ISMS FORUM
HANDBOOK IA

Guía para comprender mejor
el nuevo Reglamento de Inteligencia
Artificial RIA

GIA | GRUPO DE INTELIGENCIA ARTIFICIAL

SECCIÓN #01

RESUMEN DE LAS VARIABLES DE APLICACIÓN DEL REGLAMENTO

VARIABLES DE APLICACIÓN DEL REGLAMENTO

TIPOLOGÍA DE IA

Sistemas de IA, sistemas de IA de propósito general o modelos de IA de propósito general.

ROLES EN IA

Proveedor, responsable del despliegue, importador, distribuidor, fabricante de productos o representante autorizado. Conjuntamente se denominan "operador".

NIVEL DE RIESGO

Riesgo inaceptable, alto riesgo, riesgo limitado o riesgo mínimo para los sistemas de IA.

Para los modelos se conciben dos niveles de riesgo: **ordinario** (cualquier modelo) o **sistémico**, en función de determinados requisitos.

SECCIÓN #02

EXPLICACIÓN DE CONCEPTOS

TIPOLOGÍAS DE SISTEMAS DE IA

.01
SISTEMAS DE IA

Sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.

.02
SISTEMAS DE IA DE PROPÓSITO GENERAL

Sistema de IA basado en un modelo de IA de uso general y que puede servir para diversos fines, tanto para su uso directo como para su integración en otros sistemas de IA.

.03
MODELOS DE IA DE PROPÓSITO GENERAL

Modelo de IA o modelo de IA entrenado con un gran volumen de datos utilizando autosupervisión a gran escala, que demuestra un alto grado de generalidad y es capaz de realizar de manera competente una amplia variedad de tareas. Estos modelos pueden integrarse en diversos sistemas o aplicaciones posteriores, independientemente de cómo se introduzcan en el mercado. Esta definición excluye los modelos de IA utilizados para actividades de investigación, desarrollo o creación de prototipos antes de su introducción en el mercado.

ROLES EN IA

PROVEEDOR

Persona física o jurídica, autoridad pública, órgano u organismo que **desarrolle un sistema de IA o un modelo de IA** de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y **lo introduzca en el mercado** o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente. Se aplica tanto para sistemas como modelos de IA.

RESPONSABLE DE DESPLIEGUE

Persona física o jurídica, o autoridad pública, órgano u organismo que **utilice un sistema de IA** bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional.

IMPORTADOR

Persona física o jurídica ubicada o establecida en la Unión Europea que **introduzca en el mercado un sistema de IA** que lleve el nombre o la marca de una persona física o jurídica establecida en un tercer país.

DISTRIBUIDOR

Persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que **comercialice un sistema de IA** en el mercado de la Unión Europea.

REPRESENTANTE AUTORIZADO

Persona física o jurídica ubicada o establecida en la Unión que haya **recibido y aceptado** el mandato por escrito de un proveedor de un sistema de IA o de un modelo de IA de uso general para cumplir las obligaciones y llevar a cabo los procedimientos establecidos en el presente Reglamento en representación de dicho proveedor.

FABRICANTE DEL PRODUCTO

Fabricante en el sentido que indica la legislación armonizada listada en el Anexo I del RIA.

Los seis roles pueden aplicarse completamente al contexto de los sistemas de IA. Sin embargo, en el contexto de los modelos, sólo se pueden aplicar los roles de proveedor o representante autorizado. Es decir, con respecto a un modelo de IA, no se puede ser responsable de despliegue, importador, distribuidor o fabricante del producto.

