CLOUDFRAMEWORK · WHITE PAPER

IA Empresarial en Europa: cómo cumplir el AI Act y el resto sin que el compliance bloquee el avance

Una guía práctica para CEOs, CTOs, DPOs y responsables de compliance que quieren **desplegar IA en serio** dentro del marco regulatorio europeo — desde el inventario hasta los controles operativos.

Edición: Mayo 2026 **Audiencia:** Dirección, tecnología, privacidad y compliance

Ámbito: Empresas que operan en la Unión Europea

1 · EL MOMENTO

El AI Act ya está aplicándose por fases — y los pilotos sin marco se están convirtiendo en pasivo

El Reglamento (UE) 2024/1689 — el **AI Act** — entró en vigor el 1 de agosto de 2024 y aplica en fases. A día de hoy ya están en aplicación las prohibiciones (febrero 2025) y las obligaciones para modelos de propósito general (agosto 2025). En **agosto de 2026** aplican las obligaciones para sistemas de alto riesgo. Y a partir de **agosto de 2027** se completa el resto.

REALIDAD

Muchas empresas tienen IA fuera de control

Pilotos creados por equipos independientes, asistentes corporativos contratados sin DPIA, datos sensibles enviados a APIs externas sin contrato adecuado. El primer ejercicio de cumplimiento empieza por descubrir *qué IA hay realmente en uso* — y suele sorprender.

SANCIÓN

Las multas del AI Act no son simbólicas

Hasta **35M € o el 7% de la facturación mundial** por prácticas prohibidas. Hasta **15M € o el 3%** por incumplimiento de obligaciones de alto riesgo. Hasta **7,5M € o el 1%** por información incorrecta a las autoridades. Aplicables además del régimen GDPR.

El patrón que vemos repetirse. Empresas que llevan dos años experimentando con IA descubren ahora que (a) no saben qué sistemas tienen desplegados, (b) no pueden documentar cómo se entrenaron o configuraron, (c) no hay registro de las decisiones automatizadas tomadas, y (d) no hay supervisión humana operativa. El compliance no se resuelve con una política PDF — se resuelve con un sustrato técnico que permita responder a un inspector.

Este documento se dirige a tres perfiles a la vez

CEO

Visión de riesgo y oportunidad

Qué decisiones de negocio cambia el marco regulatorio. Dónde están las exposiciones de la organización. Qué quick wins permiten avanzar sin bloquearse en jurídico.

CTO

Arquitectura, datos y operación

Qué requisitos técnicos imponen el AI Act y normas conexas. Cómo se estructura un sistema de IA empresarial auditable. Qué evidencia técnica hay que poder presentar.

DPO / COMPLIANCE

Mapa normativo, controles y evidencia

Cómo se entrelazan AI Act, GDPR, NIS2, DORA y normas sectoriales. Qué evaluaciones (DPIA, FRIA) aplican. Qué evidencia documental hay que mantener viva.

2 · EL MAPA NORMATIVO

Cinco bloques normativos que aplican a la vez — no son silos

Cuando una empresa europea despliega IA, no se enfrenta a una única norma. Se enfrenta a un **sistema regulatorio entrelazado** donde una misma actividad activa varias normas a la vez. Entenderlo es el primer paso para no quedarse en la lectura aislada del AI Act.

Bloque	Norma clave	Estado	Qué impone (resumen operativo)
IA	Reglamento (UE) 2024/1689 — **AI Act**	En aplicación por fases (2025–2027)	Clasificación por riesgo, obligaciones de proveedor y desplegador, documentación técnica, supervisión humana, gestión post-mercado, registro de sistemas de alto riesgo en base de datos UE.
Datos personales	Reglamento (UE) 2016/679 — **GDPR**	Vigente desde 2018	Base legal de tratamiento, minimización, decisiones automatizadas (Art. 22), DPIA, derechos de los interesados, transferencias internacionales.
Ciberseguridad	Directiva (UE) 2022/2555 — **NIS2**	Transposición completada en 2024–2025	Gestión de riesgos de ciberseguridad, notificación de incidentes (24h+72h), responsabilidad de la dirección, cadena de suministro de IT.
Resiliencia financiera	Reglamento (UE) 2022/2554 — **DORA**	Aplicable desde enero 2025	Gestión de riesgos TIC para entidades financieras, pruebas avanzadas de penetración, contratos con proveedores TIC críticos (incluida IA), reporte de incidentes graves.
Responsabilidad	Directiva (UE) 2024/2853 — **Product Liability** revisada	Vigente; aplicable a productos puestos en el mercado tras dic 2026	Software e IA expresamente incluidos como "producto". Régimen de responsabilidad objetiva del fabricante por daño causado por producto defectuoso.
Gestión de IA	ISO/IEC 42001:2023	Estándar voluntario, base de cumplimiento	Sistema de gestión específico para IA. Auditable. La forma práctica de demostrar gobierno organizativo de la IA ante una autoridad.

