Inteligencia Artificial Transparente

ApisDom

DESARROLLO DE APIS INTELIGENTES Y SOLUCIONES DE SOFTWARE A MEDIDA

Cumplimiento Normativo de la Inteligencia Artificial en España y la Unión Europea

Guía técnica sobre el Reglamento europeo, la intersección con el RGPD y el marco institucional de supervisión español.

ApisDom

El Marco Legal Multicapa

Reglamento Europeo de Inteligencia Artificial (RIA)

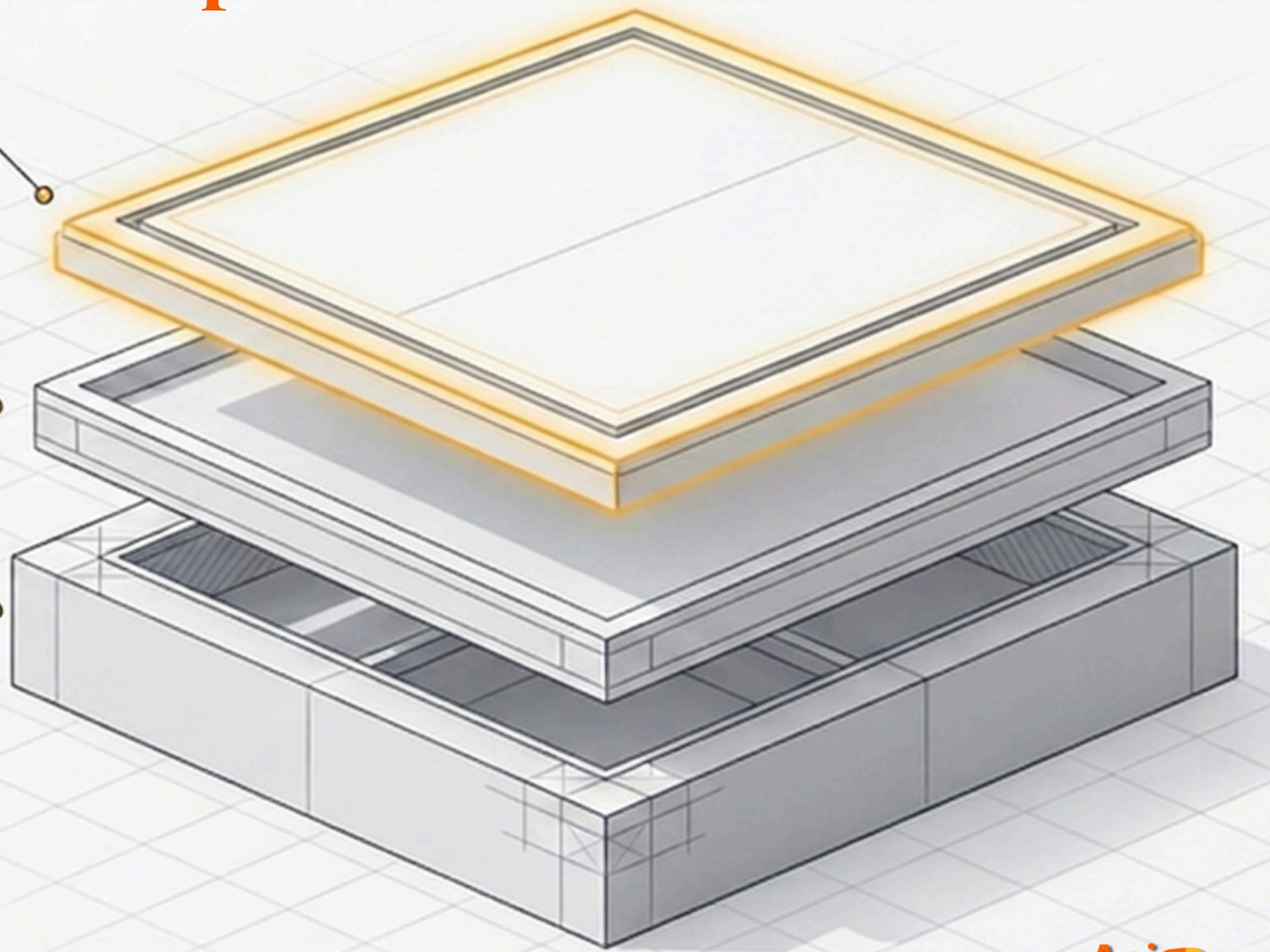
El Reglamento (UE) 2024/1689 establece el marco armonizado y vinculante de la inteligencia artificial en la Unión Europea. Su estructura se basa en la clasificación de los sistemas por niveles de riesgo e introduce obligaciones técnicas relacionadas con la gobernanza de datos, la transparencia, la supervisión humana y la gestión de riesgos.

Proyecto de Ley Orgánica para el buen uso y la gobernanza de la inteligencia

aEl proyecto español adapta el régimen sancionador y el modelo de supervisión institucional al ordenamiento interno. Prevé la atribución de funciones a las autoridades competentes y refuerza la transparencia en el uso de sistemas de inteligencia artificial por parte del sector público. El Consejo de Ministros aprobó el proyecto de Ley Orgánica para su remisión al Congreso de los Diputados el 26 de mayo de 2026.

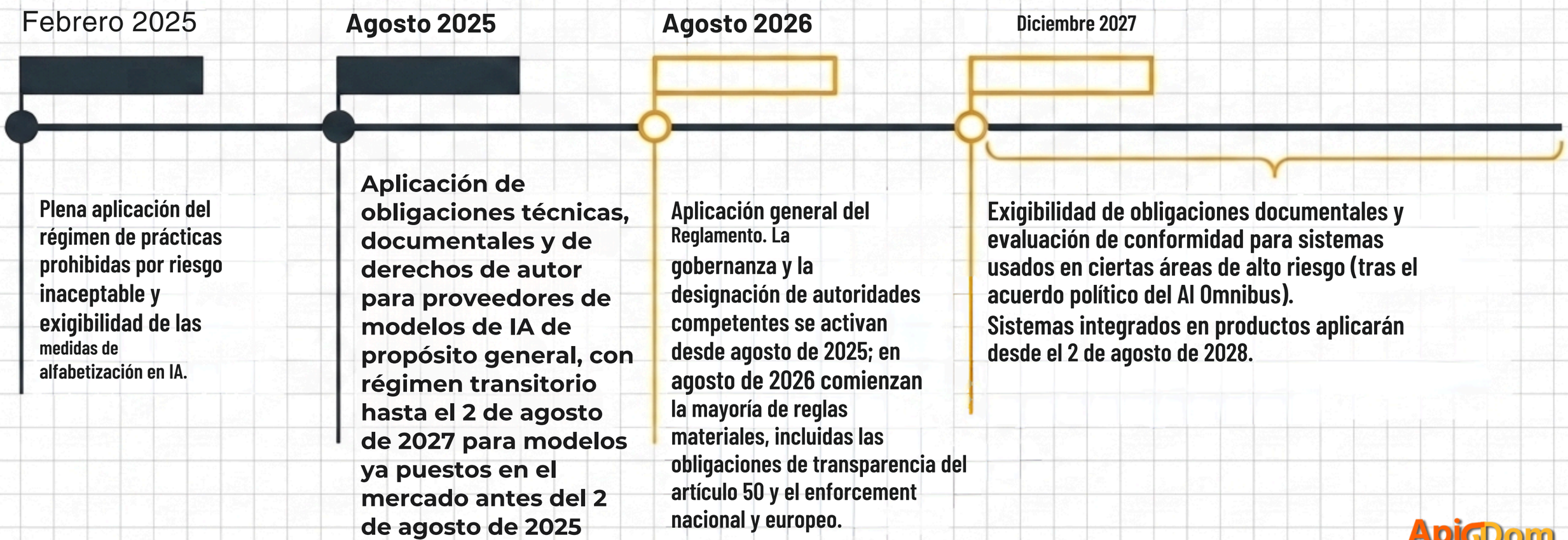
Intersección con la Privacidad (RGPD y LOPDGDD)

El desarrollo y despliegue de sistemas de inteligencia artificial debe coexistir con el Reglamento General de Protección de Datos y la LOPDGDD cuando exista tratamiento de datos personales. Esto exige una base jurídica válida, minimización de datos, limitación de la finalidad y evaluaciones de impacto cuando el tratamiento mediante IA pueda implicar alto riesgo para los derechos y libertades de las personas.



ApisDom

Calendario de Aplicación y Exigibilidad (2025-2028)



ApisDom

Gobernanza Institucional y Supervisión en España

Agencia Española de Supervisión de la Inteligencia Artificial (AESIA)

AESIA actúa como autoridad central y punto de contacto en el marco estatal de supervisión de IA, sin perjuicio de las competencias de la AEPD, el CGPJ, Banco de España y otras autoridades sectoriales.
El Ministerio dice que los productos ya regulados mantienen autoridades sectoriales y que el resto se atribuye principalmente a AESIA, AEPD y CGPJ según ámbito.

Agencia Española de Protección de Datos (AEPD)

Agencia Española de Protección de Datos (AEPD)
Mantiene sus competencias en materia de protección de datos cuando los sistemas de IA tratan datos personales, incluidos datos biométricos..
Supervisa las herramientas desplegadas en contextos de fronteras y migración.
Publica guías, criterios y orientaciones en materia de protección de datos sobre la legitimación del entrenamiento de algoritmos y los riesgos asociados a la inteligencia artificial agéntica.

Autoridades Sectoriales y Consejo General del Poder Judicial

El Consejo General del Poder Judicial supervisa el uso de algoritmos en la administración de justicia.
Las agencias sectoriales mantienen su jurisdicción para inspeccionar sistemas que operan como componentes de seguridad embebidos en productos ya regulados.