NIVEL DE RIESGO

Esta variable se divide en dos categorías principales:

- Riesgos en Sistemas de IA:
  - Riesgo Inaceptable
  - Alto Riesgo
  - Riesgo Limitado
  - Riesgo Mínimo
- Riesgos en Modelos de IA:
  - Riesgos Ordinarios
  - Riesgos de Carácter Sistémico

RIESGOS EN SISTEMAS DE IA

RIESGO INACEPTABLE

8 casos de uso prohibido:

- Categorización biométrica e individual para inferir características sensibles (raza, orientación religiosa/ideológica/sexual, etc.).
- Reconocimiento biométrico en remoto y en tiempo real en espacios públicamente accesibles con fines de prevención/investigación de delitos sin que se cumplan ciertos requisitos de excepción (tipos penales tasados + condiciones y requisitos a cumplir).
- Scraping generalizado de imágenes faciales de internet o CCTV para generar o ampliar bases de datos de reconocimiento facial.
- Reconocimiento de emociones en entornos laborales y educativos, salvo con fines médicos o de seguridad.
- Sistemas de scoring social basado en comportamiento o características personales.
- Sistemas de manipulación subliminal para influir en toma de decisiones perjudiciales.
- Sistemas que exploten vulnerabilidades de las personas (edad, solvencia, discapacidad, etc.) para influir en su comportamiento y tomar decisiones perjudiciales.
- Sistemas que evalúen y predigan el riesgo de comisión de delitos basándose únicamente en la elaboración del perfil de una persona física.

RIESGOS EN SISTEMAS DE IA

ALTO RIESGO

2 condiciones:

1) Estar destinado a utilizarse como componente de seguridad un producto o que el propio sistema de IA sea dicho producto, que entre en el ámbito de aplicación de la legislación armonizada del Anexo I del RIA.

2) Que dicho producto requiera, conforme a la legislación armonizada, someterse a una evaluación de la conformidad de terceros para su introducción en el mercado o puesta en servicio.

- Máquinas
- Seguridad de los juguetes
- Embarcaciones de recreo
- Ascensores y sus componentes de seguridad
- Sist. de protección para uso en atmósferas potencialmente explosivas
- Equipos radioeléctricos
- Equipos a presión
- Instalaciones de transporte por cable
- Aparatos que queman combustibles gaseosos
- Productos sanitarios
- Productos sanitarios para diagnóstico in vitro
- Seguridad de la aviación civil
- Homologación de vehículos de 2 o 3 ruedas y cuatriciclos
- Homologación de vehículos agrícolas o forestales
- Equipos marinos
- Homologación de vehículos agrícolas o forestales
- Homologación y vigilancia del mercado de los vehículos de motor
- Normas comunes en el ámbito de la aviación civil
- Requisitos de homologación de tipo de los vehículos

Los sistemas que identifica el Anexo III del RIA

26 casos de uso comprendidos en 8 sectores:

BIOMETRÍA

Sistemas de identificación biométrica remota.

Sistemas de IA para la categorización biométrica en función de atributos o características sensibles o protegidos basada en la inferencia de dichos atributos o características.

Sistemas de IA para el reconocimiento de emociones (cuando no aplique la prohibición de entornos educativos y profesionales).

INFRAESTRUCTURAS CRÍTICAS

Sistemas de IA destinados a ser utilizados como componentes de seguridad en la gestión y el funcionamiento de las infraestructuras digitales críticas, del tráfico rodado o del suministro de agua, gas, calefacción o electricidad.

EDUCACIÓN Y FORMACIÓN PROFESIONAL

Sistemas de IA destinados a ser utilizados para determinar el acceso o la admisión de personas físicas a centros educativos y de formación profesional a todos los niveles o para distribuir a las personas físicas entre dichos centros.

Sistemas de IA destinados a ser utilizados para evaluar los resultados del aprendizaje.

Sistemas de IA destinados a ser utilizados para evaluar el nivel de educación adecuado que recibirá una persona o al que podrá acceder, en el contexto de los centros educativos y de formación profesional o dentro de estos a todos los niveles.

Sistemas de IA destinados a ser utilizados para el seguimiento y la detección de comportamientos prohibidos por parte de los estudiantes durante los exámenes en el contexto de los centros educativos y de formación profesional o dentro de estos a todos los niveles.