> **Cómo se cruzan en la práctica.** Un asistente conversacional para empleados que procesa datos de clientes activa simultáneamente: AI Act (transparencia + posiblemente alto riesgo si decide), GDPR (base legal + DPIA), NIS2 (si la empresa es entidad esencial o importante) y, si la empresa es financiera, DORA. Pretender resolver solo "el AI Act" es no entender el sistema.

3 · CLASIFICACIÓN

Cómo clasifica el AI Act tu sistema de IA — y por qué cambia todo

El AI Act es un reglamento **basado en riesgo**. La clasificación determina prácticamente todas las obligaciones que aplican. Un mismo modelo subyacente (por ejemplo un LLM) puede caer en categorías distintas según *cómo lo despliegas y para*

qué.

PROHIBIDA

Art. 5. Prácticas inaceptables. *Manipulación subliminal que cause daño, explotación de vulnerabilidades, social scoring por autoridades públicas, identificación biométrica remota en tiempo real en espacios públicos (salvo excepciones), reconocimiento de emociones en trabajo o educación (salvo motivos médicos o de seguridad), policía predictiva basada solo en perfilado, scraping no dirigido para bases faciales.*

ALTO RIESGO

Art. 6 + Anexo III. Sistemas que pueden afectar a salud, seguridad o derechos fundamentales. *Componentes de seguridad de productos regulados; biometría; infraestructuras críticas; educación (admisión, evaluación); empleo (selección, evaluación, asignación); acceso a servicios esenciales (incluido scoring crediticio y seguros); aplicación de la ley; migración y fronteras; administración de justicia y procesos democráticos.* **Conlleva las 8 obligaciones de la siguiente sección.**

RIESGO LIMITADO

Art. 50. Sistemas con riesgo de manipulación o confusión. *Chatbots (informar de que se interactúa con IA), deepfakes y contenido sintético (etiquetado), reconocimiento de emociones o categorización biométrica fuera de los casos prohibidos.* Obligaciones principales: **transparencia y etiquetado.**

MÍNIMO

El resto. Filtros antispam, IA en videojuegos, recomendadores no críticos. No hay obligaciones específicas, pero sí **códigos de conducta voluntarios** y sigue aplicando todo lo demás (GDPR, ciberseguridad, propiedad intelectual).

Aparte: los modelos de propósito general (GPAI)

Aplicables desde agosto de 2025. Los proveedores de modelos de propósito general (LLMs, modelos de imagen, etc.) tienen **obligaciones propias** con independencia del uso final: documentación técnica, política de copyright, resumen del corpus de entrenamiento. Los modelos con **riesgo sistémico** (umbral inicial: capacidad de cómputo $\geq 10^{25}$ FLOPs) tienen obligaciones adicionales: evaluación de modelo, mitigación de riesgos sistémicos, reporte de incidentes graves, ciberseguridad reforzada.

> **Trampa frecuente.** Muchas empresas asumen que "como solo usamos ChatGPT/Claude/Gemini, no nos aplica el AI Act". *Falso.* Como desplegador (deployer) tienes obligaciones propias en cuanto despliegas el modelo en un caso de uso de riesgo limitado o alto. El proveedor del modelo no cubre tu cumplimiento — solo el suyo.

4 · LAS 8 OBLIGACIONES

Qué exige el AI Act a un sistema de alto riesgo (Cap. III, Sec. 2)

Si tu sistema cae en alto riesgo — algo más común de lo que parece, especialmente en RRHH, finanzas, salud y servicios públicos — el AI Act impone **ocho obligaciones técnicas y organizativas** que se traducen directamente en requisitos de plataforma. No son "buenas prácticas". Son condiciones para poner el sistema en el mercado europeo.

