o sus outputs**
- **Posibilidad** de que el **humano** pueda i) de manera segura e instantánea **interrumpir** la operación y ii) descartar, corregir o revertir el output

Documentación técnica

- **Documentación de todos los requisitos**
- **Actualización** continua
- **Antes de la comercialización**

Precisión, solidez y ciberseguridad

- **Precisión**: el resultado es preciso y se conoce por la documentación el nivel de precisión que tiene
- **Solidez:** resiliencia a fallos, errores o inconsistencias.
- **Ciberseguridad**: resiliencia a ataques

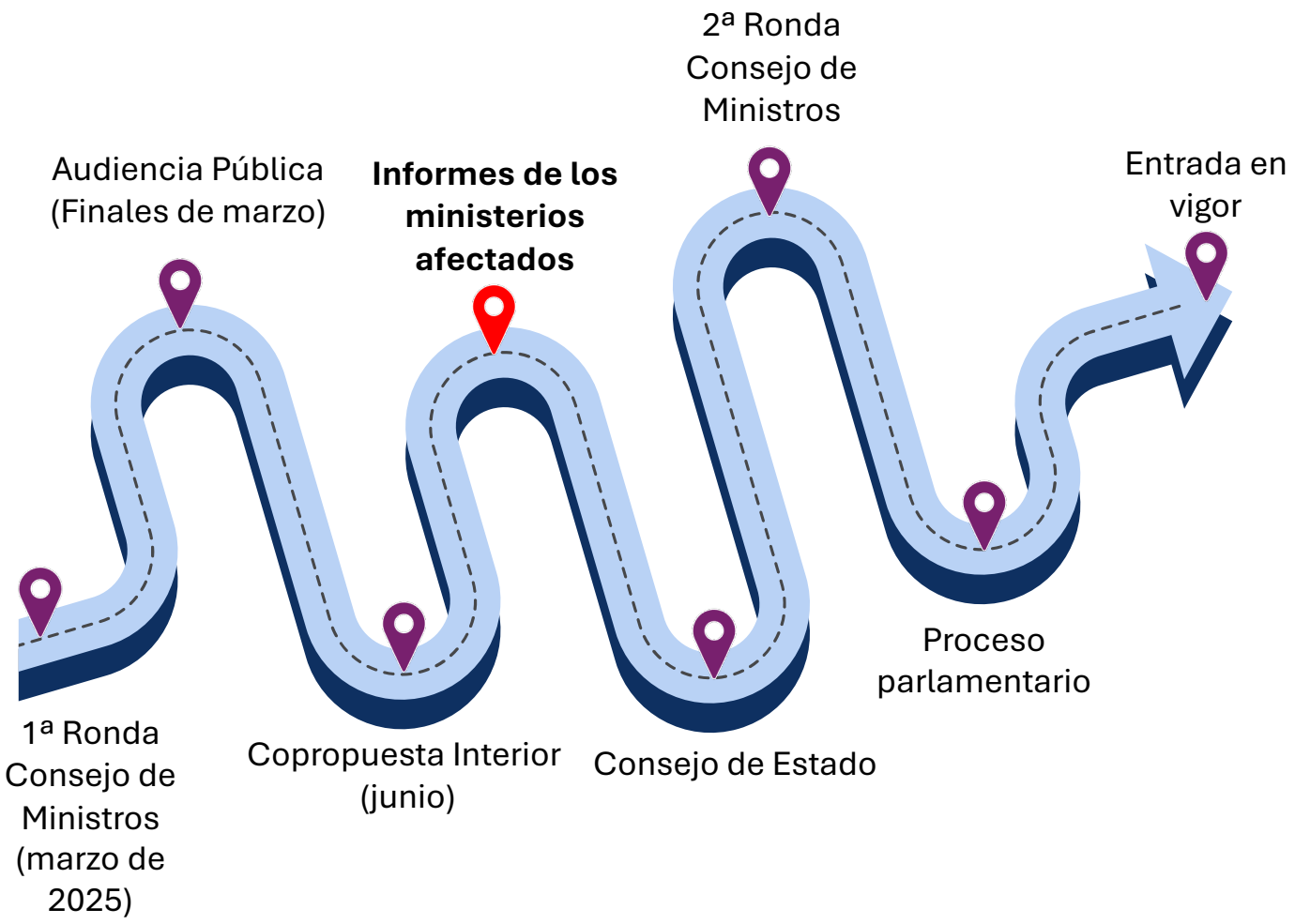
Leyenda

- Gestión
- Buen uso por parte del responsable del despliegue y el usuario final
- Técnicos

Obligaciones específicas para proveedores de GPAIS y GPAIS con riesgo sistémico

Anteproyecto de Ley de Gobernanza y Buen Uso de la IA

España es el 2º Estado miembro en iniciar el trámite legislativo



Estructura

1. Designación de las autoridades nacionales competentes y gobernanza
2. Establecimiento del marco sancionador (gravedad de las infracciones y rangos)
3. Procedimiento de autorización de identificación biométrica en tiempo real y posterior
4. Establecimiento de sandboxes regulatorios
5. Medidas para promover la IA responsable en la Administración (formación, delegado de IA)

Gracias por la Atención

Dudas y Preguntas

GOBIERNO DE ESPAÑA

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA