IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LA VIOLENCIA DE GENERO

Eva Mª Vázquez Castelo.
Consejera Técnica
Division Jurídica de la Agencia Española de Supervisión de Inteligencia Artificial (AESIA)

IA: desafío global

Abordaje internacionl

Union Europea: RIA (Reglamento 2024/1689)

España: **Enfoque español de IA centrada en el ser humano**

ENIA.2020. Objetivo Estratégico 6, la necesidad de definir un marco ético.

AESIA 2023

ENIA 2024 infraestructura y talento, sector público, AESIA: IA transparente, responsable y humanística

.

Características principaales del Reglamento

1

Norma integral y única para la UE

Armoniza los requisitos para la introducción n el mercado y el uso de sistemas de IA en toda la Unión Europea.

2

Norma de seguridad de producto

Considera los sistemas de IA de alto riesgo como productos que requieren el cumplimie-nto de estándares armonizados.

3

Regulación basada en el uso y en el riesgo

Categoriza los riesgos en niveles y prevé una intensidad regulatoria proporcional para cadu no.

4

Protección DDFF y Enfoque preventivo

Apoyo a la innovación

5

Apoyo a la innovación

6

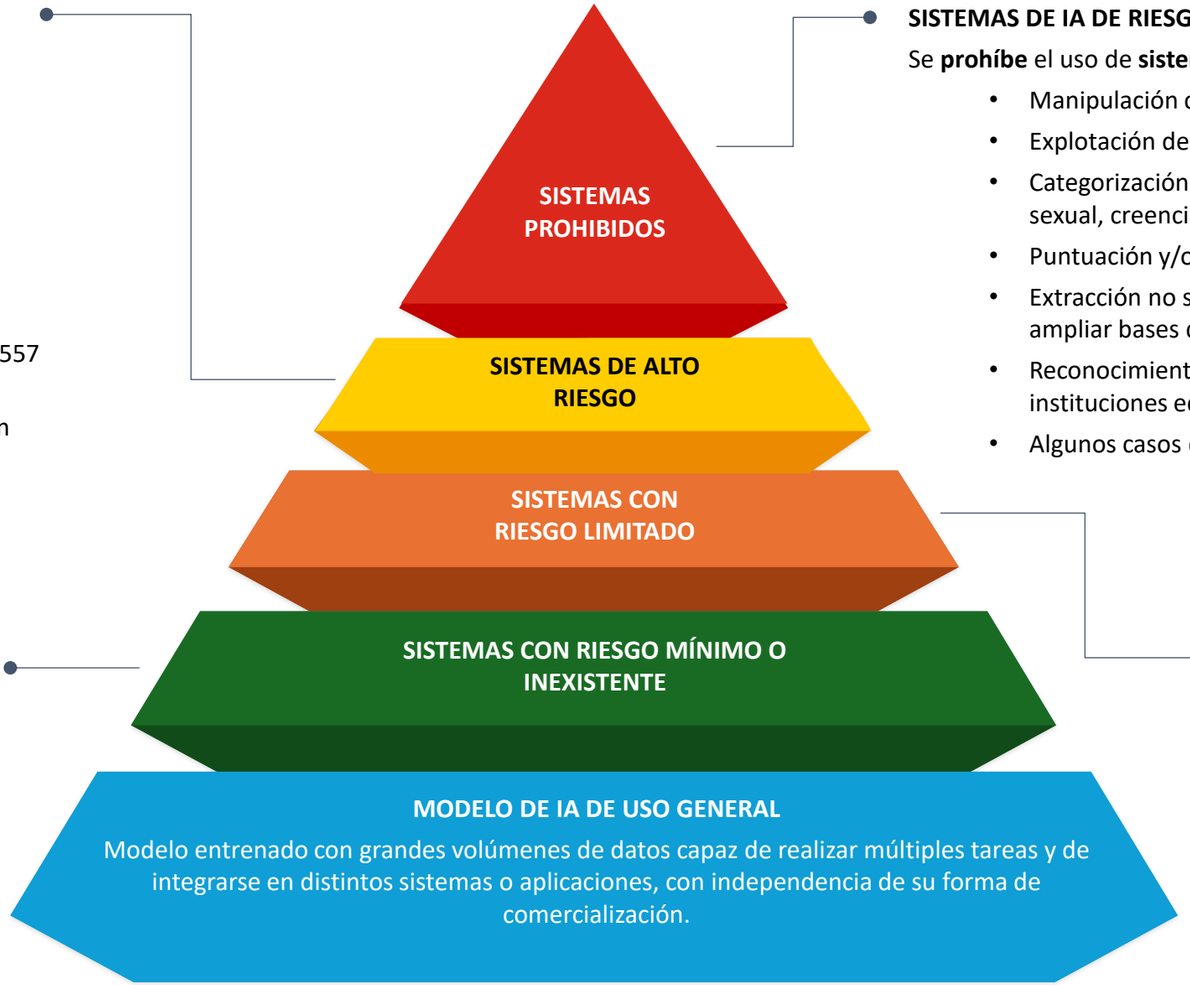
Gobernanza

La clasificación de riesgos en el Reglamento de IA

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.)



