CLOUDFRAMEWORK · WHITE PAPER CONJUNTO

Coautoría · CLOUDFRAMEWORK + LAWORATORY

Cómo construir sistemas de IA gobernables bajo el Reglamento Europeo de Inteligencia Artificial

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 **Coautoría:** CLOUDFRAMEWORK (capa técnica) + LAWORATORY (capa jurídica)

Ámbito: Empresas que operan en la Unión Europea

1 · CONTEXTO REGULATORIO

El Reglamento (UE) 2024/1689 y el enfoque basado en riesgo

El Reglamento (UE) 2024/1689 establece normas armonizadas en materia de inteligencia artificial y adopta un **enfoque basado en el riesgo**. Distingue, entre otros, entre proveedores de sistemas de IA, responsables del despliegue (deployers), proveedores de modelos de IA de uso general (GPAI), importadores y distribuidores.

En este marco, una organización que desarrolla, integra, configura o pone en servicio soluciones basadas en IA puede asumir **obligaciones regulatorias distintas según su papel en la cadena de valor**. Confundir el papel propio es el error de partida más caro: determina prácticamente todas las obligaciones que terminan aplicando.

El papel de CLOUDFRAMEWORK

CLOUDFRAMEWORK actúa como una plataforma que permite a sus clientes **desarrollar, integrar, gobernar y operar sistemas de IA** conectados con modelos de IA de uso general de terceros. Por ello, CLOUDFRAMEWORK se posiciona como una **capa técnica de gobierno, seguridad, trazabilidad y control operacional** que ayuda a las organizaciones a gestionar sistemas de IA conforme a las exigencias del Reglamento.

El papel de LAWORATORY

LAWORATORY, dirigida por Óscar López, aporta la **capa jurídica complementaria**: clasificación regulatoria de cada sistema de IA, evaluaciones DPIA y FRIA, contratos con proveedores de IA, gobierno corporativo de la IA y acompañamiento ante autoridades regulatorias. Ambas capas — técnica y jurídica — operan de forma coordinada sobre el mismo perímetro, evitando las costuras habituales entre consultoría jurídica y proveedor tecnológico.

2 · RESPONSABILIDAD COMPARTIDA

Modelo de responsabilidad compartida — quién responde de qué

La IA empresarial suele construirse mediante varias capas. Cada capa tiene un actor con responsabilidades propias. Identificarlas con claridad antes del despliegue evita ambigüedades contractuales y exposiciones regulatorias innecesarias.

CAPA 1

Proveedor del modelo de IA de uso general

OpenAI, Anthropic, Mistral, Meta u otros. Desarrolla y documenta el modelo de IA de uso general.

↓

CAPA 2

CLOUDFRAMEWORK

Capa de integración, gobierno, seguridad y trazabilidad. Aporta capacidades técnicas; no determina la clasificación jurídica ni sustituye obligaciones del cliente.

↓

CAPA 3

Sistema de IA del cliente

Asistente, copiloto, sistema RAG, flujo automatizado, motor de decisión. El cliente es habitualmente el proveedor o el responsable del despliegue de este sistema.

↓

CAPA 4

Responsable del despliegue (deployer)

Organización que utiliza el sistema de IA en su actividad. Aplica el sistema en un contexto productivo concreto y sostiene la supervisión humana operativa.

Distribución orientativa de responsabilidades

Actor	Responsabilidad principal
Proveedor del modelo de IA de uso general	Desarrollo y documentación del modelo de IA de uso general.
CLOUDFRAMEWORK	Capacidades técnicas de integración, gobierno, seguridad, trazabilidad y control.
Cliente	Finalidad prevista, clasificación de riesgo, configuración, datos, uso y cumplimiento aplicable.
Responsable del despliegue	Uso del sistema de IA conforme a las instrucciones, supervisión y control operativo.

> **Importante.** CLOUDFRAMEWORK **no sustituye** las obligaciones legales del proveedor o del responsable del despliegue del sistema de IA. La plataforma facilita controles técnicos y organizativos, pero la **evaluación jurídica final depende del caso de uso, del contexto, de los datos tratados y de la finalidad prevista**. Esa evaluación corresponde al cliente y a su asesoría legal — LAWORATORY puede acompañarla cuando así se contrate.