EMPLEO, GESTIÓN DE LOS TRABAJADORES Y ACCESO AL AUTOEMPLEO

Sistemas de IA destinados a ser utilizados para la contratación o la selección de personas físicas, en particular para publicar anuncios de empleo específicos, analizar y filtrar las solicitudes de empleo y evaluar a los candidatos.

Sistemas de IA destinados a ser utilizados para tomar decisiones que afecten a las condiciones de las relaciones de índole laboral o a la promoción o rescisión de relaciones contractuales de índole laboral, para la asignación de tareas a partir de comportamientos individuales o rasgos o características personales o para supervisar y evaluar el rendimiento y el comportamiento de las personas en el marco de dichas relaciones.

ACCESO A SERVICIOS PRIVADOS ESENCIALES Y A SERVICIOS Y PRESTACIONES PÚBLICOS ESENCIALES Y DISFRUTE DE ESTOS SERVICIOS Y PRESTACIONES

Sistemas de IA destinados a ser utilizados por las autoridades públicas o en su nombre para evaluar la admisibilidad de las personas físicas para beneficiarse de servicios y prestaciones esenciales de asistencia pública, incluidos los servicios de asistencia sanitaria, así como para conceder, reducir o retirar dichos servicios y prestaciones o reclamar su devolución.

Sistemas de IA destinados a ser utilizados para evaluar la solvencia de personas físicas o establecer su calificación crediticia, salvo los sistemas de IA utilizados al objeto de detectar fraudes financieros.

Sistemas de IA destinados a ser utilizados para la evaluación de riesgos y la fijación de precios en relación con las personas físicas en el caso de los seguros de vida y de salud.

Sistemas de IA destinados a ser utilizados para la evaluación y la clasificación de las llamadas de emergencia realizadas por personas físicas o para el envío o el establecimiento de prioridades en el envío de servicios de primera intervención en situaciones de emergencia, por ejemplo, policía, bomberos y servicios de asistencia médica, y en sistemas de triaje de pacientes en el contexto de la asistencia sanitaria de urgencia.

GARANTÍA DEL CUMPLIMIENTO DEL DERECHO

Evaluación del riesgo de que una persona física sea víctima de delitos.

Sistemas de IA destinados a ser utilizados como polígrafos o herramientas similares.

Evaluar la fiabilidad de las pruebas durante la investigación o el enjuiciamiento de delitos.

Evaluar el riesgo de que una persona física cometa un delito o reincida en la comisión de un delito atendiendo no solo a la elaboración de perfiles para evaluar rasgos y características de la personalidad o comportamientos delictivos pasados de personas físicas o colectivos.

Las anteriores conductas identifican, como sujeto que las realiza, en función del caso tanto a (i) las autoridades garantes del cumplimiento del Derecho, o en su nombre, como (ii) las instituciones, órganos y organismos de la UE en apoyo de las autoridades garantes del cumplimiento del Derecho, o en su nombre.

MIGRACIÓN, ASILO Y GESTIÓN DEL CONTROL FRONTERIZO

Sistemas de IA destinados a ser utilizados como polígrafos o herramientas similares.

Evaluación de un riesgo, por ejemplo, un riesgo para la seguridad, la salud o de migración irregular, que plantee una persona física que tenga la intención de entrar en el territorio de un Estado miembro o haya entrado en él.

Sistemas de IA destinados a ser utilizados para ayudar a las autoridades públicas competentes a examinar las solicitudes de asilo, visado o permiso de residencia y las reclamaciones conexas con el fin de determinar si las personas físicas solicitantes reúnen los requisitos necesarios para que se conceda su solicitud, con inclusión de la evaluación conexa de la fiabilidad de las pruebas.

Sistemas de IA destinados a ser utilizados, en el contexto de la migración, el asilo o la gestión del control fronterizo, con el fin de detectar, reconocer o identificar a personas físicas, con excepción de la verificación de documentos de viaje.

