CLOUDFRAMEWORK · WHITE PAPER CONJUNTO

Coautoria · **CLOUDFRAMEWORK + LAWORATORY**

Como construir sistemas de IA governáveis sob o Regulamento Europeu de Inteligência Artificial

Um guia prático para CEOs, CTOs, DPOs e responsáveis de compliance que pretendem implementar IA a sério dentro do quadro regulatório europeu — desde o **inventário** até aos **controlos operacionais**.

Edição: Maio 2026

Coautoria: CLOUDFRAMEWORK (camada técnica) + LAWORATORY (camada jurídica)

Âmbito: Empresas que operam na União Europeia

1 · CONTEXTO REGULATÓRIO

O Regulamento (UE) 2024/1689 e a abordagem baseada no risco

O Regulamento (UE) 2024/1689 estabelece normas harmonizadas em matéria de inteligência artificial e adota uma **abordagem baseada no risco**. Distingue, entre outros, entre fornecedores de sistemas de IA, responsáveis pela implementação (deployers), fornecedores de modelos de IA de uso geral (GPAI), importadores e distribuidores.

Neste quadro, uma organização que desenvolva, integre, configure ou coloque em serviço soluções baseadas em IA pode assumir **obrigações regulatórias distintas em função do seu papel na cadeia de valor**. Confundir o próprio papel é o erro inicial mais caro: determina praticamente todas as obrigações que acabarão por aplicar-se.

O papel da CLOUDFRAMEWORK

A CLOUDFRAMEWORK atua como uma plataforma que permite aos seus clientes **desenvolver, integrar, governar e operar sistemas de IA** ligados a modelos de IA de uso geral de terceiros. Por isso, a CLOUDFRAMEWORK posiciona-se como uma **camada técnica de governo, segurança, rastreabilidade e controlo operacional** que ajuda as organizações a gerir sistemas de IA conforme as exigências do Regulamento.

O papel da LAWORATORY

A LAWORATORY, dirigida por Óscar López, aporta a **camada jurídica complementar**: classificação regulatória de cada sistema de IA, avaliações DPIA e FRIA, contratos com fornecedores de IA, governo corporativo da IA e acompanhamento perante autoridades regulatórias. Ambas as camadas — técnica e jurídica — operam de forma coordenada sobre o mesmo perímetro, evitando as costuras habituais entre consultoria jurídica e fornecedor tecnológico.

2 · RESPONSABILIDADE PARTILHADA

Modelo de responsabilidade partilhada — quem responde por quê

A IA empresarial é geralmente construída através de várias camadas. Cada camada tem um ator com responsabilidades próprias. Identificá-las com clareza antes da implementação evita ambiguidades contratuais e exposições regulatórias desnecessárias.

CAMADA 1

Fornecedor do modelo de IA de uso geral

OpenAI, Anthropic, Mistral, Meta ou outros. Desenvolve e documenta o modelo de IA de uso geral.

↓

CAMADA 2

CLOUDFRAMEWORK

Camada de integração, governo, segurança e rastreabilidade. Aporta capacidades técnicas; não determina a classificação jurídica nem substitui obrigações do cliente.

↓

CAMADA 3

Sistema de IA do cliente

Assistente, copiloto, sistema RAG, fluxo automatizado, motor de decisão. O cliente é habitualmente o fornecedor ou o responsável pela implementação deste sistema.

↓

CAMADA 4

Responsável pela implementação (deployer)

Organização que utiliza o sistema de IA na sua atividade. Aplica o sistema num contexto produtivo concreto e sustenta a supervisão humana operacional.

Distribuição orientativa de responsabilidades

Ator	Responsabilidade principal
Fornecedor do modelo GPAI	Desenvolvimento e documentação do modelo de IA de uso geral.
CLOUDFRAMEWORK	Capacidades técnicas de integração, governo, segurança, rastreabilidade e controlo.
Cliente	Finalidade prevista, classificação de risco, configuração, dados, uso e cumprimento aplicável.
Responsável pela implementação	Uso do sistema de IA conforme as instruções, supervisão e controlo operacional.

> **Importante.** A CLOUDFRAMEWORK **não substitui** as obrigações legais do fornecedor ou do responsável pela implementação do sistema de IA. A plataforma facilita controlos técnicos e organizacionais, mas a **avaliação jurídica final depende do caso de uso, do contexto, dos dados tratados e da finalidade prevista**. Essa avaliação cabe ao cliente e à sua assessoria jurídica — a LAWORATORY pode acompanhá-la quando assim for contratado.

3 · CICLO DE VIDA

Governo do ciclo de vida do sistema de IA

O cumprimento do Regulamento não deve ser abordado apenas como documentação prévia ao lançamento. Deve integrar-se em **todo o ciclo de vida** do sistema de IA, desde o seu desenho até à retirada — e a evidência deve gerar-se em cada fase, não reconstruir-se a posteriori.