3 · CICLO DE VIDA

Gobierno del ciclo de vida del sistema de IA

El cumplimiento del Reglamento no debe abordarse únicamente como documentación previa al lanzamiento. Debe integrarse en **todo el ciclo de vida** del sistema de IA, desde su diseño hasta su retirada — y la evidencia debe generarse en cada fase, no reconstruirse a posteriori.

Fase	Capacidades relevantes
Diseño	Definición de finalidad prevista, políticas y restricciones.
Desarrollo	Versionado, pruebas, evaluación y trazabilidad.
Integración	Conexión con modelos de IA de uso general y sistemas empresariales.
Puesta en servicio	Controles de acceso, configuración segura y supervisión.
Operación	Registros, monitorización y control de uso.
Supervisión	Intervención humana, revisión y escalado.
Vigilancia poscomercialización	Seguimiento, incidencias y medidas correctoras.
Retirada	Desactivación, conservación de evidencias y trazabilidad histórica.

CLOUDFRAMEWORK permite incorporar estos controles de forma sistemática dentro de la operación empresarial de sistemas de IA, integrados con el resto del gobierno corporativo y no en paralelo.

4 · OBLIGACIONES RIA ⇔ CAPACIDADES

Relación entre obligaciones del RIA y capacidades de CLOUDFRAMEWORK

La siguiente matriz traduce las obligaciones del Reglamento en capacidades concretas de plataforma. La disponibilidad de la capacidad no equivale por sí misma a compliance — sigue siendo necesario que el cliente la configure, opere y documente correctamente en su caso de uso.

Obligación del Reglamento	Capacidad de CLOUDFRAMEWORK
Sistema de gestión de riesgos	Motor de políticas, controles configurables y flujos de revisión.
Gobernanza de datos	Trazabilidad de fuentes, controles de acceso y minimización.
Documentación técnica	Registro de configuración, versiones, políticas y evidencias.
Conservación de registros	Trazabilidad de peticiones, respuestas, modelos y acciones.
Transparencia e información al usuario	Metadatos, avisos, registros de interacción y mecanismos de información.
Supervisión humana	Flujos de aprobación, revisión humana e intervención operativa.
Precisión, solidez y ciberseguridad	Monitorización, controles de seguridad y detección de anomalías.
Vigilancia poscomercialización	Observabilidad continua, gestión de incidencias y evidencias.
Notificación de incidentes graves	Captura de eventos, reconstrucción de trazas y soporte documental.

5 · ARQUITECTURA RUNTIME

Arquitectura de gobierno en tiempo de ejecución

El principal reto de la IA empresarial no es solo acceder a modelos de IA de uso general, sino **gobernar cómo se utilizan en sistemas reales**. CLOUDFRAMEWORK actúa como una capa intermedia entre modelos de IA de uso general, aplicaciones empresariales, usuarios, sistemas internos y políticas corporativas.

Capacidades principales

Orquestación de modelos

- Conexión con varios modelos de IA de uso general
- Selección del modelo según política
- Sustitución o cambio de proveedor
- Rutas alternativas en caso de indisponibilidad
- Control por región, cliente o caso de uso

Aplicación de políticas

- Validación de instrucciones
- Filtrado de entradas y salidas
- Restricciones por usuario, rol o finalidad
- Bloqueo de usos no autorizados
- Reglas de seguridad y cumplimiento

Seguridad operacional

- Control de acceso basado en roles
- Aislamiento entre clientes o entornos
- Gestión segura de credenciales
- Control de conexiones
- Segregación de datos

Observabilidad y registros

- Conservación de peticiones
- Conservación de respuestas
- Identificación del modelo utilizado
- Trazabilidad de versiones
- Medición de uso, latencia y errores

Controles de gobierno

- Aprobación humana
- Revisión de resultados
- Escalado de incidencias
- Reversión de configuraciones
- Control de cambios

6 · TRAZABILIDAD

Trazabilidad y auditabilidad

El Reglamento exige que determinados sistemas de IA permitan **conservar registros y demostrar cómo han funcionado**. Sin un sustrato documental vivo no hay defensa posible ante una inspección, un auditor o una autoridad sectorial.