1

Sistema de gestión de riesgos (Art. 9)

Proceso continuo a lo largo de todo el ciclo de vida del sistema. Identificación, análisis, evaluación y mitigación de los riesgos previsibles, incluidos los que afectan a grupos vulnerables. **Evidencia esperable:** documentación viva del proceso, no un informe puntual.

2

Datos y gobernanza de datos (Art. 10)

Conjuntos de entrenamiento, validación y prueba con prácticas de gobernanza adecuadas: relevancia, representatividad, ausencia de errores, mitigación de sesgos detectables. **Evidencia:** trazabilidad de los datasets, su procedencia y los controles aplicados.

3

Documentación técnica (Art. 11 + Anexo IV)

Descripción detallada del sistema antes de su puesta en mercado y mantenida actualizada. **Evidencia:** propósito, arquitectura, especificaciones de diseño, métricas, datasets, limitaciones conocidas.

4

Mantenimiento de registros / logging (Art. 12)

Registro automático de eventos durante el funcionamiento. Trazabilidad completa de cada operación que pueda tener impacto. **Evidencia:** logs íntegros, conservados con un período definido, recuperables ante una autoridad.

5

Transparencia y suministro de información (Art. 13)

El sistema se acompaña de instrucciones claras dirigidas al desplegador: capacidades, limitaciones, condiciones de uso, qué supervisión humana requiere, cómo se mide su rendimiento. **Evidencia:** manual de instrucciones técnico-operativo del sistema.

6

Supervisión humana (Art. 14)

El sistema permite que personas autorizadas supervisen su funcionamiento, interpreten sus resultados y, cuando proceda, intervengan o lo paren. **Evidencia:** interfaz de supervisión, roles asignados, registros de intervención.

7

Precisión, robustez y ciberseguridad (Art. 15)

Niveles adecuados frente a errores, fallos, inconsistencias y ataques (incluidos data poisoning, adversarial examples, model inversion). **Evidencia:** métricas declaradas, planes de pruebas, controles frente a ataques específicos de IA.

8

Sistema de gestión de la calidad (Art. 17, para proveedores)

Procedimientos documentados que aseguren el cumplimiento del Reglamento de forma continua. **Evidencia:** políticas, controles, ciclo de auditoría interna. **ISO/IEC 42001 está pensado precisamente para esto.**

> **Cómo lo lee un inspector.** No espera ver una caja negra que funciona. Espera ver *evidencia documental viva* que demuestre, en orden: qué hace el sistema, con qué datos, con qué riesgos identificados, con qué controles, con qué supervisión, con qué resultados. Si la información está dispersa en hojas de cálculo, repositorios sueltos y conversaciones de Slack, el sistema no cumple — aunque técnicamente "funcione bien".

5 · ROLES

Provider, Deployer, Importer, Distributor — qué papel juega tu empresa

El AI Act distribuye las obligaciones entre cuatro roles principales. Una misma empresa puede tener varios a la vez según el sistema. Confundir el rol que aplica es el error inicial más común — y el más costoso.

Rol	Definición operativa	Obligaciones principales
Provider (proveedor)	Desarrolla un sistema de IA o un modelo de propósito general y lo pone en el mercado o en servicio con su marca o nombre. Incluye a quien construye con código propio sobre un modelo de terceros si lo comercializa como sistema propio.	Las 8 obligaciones de la sección anterior. Marcado CE. Declaración UE de conformidad. Registro en la base de datos UE para sistemas de alto riesgo. Sistema de calidad. Vigilancia post-mercado.
Deployer (responsable del despliegue)	Utiliza un sistema de IA bajo su autoridad, en el contexto de una actividad profesional. **Es el rol más frecuente en las empresas usuarias.**	Uso conforme a las instrucciones del proveedor. Supervisión humana operativa. Monitoreo del funcionamiento. Conservación de logs cuando los controla. **FRIA** (Fundamental Rights Impact Assessment) en alto riesgo Anexo III si es entidad pública o presta servicios públicos. Información a personas afectadas. DPIA cuando aplique GDPR.
Importer (importador)	Persona o empresa establecida en la UE que pone en el mercado de la UE un sistema de IA con el nombre o marca de un proveedor establecido fuera de la UE.	Verificar que el proveedor ha cumplido sus obligaciones. Conservar copia de la documentación técnica y la declaración UE de conformidad. Indicar nombre y dirección en el sistema o su embalaje.
Distributor (distribuidor)	Cualquier persona en la cadena de suministro, distinta del proveedor o importador, que comercializa un sistema de IA en el mercado de la UE.	Diligencia para verificar conformidad antes de comercializar. Garantizar que las condiciones de almacenamiento o transporte no comprometen el cumplimiento.