Fase	Capacidades relevantes
Desenho	Definição de finalidade prevista, políticas e restrições.
Desenvolvimento	Versionamento, testes, avaliação e rastreabilidade.
Integração	Ligação com modelos de IA de uso geral e sistemas empresariais.
Colocação em serviço	Controlos de acesso, configuração segura e supervisão.
Operação	Registos, monitorização e controlo de uso.
Supervisão	Intervenção humana, revisão e escalonamento.
Vigilância pós-comercialização	Acompanhamento, incidências e medidas corretivas.
Retirada	Desativação, conservação de evidências e rastreabilidade histórica.

A CLOUDFRAMEWORK permite incorporar estes controlos de forma sistemática dentro da operação empresarial de sistemas de IA, integrados com o resto do governo corporativo e não em paralelo.

4 · OBRIGAÇÕES RIA ⇔ CAPACIDADES

Relação entre obrigações do RIA e capacidades da CLOUDFRAMEWORK

A seguinte matriz traduz as obrigações do Regulamento em capacidades concretas da plataforma. **A disponibilidade da capacidade não equivale por si só a compliance** — continua a ser necessário que o cliente a configure, opere e documente corretamente no seu caso de uso.

Obrigação do Regulamento	Capacidade da CLOUDFRAMEWORK
Sistema de gestão de riscos	Motor de políticas, controlos configuráveis e fluxos de revisão.
Governança de dados	Rastreabilidade de fontes, controlos de acesso e minimização.
Documentação técnica	Registo de configuração, versões, políticas e evidências.
Conservação de registos	Rastreabilidade de pedidos, respostas, modelos e ações.
Transparência e informação ao utilizador	Metadados, avisos, registos de interação e mecanismos de informação.
Supervisão humana	Fluxos de aprovação, revisão humana e intervenção operacional.
Precisão, solidez e cibersegurança	Monitorização, controlos de segurança e deteção de anomalias.
Vigilância pós-comercialização	Observabilidade contínua, gestão de incidências e evidências.
Notificação de incidentes graves	Captura de eventos, reconstrução de traços e suporte documental.

5 · ARQUITETURA RUNTIME

Arquitetura de governo em tempo de execução

O principal desafio da IA empresarial não é apenas aceder a modelos de IA de uso geral, mas **governar como são utilizados em sistemas reais**. A CLOUDFRAMEWORK atua como uma camada intermédia entre modelos GPAI, aplicações empresariais, utilizadores, sistemas internos e políticas corporativas.

Capacidades principais

Orquestração de modelos

- Ligação com vários modelos GPAI
- Seleção de modelo por política
- Substituição ou troca de fornecedor
- Rotas alternativas em caso de indisponibilidade
- Controlo por região, cliente ou caso de uso

Aplicação de políticas

- Validação de instruções
- Filtragem de entradas e saídas
- Restrições por utilizador, papel ou finalidade
- Bloqueio de usos não autorizados
- Regras de segurança e cumprimento

Segurança operacional

- Controlo de acesso baseado em papéis
- Isolamento entre clientes ou ambientes
- Gestão segura de credenciais
- Controlo de ligações
- Segregação de dados

Observabilidade e registos

- Conservação de pedidos
- Conservação de respostas
- Identificação do modelo utilizado
- Rastreabilidade de versões
- Medição de uso, latência e erros

Controlos de governo

- Aprovação humana
- Revisão de resultados
- Escalonamento de incidências
- Reversão de configurações
- Controlo de mudanças

6 · RASTREABILIDADE

Rastreabilidade e auditabilidade

O Regulamento exige que determinados sistemas de IA permitam **conservar registos e demonstrar como funcionaram**. Sem um substrato documental vivo não há defesa possível perante uma inspeção, um auditor ou uma autoridade setorial.

O que deve cobrir a rastreabilidade

OPERAÇÃO

O que foi executado

- Entradas
- Saídas
- Instruções
- Versões do sistema
- Modelo utilizado

GOVERNO

Como foi governado

- Políticas aplicadas
- Utilizador ou processo que executou a operação
- Aprovações humanas
- Incidências
- Mudanças de configuração

Evidência desde o desenho

A CLOUDFRAMEWORK permite gerar e conservar evidências técnicas relacionadas com:

- Registos de uso
- Rastreabilidade de instruções
- Rastreabilidade de modelos
- Histórico de configurações
- Decisões de encaminhamento
- Controlos aplicados
- Aprovações e revisões
- Incidentes e medidas corretivas

Estas capacidades facilitam **auditorias internas, revisões de cumprimento e preparação perante requisitos de autoridades ou terceiros**.