Qué debe cubrir la trazabilidad

OPERACIÓN

Lo que se ejecutó

- Entradas
- Salidas
- Instrucciones
- Versiones del sistema
- Modelo utilizado

GOBIERNO

Cómo se gobernó

- Políticas aplicadas
- Usuario o proceso que ejecutó la operación
- Aprobaciones humanas
- Incidencias
- Cambios de configuración

Evidencia desde el diseño

CLOUDFRAMEWORK permite generar y conservar evidencias técnicas relacionadas con:

- Registros de uso
- Trazabilidad de instrucciones
- Trazabilidad de modelos
- Historial de configuraciones
- Decisiones de enrutamiento
- Controles aplicados
- Aprobaciones y revisiones
- Incidentes y medidas correctoras

Estas capacidades facilitan **auditorías internas, revisiones de cumplimiento y preparación ante requerimientos de autoridades o terceros**.

7 · SUPERVISIÓN HUMANA

Supervisión humana y control operacional

Para sistemas de IA de alto riesgo, el Reglamento exige **medidas de supervisión humana adecuadas**. No basta el discurso "el humano siempre supervisa": la supervisión humana operativa exige interfaz para revisar, intervenir y revertir; roles asignados con autoridad efectiva; y registro de las intervenciones.

Qué debe permitir la supervisión humana

El Reglamento exige que una persona con competencia y autoridad suficiente pueda:

- Comprender el funcionamiento general del sistema
- Interpretar sus resultados
- Intervenir cuando sea necesario
- Detener o modificar el uso
- Revisar resultados relevantes
- Evitar o mitigar riesgos

Mecanismos que aporta CLOUDFRAMEWORK

- Flujos de aprobación
- Revisión humana previa o posterior
- Controles de escalado
- Colas de revisión
- Intervención manual
- Bloqueo de operaciones
- Reversión de decisiones o configuraciones

8 · GOBIERNO GPAI

Gobierno de modelos de IA de uso general de terceros

Muchos sistemas empresariales se construyen sobre modelos de IA de uso general proporcionados por terceros. Esto introduce **riesgos específicos** que la organización debe gestionar de forma explícita, no asumir resueltos por defecto.

Riesgos específicos del uso de GPAI de terceros

OPERACIONAL

- Dependencia de proveedor
- Cambios de modelo
- Disponibilidad
- Variaciones de rendimiento

VISIBILIDAD Y DATOS

- Falta de visibilidad
- Transferencia de datos
- Residencia de datos
- Diferencias de políticas contractuales

Cómo CLOUDFRAMEWORK ayuda a gestionar estos riesgos

- Registro de modelos autorizados
- Control de versiones
- Listas de modelos permitidos o prohibidos
- Selección de modelo conforme a política
- Restricciones geográficas
- Separación por entorno o cliente
- Trazabilidad del modelo utilizado en cada operación
- Sustitución controlada de proveedor

9 · CLASIFICACIÓN DE RIESGO

Apoyo a la clasificación de riesgo

La clasificación de un sistema de IA bajo el Reglamento depende principalmente de su finalidad prevista, el sector, el contexto de uso, los datos tratados, el impacto potencial sobre personas físicas, el grado de autonomía y los efectos jurídicos o significativos similares. **No es una decisión técnica única: es una evaluación jurídica integral.**

Factores relevantes para la clasificación

- La finalidad prevista
- El sector
- El contexto de uso
- Los datos tratados

- El impacto potencial sobre personas físicas
- El grado de autonomía
- Los efectos jurídicos o significativos similares

Ejemplos orientativos

Caso de uso	Posible clasificación
Asistente documental interno	Riesgo limitado o mínimo
Copiloto corporativo general	Riesgo limitado o mínimo
Cribado de candidatos	Alto riesgo
Evaluación crediticia	Alto riesgo
Triaje médico	Alto riesgo
Identificación biométrica	Alto riesgo o prohibido, según el caso
Asistente jurídico	Variable según finalidad y uso

CLOUDFRAMEWORK puede ayudar a documentar, controlar y monitorizar el sistema, pero no determina por sí mismo la clasificación jurídica definitiva. Esa determinación corresponde al cliente y a su asesoría legal — LAWORATORY puede acompañarla con análisis caso por caso cuando así se contrate.