ApisDom

Clasificación de Sistemas y Niveles de Riesgo

Prácticas prohibidas. Incluye sistemas de calificación social, explotación de vulnerabilidades e identificación biométrica remota en tiempo real en espacios de acceso público con fines policiales, salvo excepciones estrictamente tasadas. Además, el AI Omnibus acordó incorporar la prohibición de sistemas que generen contenido íntimo o sexual no consentido.

**Sistemas permitidos bajo cumplimiento estricto. Incluye herramientas de selección de personal, evaluación crediticia e infraestructuras críticas. Requieren evaluación de conformidad, registro de actividad,
gestión de calidad y supervisión humana obligatoria.**

Sistemas sujetos a obligaciones de transparencia. Obligan a informar al usuario de que interactúa con una máquina, aplica a asistentes virtuales y sistemas de reconocimiento de emociones. Exige etiquetado legible por máquina de los contenidos generados.

Sistemas de riesgo mínimo o nulo. No tienen obligaciones específicas bajo el Reglamento de IA. Abarcan aplicaciones como filtros de correo no deseado o videojuegos y representan la mayoría de los sistemas de IA utilizados actualmente en la Unión Europea.

ApisDom

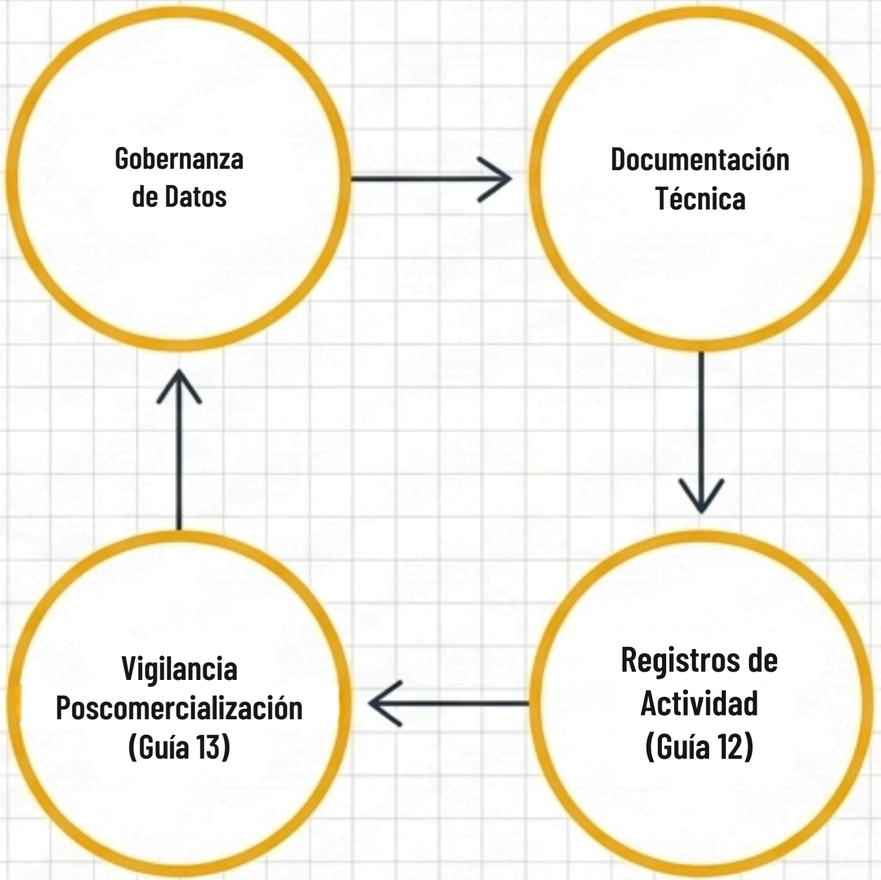
Obligaciones Operativas para Sistemas de Alto Riesgo

Gobernanza de Datos (Guía 7)

Los conjuntos de datos utilizados para el entrenamiento, validación y prueba deben ser pertinentes, suficientemente representativos y, en la mayor medida posible, estar libres de errores y completos. Se exige documentar las metodologías aplicadas para identificar, prevenir y mitigar posibles sesgos discriminatorios antes del despliegue.

Vigilancia Poscomercialización (Guía 13)

El proveedor está obligado a establecer un plan continuo para recopilar y analizar sistemáticamente los datos sobre el rendimiento del sistema en entornos reales, facilitando la detección temprana de incidencias.