7 · SUPERVISÃO HUMANA

Supervisão humana e controlo operacional

Para sistemas de IA de alto risco, o Regulamento exige **medidas de supervisão humana adequadas**. Não basta o discurso "o humano supervisiona sempre": a supervisão humana operacional exige interface para rever, intervir e reverter; papéis atribuídos com autoridade efetiva; e registo das intervenções.

O que deve permitir a supervisão humana

O Regulamento exige que uma pessoa com competência e autoridade suficientes possa:

- Compreender o funcionamento geral do sistema
- Interpretar os seus resultados
- Intervir quando necessário
- Parar ou modificar o uso
- Rever resultados relevantes
- Evitar ou mitigar riscos

Mecanismos que a CLOUDFRAMEWORK fornece

- Fluxos de aprovação
- Revisão humana prévia ou posterior
- Controlos de escalonamento
- Filas de revisão
- Intervenção manual
- Bloqueio de operações
- Reversão de decisões ou configurações

8 · GOVERNO GPAI

Governo de modelos de IA de uso geral de terceiros

Muitos sistemas empresariais são construídos sobre modelos GPAI fornecidos por terceiros. Isto introduz **riscos específicos** que a organização deve gerir de forma explícita, não assumir resolvidos por defeito.

Riscos específicos do uso de GPAI de terceiros

OPERACIONAL

- Dependência de fornecedor
- Mudanças de modelo
- Disponibilidade
- Variações de desempenho

VISIBILIDADE E DADOS

- Falta de visibilidade
- Transferência de dados
- Residência de dados
- Diferenças de políticas contratuais

Como a CLOUDFRAMEWORK ajuda a gerir estes riscos

- Registo de modelos autorizados
- Controlo de versões
- Listas de modelos permitidos ou proibidos
- Seleção de modelo conforme política
- Restrições geográficas
- Separação por ambiente ou cliente
- Rastreabilidade do modelo utilizado em cada operação
- Substituição controlada de fornecedor

9 · CLASSIFICAÇÃO DE RISCO

Apoio à classificação de risco

A classificação de um sistema de IA sob o Regulamento depende principalmente da sua finalidade prevista, do setor, do contexto de uso, dos dados tratados, do impacto potencial sobre pessoas singulares, do grau de autonomia e dos efeitos jurídicos ou significativos similares. **Não é uma decisão técnica única: é uma avaliação jurídica integral.**

Fatores relevantes para a classificação

- A finalidade prevista
- O setor
- O contexto de uso
- Os dados tratados

- O impacto potencial sobre pessoas singulares
- O grau de autonomia
- Os efeitos jurídicos ou significativos similares

Exemplos orientativos

Caso de uso	Possível classificação
Assistente documental interno	Risco limitado ou mínimo
Copiloto corporativo geral	Risco limitado ou mínimo
Triagem de candidatos	Alto risco
Avaliação de crédito	Alto risco
Triagem médica	Alto risco
Identificação biométrica	Alto risco ou proibido, conforme o caso
Assistente jurídico	Variável segundo finalidade e uso

A CLOUDFRAMEWORK pode ajudar a documentar, controlar e monitorizar o sistema, mas não determina por si mesma a classificação jurídica definitiva. Essa determinação cabe ao cliente e à sua assessoria jurídica — a LAWORATORY pode acompanhá-la com análise caso a caso quando assim for contratado.

Segurança, soberania e residência de dados

Os sistemas de IA empresariais podem gerar **novos riscos de segurança** que não existiam antes da adoção massiva de modelos GPAI de terceiros. A empresa que implementa IA herda esses riscos e deve articular controlos concretos para mitigá-los.

Novos riscos a considerar

- Exposição de informação confidencial
- Fuga de dados pessoais
- Uso não autorizado de modelos
- Transferência internacional de dados
- Perda de controlo sobre instruções ou respostas
- Uso de ferramentas não aprovadas

Capacidades que a CLOUDFRAMEWORK aporta

- Isolamento de ambientes
- Controlo de acesso
- Gestão segura de credenciais
- Cifragem
- Mascaramento de dados pessoais
- Restrição por região
- Políticas de residência
- Controlo de fornecedores autorizados
- Rastreabilidade de transferências e acessos

Estas capacidades são **especialmente relevantes para organizações reguladas, administrações públicas, saúde, serviços financeiros e infraestruturas críticas**, onde a combinação de regulação setorial, RGPD, NIS2 e AI Act exige uma arquitetura técnica defensável desde o primeiro dia.

11 · PÓS-COMERCIALIZAÇÃO

Vigilância pós-comercialização

A conformidade **não termina com a colocação em serviço**. Os sistemas de IA devem ser monitorizados durante a sua operação para detetar desvios, usos indevidos, degradação de desempenho e riscos não previstos no desenho inicial.