Seguridad, soberanía y residencia de datos

Los sistemas de IA empresariales pueden generar **nuevos riesgos de seguridad** que no existían antes de la adopción masiva de modelos GPAI de terceros. La empresa que despliega IA hereda esos riesgos y debe articular controles concretos para mitigarlos.

Nuevos riesgos a considerar

- Exposición de información confidencial
- Fuga de datos personales
- Uso no autorizado de modelos
- Transferencia internacional de datos
- Pérdida de control sobre instrucciones o respuestas
- Uso de herramientas no aprobadas

Capacidades que aporta CLOUDFRAMEWORK

- Aislamiento de entornos
- Control de acceso
- Gestión segura de credenciales
- Cifrado
- Enmascaramiento de datos personales
- Restricción por región
- Políticas de residencia
- Control de proveedores autorizados
- Trazabilidad de transferencias y accesos

Estas capacidades son **especialmente relevantes para organizaciones reguladas, administraciones públicas, salud, servicios financieros e infraestructuras críticas**, donde la combinación de regulación sectorial, GDPR, NIS2 y AI Act exige una arquitectura técnica defendible desde el primer día.

11 · POSCOMERCIALIZACIÓN

Vigilancia poscomercialización

La conformidad **no finaliza con la puesta en servicio**. Los sistemas de IA deben ser monitorizados durante su operación para detectar desviaciones, usos indebidos, degradación de rendimiento y riesgos no previstos en el diseño inicial.

Qué hay que detectar durante la operación

- Errores
- Desviaciones
- Usos indebidos
- Degradación de rendimiento
- Incidentes
- Incumplimientos de políticas
- Riesgos no previstos

Capacidades de vigilancia que aporta CLOUDFRAMEWORK

- Monitorización continua
- Detección de anomalías
- Alertas
- Revisión de eventos
- Seguimiento de incidencias
- Análisis de uso
- Conservación de evidencias
- Soporte a medidas correctoras

12 · EVIDENCIAS Y AUDITORÍA

Generación de evidencias y preparación para auditoría

Uno de los principales retos del cumplimiento del Reglamento es **demostrar de forma verificable** que existen controles efectivos. No basta con tener procedimientos: hay que poder mostrar evidencia material, fechada, íntegra y trazable hasta su origen.

Sobre qué se consolida la evidencia

- Configuración del sistema
- Finalidad prevista
- Modelos utilizados
- Versiones
- Políticas aplicadas
- Registros de uso
- Revisiones humanas
- Incidencias
- Medidas correctoras
- Cambios relevantes

Para qué sirve esa evidencia

- Preparación para auditoría
- Revisiones internas
- Cumplimiento contractual
- Respuestas ante autoridades

- Certificaciones
- Evaluaciones de proveedores
- Continuidad del gobierno del sistema de IA

13 · LIMITACIONES

Limitaciones y responsabilidades

CLOUDFRAMEWORK proporciona una plataforma técnica para **integrar, gobernar, operar y monitorizar** sistemas de IA empresariales. Es importante delimitar con precisión qué no hace — y qué corresponde siempre al cliente y a su asesoría legal.

Lo que CLOUDFRAMEWORK no hace

- **No presta asesoramiento jurídico.**
- **No sustituye la evaluación de conformidad** cuando sea exigible.
- **No determina automáticamente la clasificación de riesgo.**
- **No garantiza por sí solo el cumplimiento del Reglamento.**
- **No reemplaza las obligaciones del proveedor** ni del responsable del despliegue.

Qué debe evaluar cada organización en su caso

Cada organización debe evaluar su caso concreto atendiendo a:

- Finalidad prevista
- Datos tratados
- Sector
- Usuarios afectados

- Impacto potencial
- Grado de autonomía
- Integración con otros sistemas
- Obligaciones sectoriales aplicables

Cómo encaja LAWORATORY. Cuando el cliente lo solicita, LAWORATORY asume esa capa de evaluación jurídica: clasificación regulatoria del sistema, DPIA, FRIA, contratos con proveedores de IA, gobierno corporativo, acompañamiento ante autoridades. La capa técnica y la capa jurídica trabajan sobre el mismo perímetro de evidencia.