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 DE RIESGO MÍNIMO O INEXISTENTE

Permitidos sin restricciones (ejemplo: mantenimiento predictivo)

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

Requisitos de sistemas de alto riesgo

Datos y gobernanza de datos

- Datos de alto valor y gobernanza de datos:
  - Captura de datos
  - Procesado de datos: etiquetado, depuración, cifrado, agregación
  - Asunciones sobre datos
  - Evaluación previa de disponibilidad y cantidad
  - Examinar sesgo
- Datos deben ser relevantes, representativos, libres de error y completos
- Se deben aplicar técnicas de Gobierno del Dato apropiadas

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

Deben ser registrados en la BD de la UE para sistemas de alto riesgo

Transparencia y comunicación a los usuarios

- Usuarios deben poder entender y controlar el HRAIS
- Incluye información concisa, clara, no técnica, accesible y entendible por usuario
- Lista de lo que debe incluir la documentación

Registros

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

Supervisión 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

Sistema de Gestión de calidad

Autoridad de Vigilancia de Mercado (AVM)

Entidad encargada de supervisar y garantizar que los productos y sistemas de inteligencia artificial que se comercializan cumplen con los requisitos y regulaciones establecidas por el reglamento de IA. Para lograr su objetivo, la legislación europea ha diseñado diversos mecanismos y actividades para las AVM, conocidos como actividades de vigilancia del mercado.

COMPETENCIAS

1. Imposición de **sanciones**
2. Actividades conjuntas de **inspección entre la Comisión y otras AVMs**
3. Mecanismos de **información** entre **otras AVMs**
4. **Notificación de incidentes graves**
5. **Retirada** de **productos** que presente un **riesgo grave**

REQUISITOS

- El Reglamento de IA establece que debe haber al menos una autoridad de vigilancia del mercado.
- Ejercerá sus competencias y poderes de manera independiente, imparcial y sin sesgos

Reglamentos de referencia

- *Reglamento (UE) 2019/1020 sobre VM (Norma general de VM):*
  - Juguetes, Ascensores, Productos sanitarios, Sistemas de IA, etc.
- *Reglamento Europeo de IA (Norma específica de IA):*
  - *Sistemas de IA*

Calendario de Aplicación de las Disposiciones

Las obligaciones y requisitos para los sistemas de IA de alto riesgo se aplican de forma escalonada, con plazos diferenciados según el anexo correspondiente y las medidas de simplificación del **Digital Omnibus**.

1

2 de agosto de 2026

Aplicación de obligaciones y requisitos para los sistemas de IA de alto riesgo del **Anexo III** (plazo original).

2

2 de agosto de 2027

Aplicación de obligaciones y requisitos para los sistemas de IA de alto riesgo del **Anexo I** (plazo original).

3

2 de diciembre de 2027

Nueva fecha para el **Anexo III** tras las medidas de simplificación y prórroga del Digital Omnibus.

4

2 de agosto de 2028

Nueva fecha para el **Anexo I** tras las medidas de simplificación y prórroga del Digital Omnibus.

El **Digital Omnibus** adopta medidas de simplificación y prorroga la aplicación de las obligaciones y requisitos para los sistemas de IA de alto riesgo, ampliando los plazos tanto para el Anexo III como para el Anexo I.

AESIA

CATALIZADOR DE UNA IA CENTRADA EN EL SER HUMANO

IA CONFIABLE Y COMPETITIVA

SUPERVISIÓN/ AUTORIDAD VIGILANCIA DE MERCADO

ALFABETIZACIÓN Y FORMACIÓN

ANTICIPACIÓN: PROSPECTIVA Y SENSIBILIZACIÓN.

PROMOCIÓN DE LA INNOVACIÓN.

DIMENSIÓN INSTITUCIONAL E INTERNACIONAL.

RETOS de la IA

Capacidad de potenciar amenazas existentes

- Violencia, abuso
- Sesgos
- Discriminación
- Desigualdad
- Brecha digital
- Falta de representación
- Desinformación
- Manipulación
- Fraude
- Concentración de poder (económico, social, ideológico o político)
- Incremento de la vulnerabilidad

Nuevos retos

- Fallo (error o ataque)
- Etica (autonomía, papel humano)

IA Y VIOLENCIA SOBRE LA MUJER

La violencia digital como extensión tecnológica de la violencia estructural

Escalada con IA:

- Rápidez
- Propagación y alcance
- Tecnología accesible
- Facilidad de acceso y uso
- Relativa sensación de anonimato e impunidad
- Deshumanización propia de la vida digital
- Pérdida de control de la información : incrementa riesgo, agrava impacto, perdurabilidad

Estudios:

- Macroencuesta
- Encuesta UE
- Estudios ONU

RESPUESTA

REGULACION

- Normas claras para plataformas y sistemas de IA
- Supervisión / sanción
- Tecnología: Transparencia algorítmica, datos, sesgos ,Identificación de contenidos generados por IA

SENSIBILIZACION

- Alfabetización digital
- Concienciación social

CAPACIDAD: investigar y medir, proteger, garantizar fiabilidad, despliegue responsable

COMPROMISO:

Social

Institucional: Coordinación entre autoridades

Sector privado: proveedores, responsables, plataformas

INICIATIVAS DE AESIA EN LA PROTECCIÓN DE DERECHOS FUNDAMENTALES /MUJER

PRINCIPIO INFORMADOR ACTIVIDAD:

LABORATORIO DE IDEAS

CONVENIO INSTITUTO DE LAS MUJERES

COORDINACION INTERNACIONAL