ADMINISTRACIÓN DE JUSTICIA Y PROCESOS DEMOCRÁTICOS

Sistemas de IA destinados a ser utilizados por una autoridad judicial, o en su nombre, para ayudar a una autoridad judicial en la investigación e interpretación de hechos y de la ley, así como en la garantía del cumplimiento del Derecho a un conjunto concreto de hechos, o a ser utilizados de forma similar en una resolución alternativa de litigios.

Sistemas de IA destinados a ser utilizados para influir en el resultado de una elección o referéndum o en el comportamiento electoral de personas físicas que ejerzan su derecho de voto en elecciones o referendos (salvo que los resultados de salida no estén expuestos directamente a las personas).

RIESGOS EN MODELOS DE IA

ORDINARIOS

Todos los modelos no calificados como de riesgo sistémico.

DE RIESGO SISTÉMICO

Los calificados por la Comisión Europea como de riesgo sistémico en atención a criterios tasados.

Concretamente:

- El número de parámetros del modelo;
- La calidad o el tamaño del conjunto de datos, por ejemplo medidos a través de criptofichas;
- La cantidad de cálculo utilizada para entrenar el modelo, medida en operaciones de coma flotante o indicada con una combinación de otras variables, como el coste estimado del entrenamiento, el tiempo estimado necesario o el consumo de energía estimado para el mismo;
- Las modalidades de entrada y salida del modelo, como la conversión de texto a texto (grandes modelos de lenguaje), la conversión de texto a imagen, la multimodalidad y los umbrales punteros para determinar las capacidades de gran impacto de cada modalidad, y el tipo concreto de entradas y salidas (por ejemplo, secuencias biológicas);
- Los parámetros de referencia y las evaluaciones de las capacidades del modelo, también teniendo en cuenta el número de tareas sin entrenamiento adicional, la adaptabilidad para aprender tareas nuevas distintas, su nivel de autonomía y capacidad de ampliación y las herramientas a las que tiene acceso;
- Si sus repercusiones para el mercado interior son importantes debido a su alcance, lo que se dará por supuesto cuando se haya puesto a disposición de al menos 10 000 usuarios profesionales registrados establecidos en la UE;
- El número de usuarios finales registrados.

SECCIÓN #03

ÁMBITO DE APLICACIÓN DEL REGLAMENTO

PROPÓSITO DEL REGLAMENTO

El Reglamento de Inteligencia Artificial (RIA) está diseñado para **supervisar y regular la implementación de la Inteligencia Artificial, enfocándose particularmente en mitigar los riesgos asociados con su uso.**

EXCEPCIONES

AUTORIDADES PÚBLICAS Y ORGANIZACIONES INTERNACIONALES

No se aplica a las autoridades públicas de países terceros ni a organizaciones internacionales que utilicen sistemas de IA en el contexto de la cooperación policial o judicial con la UE o sus estados miembros.

SISTEMAS DE IA EXCLUIDOS

Los sistemas de IA utilizados exclusivamente para fines militares, de seguridad nacional o de investigación y desarrollo científico también están excluidos de este reglamento.

SECCIÓN #04

PRINCIPIOS DEL RIA

PROPÓSITO DEL REGLAMENTO

El RIA de la Unión Europea se fundamenta en un enfoque racional y principios claros diseñados para regular el desarrollo y uso de la inteligencia artificial dentro de la Unión Europea, enfocándose particularmente en salvaguardar los derechos fundamentales y la seguridad pública.

ENFOQUE BASADO EN EL RIESGO

El RIA establece un marco regulatorio que clasifica los sistemas de IA según el nivel de riesgo que representan. Esta clasificación es la piedra angular del reglamento, determinando el grado de regulación y supervisión necesarios.

ÉNFASIS EN LOS SISTEMAS DE ALTO RIESGO

Los sistemas de IA clasificados como de alto riesgo, tales como aquellos utilizados en contextos médicos, judiciales o relacionados con la seguridad, están sujetos a requisitos regulatorios más rigurosos. Estos incluyen auditorías y controles regulares, evaluaciones de impacto antes de su lanzamiento al mercado y mecanismos continuos de supervisión para asegurar que se cumplen los estándares éticos y técnicos establecidos.