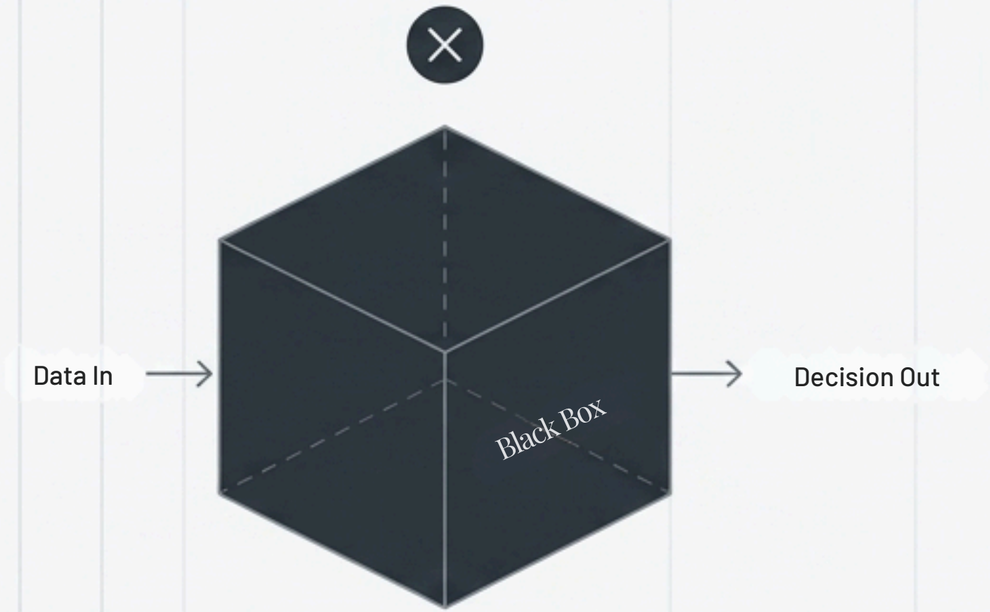
Documentación Técnica (Guía 15)

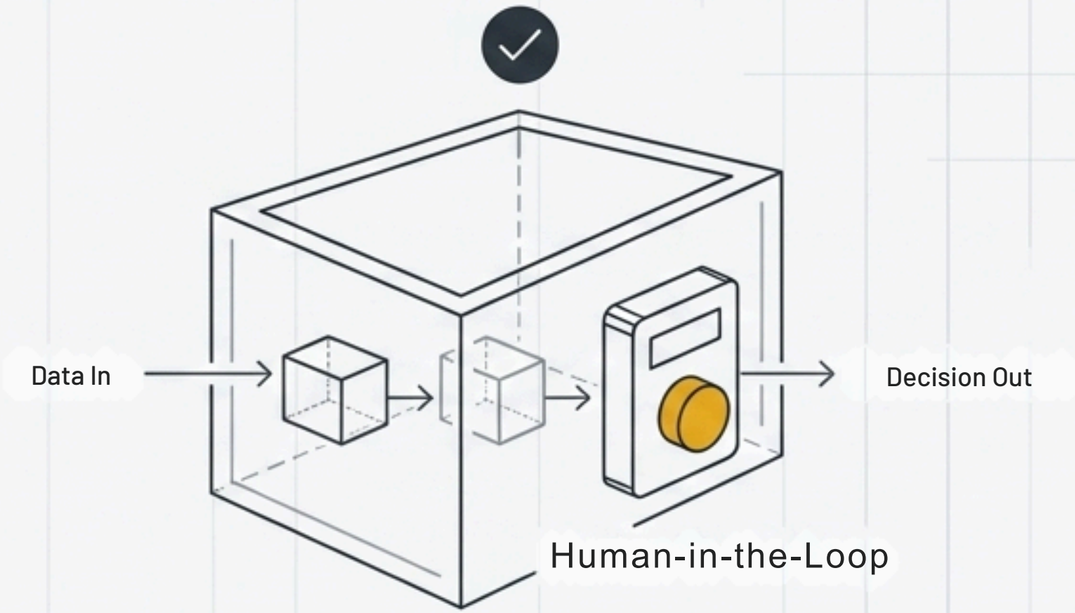
El proveedor debe elaborar documentación técnica antes de la comercialización o puesta en servicio del sistema, mantenerla actualizada y describir de forma clara la arquitectura, las limitaciones y el funcionamiento del sistema. Esta documentación debe permitir evaluar el cumplimiento del Reglamento y conservarse conforme a los plazos aplicables.

Registros de Actividad (Guía 12)

El sistema debe incorporar capacidades para generar registros automáticos de eventos durante su funcionamiento. En los sistemas de identificación biométrica remota de alto riesgo, estos registros deben incluir el periodo de uso, la base de datos de referencia y los datos de entrada que hayan producido una coincidencia.

Supervisión Humana, Transparencia y Explicación





Intervención y Control Efectivo

El artículo 14 del Reglamento y la Guía 6 de la AESIA establecen que los sistemas de alto riesgo deben diseñarse para ser supervisados por personas físicas. Esta supervisión exige interfaces adecuadas que permitan al operador comprender el funcionamiento, intervenir en el proceso y detener el sistema mediante mecanismos de interrupción seguros ante comportamientos imprevistos.