> **La trampa del "personalizado".** Si tu empresa toma un modelo de terceros y lo personaliza sustancialmente, lo entrena adicionalmente, o lo comercializa bajo su propia marca, puede convertirse en **provider** de un nuevo sistema — con todas sus obligaciones. La línea entre deployer y provider no es siempre obvia y debe analizarse caso por caso.

6 · SECTORIALES CRÍTICOS

Cuatro verticales donde la IA cruza otras normativas además del AI Act

En estos sectores no basta con cumplir el AI Act. La actividad ya estaba regulada antes — y la IA añade una capa de obligaciones específicas que **no se derogan**: se suman.

BANCA · SEGUROS · FINTECH

AI Act + DORA + supervisión sectorial

Scoring crediticio y de riesgo de seguros son **alto riesgo** (Anexo III). DORA exige gestión avanzada de riesgos TIC, pruebas de penetración, y contratos reforzados con proveedores de IA críticos. El BCE y la EBA están emitiendo guías específicas sobre uso de IA en entidades supervisadas.

SALUD Y DISPOSITIVOS MÉDICOS

AI Act + MDR/IVDR

Software médico con IA cae en alto riesgo del AI Act **y** mantiene su régimen de dispositivo médico (MDR 2017/745, IVDR 2017/746). La evaluación de conformidad combina ambos. Centros sanitarios como deployers deben hacer FRIA además de las evaluaciones clínicas.

RECURSOS HUMANOS

Alto riesgo casi por defecto

Sistemas de selección, evaluación de desempeño, asignación de tareas, decisiones de promoción o despido son **alto riesgo** (Anexo III, punto 4). Aplican las 8 obligaciones del AI Act + GDPR Art. 22 (decisiones automatizadas) + derecho laboral nacional + información reforzada a representantes de trabajadores.

SECTOR PÚBLICO Y SERVICIOS ESENCIALES

FRIA obligatoria + transparencia

Administraciones, entidades de derecho público y operadores de servicios esenciales (energía, agua, transporte) tienen obligaciones reforzadas como deployers. FRIA obligatoria antes del despliegue. Información clara a las personas afectadas. Registro en base de datos UE.

Patrón común a todos los verticales. El AI Act no sustituye a la regulación sectorial — se superpone. La estrategia de cumplimiento debe partir de *qué normas ya aplican*, identificar dónde la IA añade obligaciones, y diseñar controles que cubran el conjunto, no uno a uno.

Cinco condiciones técnicas para que el cumplimiento sea operativo, no decorativo

Las políticas en PDF no cumplen el AI Act. Lo que cumple es **poder demostrar**, en cualquier momento, cómo se decide, con qué datos, bajo qué supervisión y con qué resultados. Eso exige un sustrato técnico-organizativo concreto.

1

Documentación viva — no estática

Procesos, modelos, datasets y controles documentados en un sistema que se actualiza cuando el sistema cambia, no en un PDF firmado hace seis meses que ya no refleja la realidad.

2

Trazabilidad de cada interacción

Logs íntegros de cada llamada al modelo: quién, cuándo, qué se le envió, qué devolvió, con qué versión, con qué configuración. Conservados de forma auditada y recuperables a demanda.

3

Perímetro de datos auditable

Saber exactamente qué datos toca la IA, dónde se almacenan, quién accede y bajo qué base legal. Sin esto no hay GDPR posible — y sin GDPR no hay AI Act posible.

4

Supervisión humana operativa

No el discurso de "el humano siempre supervisa". La supervisión real requiere interfaz para revisar, intervenir, revertir; roles asignados con autoridad efectiva; registro de las intervenciones.