LAWORATORY · PARTNER INTEGRADO

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 coautoría de este whitepaper conjunto la firma él en la dimensión jurídica.

La combinación aporta a cada cliente: **clasificación de sistemas bajo el AI Act, evaluaciones DPIA y FRIA, contratos con proveedores de IA, modelo de responsabilidad compartida documentado, 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 en cada actor del shared responsibility model descrito en la sección 2.

Principio operativo. El compliance no se añade *después* a la IA empresarial — se construye *con* ella desde el principio. CLOUDFRAMEWORK aporta la capa técnica de governance y compliance enablement; LAWORATORY aporta el conocimiento jurídico y la clasificación de cada sistema. 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 — sin trasladar al cliente la falsa promesa de que "usar la plataforma = compliant".

14 · CONCLUSIÓN

La IA empresarial como disciplina de gobierno continuo

El Reglamento Europeo de Inteligencia Artificial transforma la IA empresarial en una **disciplina de gobierno técnico, jurídico y operativo continuo**. Las organizaciones que desarrollen, integren o utilicen sistemas de IA necesitarán capacidades permanentes — no proyectos puntuales.

Capacidades permanentes que la empresa debe sostener

- Controlar el uso de modelos de IA de uso general
- Conservar registros
- Documentar configuraciones
- Supervisar resultados
- Gestionar riesgos
- Aplicar políticas
- Monitorizar incidencias
- Generar evidencias

CLOUDFRAMEWORK se posiciona como una **capa de gobierno y operación** para sistemas de IA empresariales, diseñada para ayudar a las organizaciones a desplegar IA de forma **trazable, segura, auditable y alineada** con las exigencias del marco regulatorio europeo. LAWORATORY aporta la capa jurídica que complementa esa operación con la evaluación de cumplimiento exigible en cada caso.

Calendario de aplicación del Reglamento

El Reglamento (UE) 2024/1689 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.

✓ Feb 2025
Prácticas **prohibidas** (Art. 5) en aplicación

✓ Ago 2025
Obligaciones para **GPAI** (Cap. V)

⏱ Ago 2026
Obligaciones para **sistemas de alto riesgo** (Cap. III, Sec. 2)

2027
Sistemas regulados sectorialmente y resto de obligaciones

Nuevo calendario para sistemas de alto riesgo — Reglamento Ómnibus Digital

El **Reglamento Ómnibus Digital en materia de Inteligencia Artificial** retrasa la aplicación de las normas para sistemas de alto riesgo, con el objeto de permitir una mejor preparación técnica:

2 DIC 2027

Sistemas autónomos de alto riesgo

Biometría, infraestructuras, educación, empleo. Aplicables a partir del **2 de diciembre de 2027**.

2 AGO 2028

Sistemas integrados en productos

Juguetes, ascensores, dispositivos médicos. Aplicables a partir del **2 de agosto de 2028**.

Lectura comercial. La extensión de plazos por el Reglamento Ómnibus es una oportunidad de preparación, no una excusa para retrasar el gobierno de la IA. Las organizaciones que arranquen ahora estarán listas — con evidencia y con criterio — cuando aplique. Las que esperen al último trimestre llegarán con la documentación incompleta y sin sustrato técnico.

Siguiente paso: una sesión conjunta CLOUDFRAMEWORK + LAWORATORY

Una conversación de 60 minutos con tu dirección, tu CTO/CISO y tu DPO/legal counsel. Mapeamos los sistemas de IA en uso o desarrollo, clasificamos el rol probable de tu organización para cada uno y proponemos — si tiene sentido — un diagnóstico formal técnico-jurídico. Sin compromiso.

cloudframework.io/cloudia

CLOUDFRAMEWORK aporta capacidades técnicas (gobierno, trazabilidad, control operacional). LAWORATORY aporta evaluación jurídica y clasificación regulatoria. Ambas capas trabajan sobre el mismo perímetro.

© 2026 CLOUDFRAMEWORK y LAWORATORY. White paper de uso comercial — no distribuir sin autorización. *Este documento es informativo y no constituye asesoramiento jurídico. La evaluación jurídica, la clasificación de riesgo de los sistemas de IA y la conformidad regulatoria corresponden al proveedor/deployer del sistema y a su asesoría legal.*