Evitar el Sesgo de Automatización

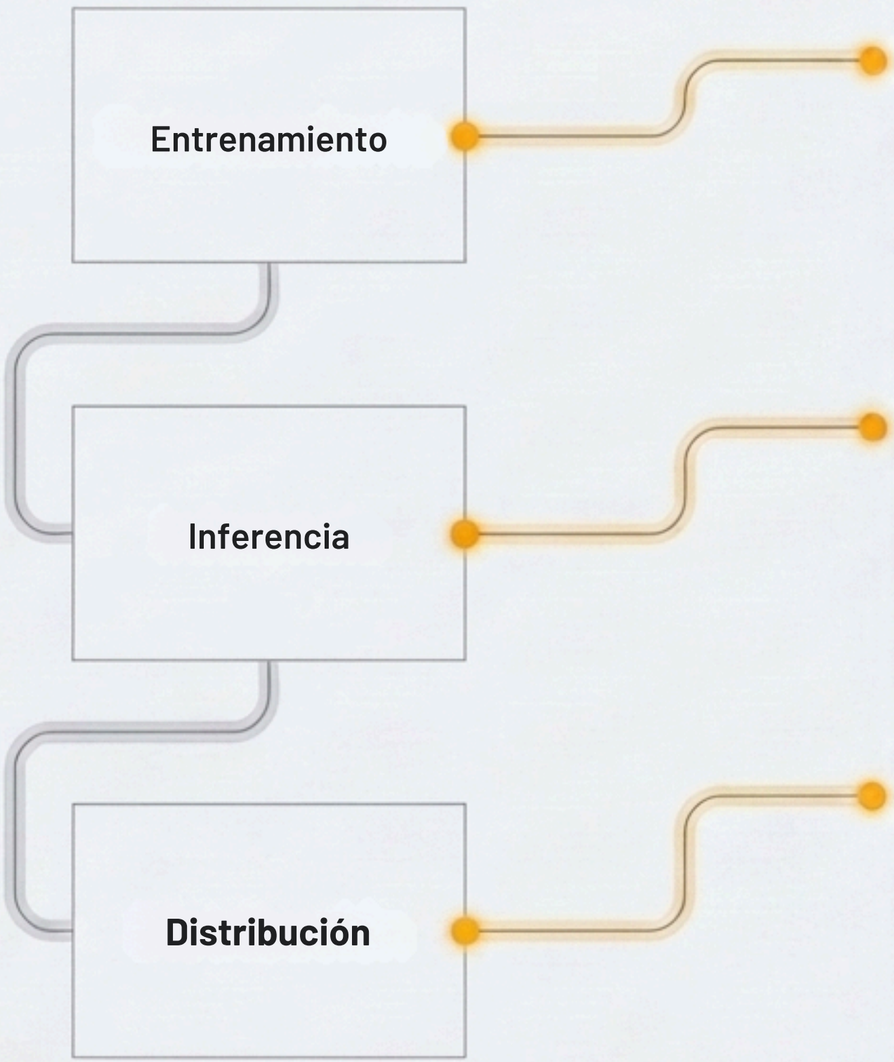
Las organizaciones deben proporcionar formación especifica a su personal sobre las limitaciones del sistema algoritmico. Resulta obligatorio adoptar medidas para gestionar el riesgo de que el elemento humano acepte sistemáticamente las decisiones automatizadas sin ejercer un escrutinio crítico e independiente.

Transparencia Hacia el Usuario

Más allá de la documentación interna, los sistemas de alto riesgo deben ser suficientemente transparentes para que el desplegador pueda interpretar sus resultados y utilizarlos adecuadamente. Cuando una decisión basada en un sistema de alto riesgo produzca efectos jurídicos o afecte significativamente a una persona, esta debe recibir una explicación clara y significativa sobre el papel del sistema en el proceso de decisión y sus principales elementos.

ApisDom

Intersección con la Privacidad y el RGPD



Evaluación de Impacto Relativa a la Protección de Datos

La realización de una EIPD es obligatoria únicamente cuando el tratamiento de datos personales mediante IA implique un alto riesgo para los derechos y libertades de los interesados, según los criterios de la AEPD.

No todo tratamiento de IA requiere EIPD; debe evaluarse el riesgo específico.

Minimización desde el Diseño

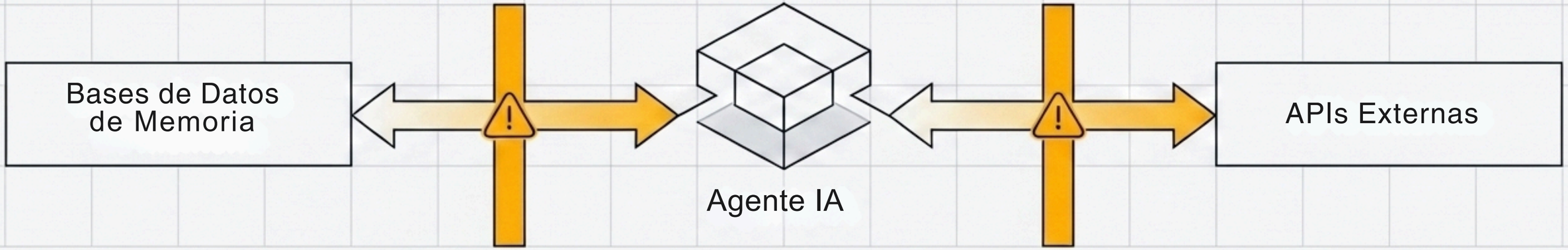
Las estrategias de minimización deben integrarse desde el diseño, aplicando medidas técnicas y organizativas proporcionadas al riesgo del tratamiento. Esto incluye la anonimización o seudonimización de datos cuando sea posible y limitar la recogida a lo estrictamente necesario para la finalidad concreta, evitando la acumulación innecesaria.