EXCEPCIONES LIMITADAS

El RIA también contempla una serie de excepciones limitadas para ciertos usos de la IA, que incluyen aplicaciones militares, judiciales y científicas, así como para ciertos modelos de identificación biométrica remota. Estas excepciones reconocen la necesidad de adaptar la regulación a la naturaleza especializada de algunas aplicaciones de IA que son esenciales para la seguridad nacional o el avance científico.

OBLIGACIONES ESPECÍFICAS PARA MODELOS DE IA DE USO GENERAL

Los modelos de IA de Uso General (p.ej. GPT o Gemini) están sujetos a un conjunto específico de obligaciones regulatorias. Esto incluye la necesidad de garantizar la transparencia, la verificabilidad de los datos usados y la explicabilidad de sus operaciones y decisiones, lo cual es crucial para mitigar los riesgos de mal uso o resultados sesgados. Estas funciones varían según el modelo sea de riesgo ordinario o sistémico.

SECCIÓN #05

CRONOLOGÍA ENTRADA EN VIGOR EN 2026

El RIA entrará **en vigor veinte días después de su publicación en el Diario Oficial de la Unión Europea y será aplicable para la mayoría de los casos dos años después (2026)**, aunque nos encontramos algunas excepciones importantes:

1. Las prohibiciones surtirán efecto al cabo de **seis meses.**
2. Las normas de gobernanza y las obligaciones para los modelos de IA de uso general serán aplicables al cabo de **doce meses (1 año).**
3. Las normas para los sistemas de IA —integrados en productos regulados— se aplicarán al cabo de **treinta y seis meses (3 años).**

Para facilitar la adopción por parte de los actores interesados, desde la Comisión se ha puesto en marca el **Pacto Sobre la IA**, una iniciativa voluntaria que pretende dar apoyo a la futura aplicación e invita a los desarrolladores de IA de Europa y de fuera de ella a cumplir con antelación las obligaciones clave del RIA.

CRONOGRAMA DE IMPLEMENTACIÓN DEL REGLAMENTO

12 JULIO 2024	**PUBLICACIÓN EN EL DIARIO OFICIAL DE LA UE**
1 AGOSTO 2024	**ENTRADA EN VIGOR** (20 días tras la publicación)
2 FEBRERO 2025	**ENTRADA EN APLICACIÓN DE LAS PROHIBICIONES DE USO** (6 meses tras entrar en vigor)
2 MAYO 2025	**CONCLUYE EL PLAZO DE FINALIZACIÓN DE CÓDIGOS DE BUENAS PRÁCTICAS** (9 meses tras entrar en vigor)
2 AGOSTO 2025	**ENTRADA EN APLICACIÓN DE LAS DISPOSICIONES DIRIGIDAS A MODELOS DE IA** (12 meses tras entrar en vigor)
2 AGOSTO 2026	**ENTRADA EN APLICACIÓN DEL RESTO DE LA NORMA** (24 meses tras entrar en vigor)
2 AGOSTO 2027	**ENTRADA EN APLICACIÓN DEL ARTÍCULO 6.1 Y ANEXO I DEL RIA PARA CALIFICAR SISTEMAS DE IA COMO ALTO RIESGO** (36 meses tras entrar en vigor)

SECCIÓN #06

INCUMPLIMIENTO Y SANCIONES

Las medidas punitivas están diseñadas para garantizar el cumplimiento del RIA y fomentar un uso ético y responsable de la inteligencia artificial. Algunas de las sanciones que podrían aplicarse son las siguientes:

MULTAS ECONÓMICAS

Las multas por infracción del RIA se fijaron como un porcentaje del volumen de negocios anual global de la empresa infractora en el ejercicio financiero anterior o una cantidad predeterminada, la que fuera más alta. **Como máximo representaría el 7% del volumen de negocio global.**

Las medidas punitivas están diseñadas para garantizar el cumplimiento del RIA y fomentar un uso ético y responsable de la inteligencia artificial. Algunas de las sanciones que podrían aplicarse son las siguientes:

En Modelos de IA:

Hasta 15M de €, o 3% por el volumen de negocio para el incumplimiento de las obligaciones.