5

Gobierno plurimodelo y reversible

Capacidad de cambiar de modelo o proveedor sin reescribir lo construido. Sin lock-in al LLM del mes. Esto es a la vez exigencia técnica y exigencia de DORA para entidades financieras.

6

Inventario IA único y actualizado

Una lista — no un Excel disperso — de todos los sistemas de IA en uso o desarrollo en la organización, con su clasificación, su responsable, su estado de cumplimiento y sus evidencias asociadas.

> **El test del inspector.** Si en menos de 24 horas una autoridad te pide ver (a) la lista de sistemas de IA en uso, (b) la clasificación de uno de ellos, (c) la DPIA o FRIA asociada, (d) los logs de las últimas 48 horas, (e) los registros de supervisión humana, y tu organización puede entregarlos sin pánico — el sustrato funciona. Si no, no.

8 · LA SOLUCIÓN

CLOUDFRAMEWORK: la plataforma EaaS que ya nace cumpliendo

CLOUDFRAMEWORK no es una capa de IA encima de tus sistemas — es una **plataforma Enterprise as a Service** que centraliza documentación, desarrollo, IA y formación en un mismo perímetro auditable, con ISO 27001 certificado y diseñada desde el primer día para encajar con el AI Act, GDPR, NIS2 y DORA.

Cómo CLOUDFRAMEWORK cubre cada obligación del AI Act

Obligación AI Act	Cómo lo resuelve CLOUDFRAMEWORK
Documentación técnica (Art. 11)	**CLOUD Documentum** mantiene viva la documentación de procesos, modelos, datasets y controles. Estructurada en negocio, desarrollo y producción. Versionado y trazable.
Gobernanza de datos (Art. 10)	Datos del cliente *siempre* en su infraestructura. Sin entrenamiento con datos externos. Procedencia y controles aplicados a cada dataset documentados en el sistema.
Logs e identificación (Art. 12)	**CloudIA** opera sobre MCPs con autenticación, 2FA y trazabilidad por defecto. Cada interacción queda registrada con usuario, modelo, prompt, respuesta, versión y configuración.
Transparencia (Art. 13)	Cada sistema desplegado se acompaña de su manual técnico-operativo generado desde la propia documentación viva, no como entregable separado que se queda obsoleto.
Supervisión humana (Art. 14)	Modelo "la IA propone, el humano decide" embebido en el flujo. Interfaces de revisión y aprobación. Roles y autoridad efectiva.
Robustez y ciberseguridad (Art. 15)	Infraestructura sobre Google Cloud / AWS con ISO 27001. Separación de entornos. Controles frente a ataques específicos de IA. Compatible con requisitos NIS2 y DORA.
Sistema de calidad (Art. 17)	Marco compatible con ISO/IEC 42001:2023 — el estándar específico para sistemas de gestión de IA. Estructura organizativa, ciclo de auditoría y políticas documentadas.
Gestión de riesgos (Art. 9)	Documentación viva integrada con el ciclo de desarrollo. Riesgos identificados se materializan en requisitos técnicos rastreables a lo largo del ciclo.

Lo que esto significa en la práctica

PLURIMODELO

Sin lock-in al LLM

La plataforma trabaja con cualquier modelo (Anthropic, OpenAI, Google, Mistral, modelos propios). Cambias de modelo sin reescribir nada. Cumple la exigencia de reversibilidad de DORA.

PERÍMETRO

Datos dentro de tu infraestructura

Los datos no salen del perímetro del cliente. Sin entrenamiento con tus datos por defecto. Acuerdos contractuales sobre uso de subprocesadores cuando aplica.

ISO 27001 + 42001

Compliance integrado

Operación bajo SGSI ISO 27001 certificado. Marco de gestión de IA alineado con ISO/IEC 42001. Auditorías documentadas. Evidencia presentable ante autoridades.

LAWORATORY — parte de nuestra solución LegalTech y partner de gobernanza

CLOUD LEGALTECH · PARTNER INTEGRADO

Conocimiento jurídico y gobernanza dentro del propio ecosistema CLOUDFRAMEWORK

LAWORATORY, fundada por **Óscar López**, forma parte de la **solución LegalTech de CLOUDFRAMEWORK**: opera sobre la misma plataforma EaaS que el resto de verticales (CLOUD Hipotech, CLOUD HRMS…) y comparte arquitectura, gobierno de datos e integración con CloudIA. No es un tercero asociado: es una pieza nativa del ecosistema.