Legitimación y Derechos de los Interesados

Todo tratamiento de datos personales requiere una base jurídica válida. Si se utilizan datos de terceros, el responsable debe verificar su origen legítimo.

Los sistemas de IA deben diseñarse para permitir técnicamente el ejercicio de derechos (acceso, rectificación, supresión, oposición) sobre los datos personales, incluidos los inferidos, cuando proceda según la finalidad.

Riesgos de la Inteligencia Artificial Agéntica



El Desafío de la Autonomía

Las orientaciones de la AEPD sobre inteligencia artificial agéntica advierten que los sistemas con capacidad para planificar, dividir tareas y ejecutar acciones mediante herramientas externas alteran los riesgos tradicionales del tratamiento de datos.

Compartimentación de Memoria

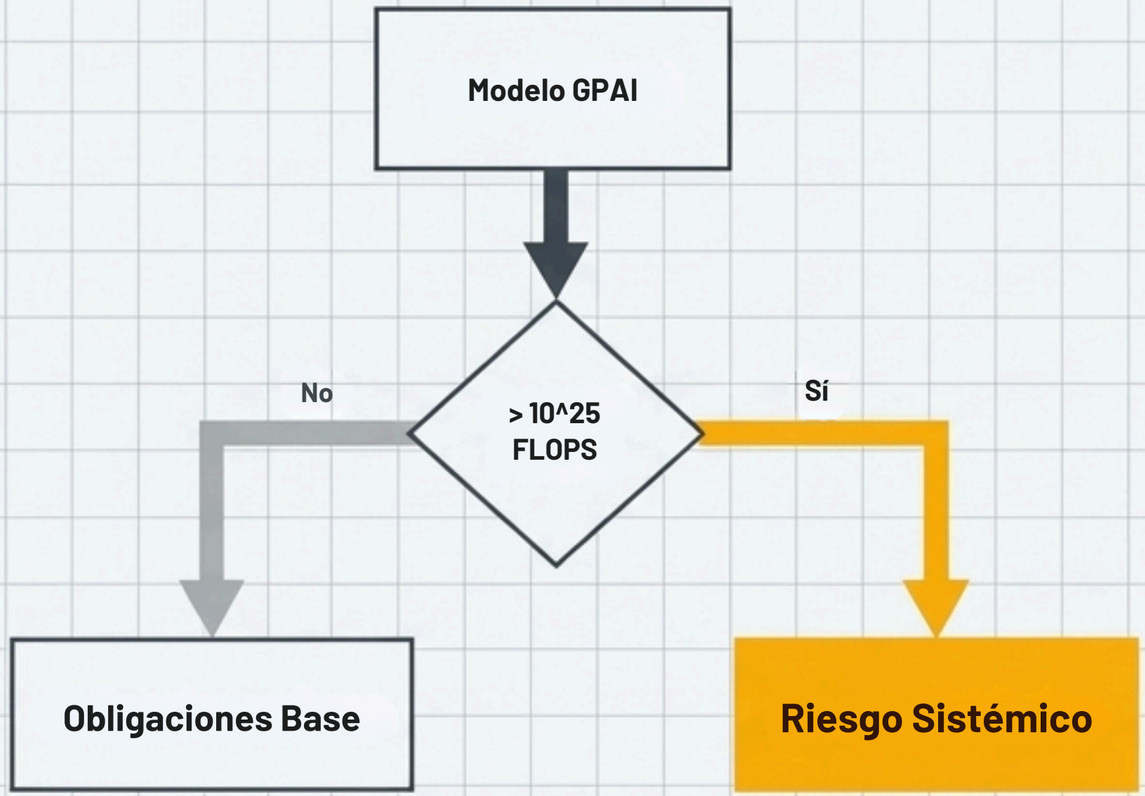
El responsable del tratamiento debe valorar e implantar medidas proporcionadas de retención, limpieza, aislamiento de contexto y control de herramientas cuando el análisis de riesgos lo exija. La AEPD habla de medidas que podría adoptar el responsable o encargado para cumplir y reducir impactos, no de una obligación única cerrada para todos los agentes.

Prevención de Exfiltración de Datos

El despliegue de arquitecturas multiagente requiere valorar controles de seguridad, auditorías, aislamiento de contexto y revisión de herramientas cuando el análisis de riesgos lo justifique. La AEPD identifica amenazas como la inyección de prompts, la exfiltración de datos, las instrucciones ocultas y el uso no autorizado de servicios externos, por lo que deben implantarse medidas proporcionadas para reducir esos riesgos.