En Sistemas de IA:

Hasta 35M de €, o 7% del volumen anual de negocio para empresas por incumplir las prohibiciones del Reglamento.

Hasta 15M de €, o 3% del volumen anual de negocio por incumplir las obligaciones del Reglamento a proveedores, importadores, distribuidores, usuarios.

Hasta 7,5M de €, o 1% del volumen anual de negocio por suministrar información incorrecta a entidades notificadas o autoridades nacionales competentes.

CONSECUENCIAS ADICIONALES

Además de las sanciones económicas, las empresas pueden enfrentarse a una serie de consecuencias derivadas de las infracciones del RIA.

Prohibición de uso. En casos graves de incumplimiento, las autoridades competentes pueden imponer la prohibición del uso de ciertos sistemas de inteligencia artificial o de toda la actividad relacionada con la IA a la empresa infractora.

Retirada de certificaciones y licencias. Si una empresa ha obtenido certificaciones o licencias para el uso de sistemas de inteligencia artificial y se descubre que ha incumplido las regulaciones del RIA, estas certificaciones o licencias pueden ser revocadas.

Responsabilidad civil y penal. Además de las sanciones administrativas, las empresas y personas responsables del desarrollo o uso indebido de sistemas de IA pueden enfrentarse a acciones legales civiles y penales por daños causados a terceros o por violaciones de derechos fundamentales.

SECCIÓN #07

ENTIDADES DE SUPERVISIÓN

El Reglamento define varias entidades de supervisión:

AUTORIDAD NACIONAL

Existirá al menos una autoridad nacional notificante y al menos una una autoridad de supervisión de mercado como autoridades nacionales competentes para los propósitos del Reglamento.

En España, la **autoridad de supervisión es la AESIA**, Agencia Española de Supervisión de la Inteligencia Artificial. Cuyas principales funciones son:

NIVEL EUROPEO

Se constituirá un **Comité Europeo de Inteligencia Artificial,** donde participará un representante de cada Estado miembro. El Comité **orientará sobre la implementación del reglamento, elaborará guías y establecerá las reglas básicas para elaborar sandboxes.**

Además se ha creado la **Oficina Europea de IA**, que desempeña un papel crucial en la **supervisión del cumplimiento y la aplicación del RIA a lo largo de los Estados miembros de la Unión Europea.** Esta oficina actúa como la autoridad central en la gestión de la implementación del RIA, asegurando que las disposiciones del acta sean aplicadas de manera uniforme y efectiva en todos los sectores donde se utilicen sistemas de inteligencia artificial.

Para fortalecer la aplicación de la ley, la Oficina Europea de IA **trabaja en colaboración con las autoridades nacionales de supervisión de cada Estado miembro, coordinando actividades de control y formación para garantizar que se respeten los estándares establecidos.** Esta colaboración también se extiende a la esfera internacional, donde la Oficina participa en foros y acuerdos globales para promover una gobernanza de IA alineada a nivel mundial, buscando establecer prácticas comunes y compartir estrategias de regulación.

AUTORES

Participantes

Ángel Pérez

Gary Robertson

Julio San José

Gestión de proyectos

Beatriz García

Diseño y maquetación

Marta Barroso

Lydia García

CONTACTA CON NOSOTROS

www.ismsforum.es

proyectos@ismsforum.es

C/ Segre 29, 1ºB

Infografía IA

Grupo GIA ISMS Forum

Grupo de trabajo especializado en inteligencia artificial, que tiene como objetivo:

- **Generar y difundir conocimiento en materia de seguridad, gobernanza y cumplimiento;**
- **Facilitar la participación dinámica de los asociados y stakeholders;**
- **Ser un actor relevante e influyente en el sector para todos los asociados y la sociedad en general.**

GIA | GRUPO DE INTELIGENCIA ARTIFICIAL