Óscar es además **socio de CLOUDFRAMEWORK y responsable asesor del cumplimiento** de la propia compañía — la misma exigencia que aplicamos a nuestros clientes la sostenemos puertas adentro.

La combinación aporta a cada cliente: **clasificación de sistemas bajo el AI Act, evaluaciones DPIA y FRIA, contratos con proveedores de IA, gobierno corporativo de la IA y acompañamiento ante autoridades regulatorias**, todo conectado con el sustrato técnico de la plataforma — no en un Word aparte.

Resultado para el cliente: un único interlocutor para la dimensión técnica y la dimensión legal del cumplimiento — sin las costuras habituales entre consultora jurídica y proveedor tecnológico, y con responsabilidades claramente asignadas.

> **Principio operativo.** El compliance no se añade *después* a la IA empresarial — se construye *con* ella desde el principio. CLOUDFRAMEWORK aporta la plataforma y la operación; LAWORATORY aporta el conocimiento jurídico y la gobernanza. Juntos hacen que la regulación deje de ser el freno de los proyectos de IA y se convierta en el suelo desde el que despegan.

9 · HOJA DE RUTA

Seis pasos para llevar tu organización al cumplimiento operativo

No se cumple de una vez. Se cumple por orden, empezando por descubrir el alcance real de lo que ya está en uso. Esta es la secuencia que recomendamos a los clientes que arrancan con nosotros.

PASO 1

Inventario IA

Descubrir todos los sistemas de IA en uso o desarrollo en la organización. Incluye asistentes contratados, plugins, scripts internos, pilotos sin formalizar.

1–2 semanas

PASO 2

Clasificación AI Act

Aplicar el árbol de decisión a cada sistema: prohibido, alto riesgo, riesgo limitado o mínimo. Identificar el rol (provider / deployer) en cada uno.

2 semanas

PASO 3

Análisis de gaps

Para cada sistema clasificado, evaluar qué obligaciones cumple ya y qué falta. Incluye GDPR, NIS2 y normativa sectorial cuando aplique.

3–4 semanas

PASO 4

Evaluaciones (DPIA + FRIA)

Realizar DPIA para los sistemas que tratan datos personales y FRIA para los de alto riesgo del Anexo III. Documentación viva, no entregable PDF.

4–6 semanas

PASO 5

Implantación de controles

Desplegar el sustrato técnico (documentación viva, trazabilidad, supervisión humana operativa, inventario único) y los controles organizativos asociados. Conectar la IA con el gobierno existente, no en paralelo.

2–3 meses

PASO 6

Gobierno continuo

Establecer el ciclo de revisión periódica, las métricas, la vigilancia post-mercado, el reporting de incidentes, la formación recurrente. El cumplimiento no es un proyecto — es un sistema operativo.

Continuo

Qué se resuelve en cada horizonte

Horizonte	Resultado
Semana 4	Inventario IA cerrado, clasificación AI Act realizada, mapa de gaps por sistema. La organización sabe qué tiene y dónde está expuesta.
Mes 3	Evaluaciones DPIA/FRIA hechas para los sistemas prioritarios. Sustrato técnico básico desplegado. Decisiones críticas tomadas (qué se mantiene, qué se rediseña, qué se retira).
Mes 6	Sistemas de alto riesgo con todas las obligaciones cubiertas. Gobierno continuo en marcha. La organización opera IA en producción con evidencia presentable.
Largo plazo	Capacidad organizativa de cumplir por defecto al lanzar nuevos sistemas. La IA deja de ser proyecto excepcional y se integra al sistema de gestión normal de la empresa.

Siguiente paso: una sesión de diagnóstico regulatorio

Una primera conversación de 60 minutos con tu dirección, tu CTO y tu DPO para mapear los sistemas de IA en uso o desarrollo, identificar las exposiciones críticas bajo el marco europeo y proponer si — y cómo — tiene sentido un diagnóstico formal. Sin compromiso.

cloudframework.io/cloudia