ApisDom

Modelos de Uso General (GPAI) y Riesgo Sistémico



Regulación de la Capa Fundacional

El Reglamento distingue entre los sistemas de IA finales y los modelos de IA de uso general que pueden integrarse en ellos. Los proveedores de modelos de IA de uso general deben elaborar y mantener documentación técnica actualizada, poner a disposición información suficiente para los proveedores que integren el modelo en sistemas de IA y publicar un resumen suficientemente detallado del contenido utilizado para el entrenamiento.

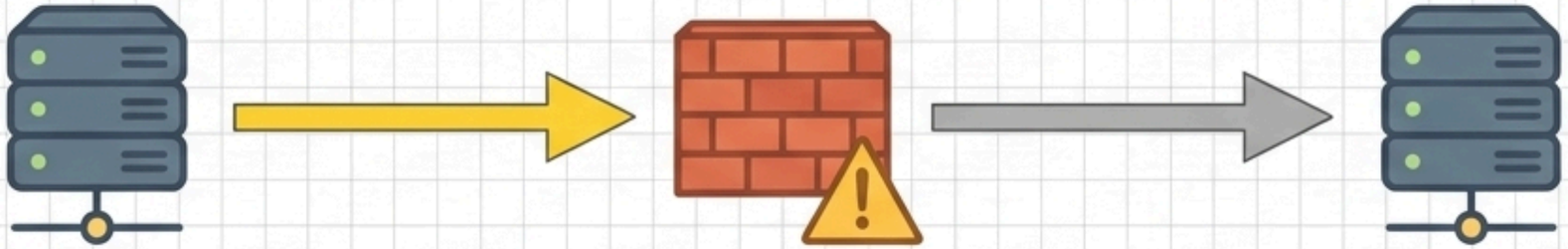
Umbrales de Riesgo Sistémico

Cuando un modelo excede una capacidad computacional de operaciones de coma flotante específica, se presume que posee un riesgo sistémico. Esta clasificación activa obligaciones de cumplimiento sustancialmente más severas para el proveedor.

Obligaciones Adicionales

Los proveedores de modelos de IA de uso general con riesgo sistémico deben evaluar el modelo conforme a protocolos y herramientas normalizados, incluyendo pruebas adversariales documentadas para identificar y mitigar riesgos sistémicos. También deben evaluar y mitigar riesgos a escala de la Unión, documentar y notificar sin demora los incidentes graves a la Oficina de IA y, cuando proceda, a las autoridades nacionales competentes, y garantizar un nivel adecuado de ciberseguridad del modelo y de su infraestructura física.

Propiedad Intelectual y Entrenamiento de Modelos



Data Mining / Crawler

Protocolo Opt-Out
Legible por Máquina

Dominio del Autor

Respeto a los Derechos de Autor

El Reglamento exige a los proveedores de modelos de inteligencia artificial establecer directrices formales para cumplir con la normativa europea de propiedad intelectual, específicamente con la Directiva 2019/790 sobre derechos de autor en el mercado único digital.

Mecanismos de Exclusión Tecnológica

Los proveedores de GPAI deben establecer una política para cumplir el Derecho de autor de la Unión e identificar y respetar reservas de derechos, incluyendo mediante tecnologías adecuadas cuando proceda. El artículo 53 exige política de copyright y respeto de reservas de derechos, pero no convierte robots.txt, ai.txt, XMP o marcas de agua en garantía absoluta.

Resúmenes de Datos de Entrenamiento

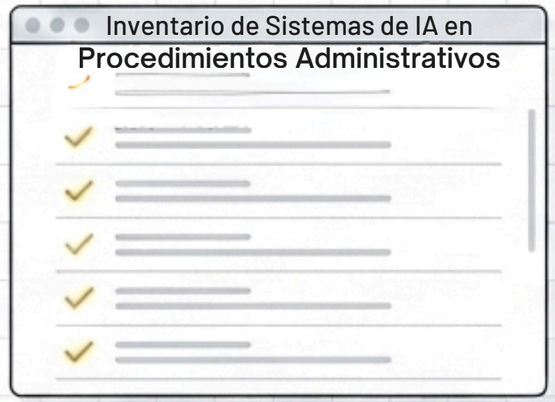
Los proveedores de modelos de IA de uso general deben elaborar y poner a disposición del público un resumen suficientemente detallado del contenido utilizado para el entrenamiento del modelo, conforme a la plantilla proporcionada por la Oficina de IA. Este resumen debe permitir una comprensión razonable de las categorías de contenido empleadas sin convertirlo en una garantía absoluta de control individual sobre cada obra o fuente concreta.

ApisDom

Entornos de Prueba y Sector Público

El Sandbox Regulatorio de la AESIA

El Reglamento de IA exige que los Estados miembros establezcan al menos un espacio controlado de pruebas a escala nacional. En España, el proyecto de Ley Orgánica prevé que este sandbox nacional sea operado por la AESIA y que permita probar sistemas de IA en un entorno controlado antes de su comercialización o puesta en servicio, con el objetivo de facilitar el cumplimiento normativo, fomentar la innovación y detectar riesgos bajo supervisión.



Inventario de Sistemas de IA utilizados en Procedimientos Administrativos

El Proyecto de Ley Orgánica para el buen uso y la gobernanza de la inteligencia artificial, en tramitación parlamentaria, impone obligaciones específicas de transparencia al sector público. La Administración General del Estado debe mantener un inventario de sistemas de IA utilizados en procedimientos administrativos, reforzando la transparencia.

Evaluaciones Previas en el Estado

Las entidades del sector público deben evaluar los riesgos de los sistemas de IA que utilicen en procedimientos administrativos, especialmente cuando puedan afectar a derechos fundamentales, decisiones públicas o garantías de los ciudadanos. Estas evaluaciones deben orientarse a detectar y mitigar riesgos, incluidos posibles sesgos, errores o impactos discriminatorios, conforme al Reglamento de IA, al RGPD y al desarrollo normativo español aplicable.

Régimen Sancionador y Consecuencias

El Proyecto de Ley Orgánica adapta al ordenamiento español el régimen sancionador del Reglamento Europeo de Inteligencia Artificial. El marco se basa en sanciones efectivas, proporcionadas y disuasorias, graduadas según la gravedad de la infracción, el volumen económico del infractor y las circunstancias del caso.

Infracciones Muy Graves	**Incumplimiento de la prohibición de** prácticas de IA (Art. 5 AI Act).	**Hasta 35 millones € o 7% del volumen global**
Infracciones Graves	**Otros incumplimientos de operadores, incluyendo obligaciones de transparencia (Art. 50 AI Act), gobernanza de datos y supervisión humana.**	**Hasta 15 millones € o 3% del volumen global**
Infracciones por Información Incorrecta	**Suministro de información incorrecta, incompleta o engañosa a las autoridades.**	**Hasta 7,5 millones € o 1% del volumen global**

ApisDom

Fuentes Oficiales Consultadas

Las disposiciones detalladas en este documento se sustentan en el marco regulatorio vigente y en la documentación técnica oficial publicada por las autoridades competentes.

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial. Se referencian específicamente los artículos 5, 10, 11, 12, 13, 14, 50, 51, 53, 55, 57, 72, 86, 99, 111 y 113.
https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Proyecto de Ley Orgánica para el buen uso y la gobernanza de la inteligencia artificial. Nota oficial del Ministerio para la Transformación Digital y de la Función Pública, 26 de mayo de 2026, sobre la aprobación del proyecto para su remisión al Congreso de los Diputados.
https://digital.gob.es/comunicacion/notas-prensa/mtdfp/2026/05/el-gobierno-aprueba-el-proyecto-de-ley-que-garantizara-una-super

Guías prácticas y recursos de la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA) para el cumplimiento del Reglamento Europeo de Inteligencia Artificial. Estas guías tienen carácter orientativo y no vinculante.
https://aesia.digital.gob.es/es/actualidad/recursos/guias-practicas-para-el-cumplimiento-del-ria

Guías y orientaciones de la Agencia Española de Protección de Datos (AEPD) sobre adecuación al RGPD de tratamientos que incorporan inteligencia artificial e inteligencia artificial agéntica desde la perspectiva de protección de datos.
https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf
https://www.aepd.es/guias/orientaciones-ia-agentica.pdf

ApisDom

Anexo: Registro de Cambios Críticos

Este documento ha sido depurado para eliminar incongruencias y estandarizar la terminología técnica respecto a las fuentes originales.

Precisión Terminológica	Se ha unificado la denominación de la Agencia Española de Supervisión de la Inteligencia Artificial exclusivamente bajo las siglas oficiales AESIA, corrigiendo errores tipográficos de las fuentes secundarias.
Diferenciación Normativa	Se ha establecido una distinción estricta entre el Reglamento (UE) 2024/1689 (normativa europea vigente de aplicación directa) y el Proyecto de Ley Orgánica (legislación nacional en tramitación destinada a regular las autoridades y sanciones internas).
Fechas de Exigibilidad	Se han incorporado las fechas verificadas conforme al artículo 113 del Reglamento (UE) 2024/1689, al calendario oficial del AI Act Service Desk y al acuerdo político del AI Omnibus. Este calendario distingue entre la aplicación general del Reglamento, las obligaciones de modelos de IA de uso general, la gobernanza, las obligaciones de transparencia y las fechas aplicables a sistemas de alto riesgo.
Inteligencia Artificial Agéntica	Se han incorporado las orientaciones específicas de la AEPD sobre inteligencia artificial agéntica desde la perspectiva de protección de datos. Estas orientaciones no constituyen normativa vinculante, sino una guía técnica sobre los riesgos, vulnerabilidades y posibles medidas que responsables y encargados pueden valorar cuando utilicen sistemas de IA agéntica en tratamientos de datos personales.

Regulación IA

ApisDom

Intelligence Group

inteligencia artificial transparente

ApisDom.com