O que detetar durante a operação

- Erros
- Desvios
- Usos indevidos
- Degradação de desempenho
- Incidentes
- Incumprimentos de políticas
- Riscos não previstos

Capacidades de vigilância que a CLOUDFRAMEWORK aporta

- Monitorização contínua
- Deteção de anomalias
- Alertas
- Revisão de eventos
- Acompanhamento de incidências
- Análise de uso
- Conservação de evidências
- Suporte a medidas corretivas

12 · EVIDÊNCIAS E AUDITORIA

Geração de evidências e preparação para auditoria

Um dos principais desafios do cumprimento do Regulamento é **demonstrar de forma verificável** que existem controlos efetivos. Não basta ter procedimentos: é preciso poder mostrar evidência material, datada, íntegra e rastreável até à sua origem.

Sobre o que se consolida a evidência

- Configuração do sistema
- Finalidade prevista
- Modelos utilizados
- Versões
- Políticas aplicadas
- Registos de uso
- Revisões humanas
- Incidências
- Medidas corretivas
- Mudanças relevantes

Para que serve essa evidência

- Preparação para auditoria
- Revisões internas
- Cumprimento contratual
- Respostas perante autoridades

- Certificações
- Avaliações de fornecedores
- Continuidade do governo do sistema de IA

13 · LIMITAÇÕES

Limitações e responsabilidades

A CLOUDFRAMEWORK fornece uma plataforma técnica para **integrar, governar, operar e monitorizar** sistemas de IA empresariais. É importante delimitar com precisão o que não faz — e o que cabe sempre ao cliente e à sua assessoria jurídica.

O que a CLOUDFRAMEWORK não faz

- **Não presta assessoria jurídica.**
- **Não substitui a avaliação de conformidade** quando exigível.
- **Não determina automaticamente a classificação de risco.**
- **Não garante por si só o cumprimento do Regulamento.**
- **Não substitui as obrigações do fornecedor** nem do responsável pela implementação.

O que cada organização deve avaliar no seu caso

Cada organização deve avaliar o seu caso concreto atendendo a:

- Finalidade prevista
- Dados tratados
- Setor
- Utilizadores afetados

- Impacto potencial
- Grau de autonomia
- Integração com outros sistemas
- Obrigações setoriais aplicáveis

Como a LAWORATORY se encaixa. Quando o cliente o solicita, a LAWORATORY assume essa camada de avaliação jurídica: classificação regulatória do sistema, DPIA, FRIA, contratos com fornecedores de IA, governo corporativo, acompanhamento perante autoridades. A camada técnica e a camada jurídica trabalham sobre o mesmo perímetro de evidência.

LAWORATORY · PARCEIRO INTEGRADO

LAWORATORY — parte da nossa solução LegalTech e parceiro de governança

CLOUD LEGALTECH · PARCEIRO INTEGRADO

Conhecimento jurídico e governança dentro do próprio ecossistema CLOUDFRAMEWORK

A **LAWORATORY**, fundada por **Óscar López**, faz parte da **solução LegalTech da CLOUDFRAMEWORK**: opera sobre a mesma plataforma EaaS que o resto das verticais (CLOUD Hipotech, CLOUD HRMS...) e partilha arquitetura, governo de dados e integração com CloudIA. Não é um terceiro associado: é uma peça nativa do ecossistema.

Óscar é também **sócio da CLOUDFRAMEWORK e responsável assessor do cumprimento** da própria empresa — a mesma exigência que aplicamos aos nossos clientes sustentamo-la portas adentro. A coautoria deste whitepaper conjunto é assinada por ele na dimensão jurídica.

A combinação aporta a cada cliente: **classificação de sistemas sob o AI Act, avaliações DPIA e FRIA, contratos com fornecedores de IA, modelo de responsabilidade partilhada documentado, governo corporativo da IA e acompanhamento perante autoridades regulatórias**, tudo ligado ao substrato técnico da plataforma — não num Word à parte.

Resultado para o cliente: um único interlocutor para a dimensão técnica e a dimensão jurídica do cumprimento — sem as costuras habituais entre consultoria jurídica e fornecedor tecnológico, e com responsabilidades claramente atribuídas a cada ator do shared responsibility model descrito na secção 2.

Princípio operacional. O compliance não se adiciona *depois* à IA empresarial — constrói-se *com* ela desde o início. A CLOUDFRAMEWORK aporta a camada técnica de governança e compliance enablement; a LAWORATORY aporta o conhecimento jurídico e a classificação de cada sistema. Juntas fazem com que a regulação deixe de ser o travão dos projetos de IA e se converta no chão a partir do qual descolam — sem transmitir ao cliente a falsa promessa de que "usar a plataforma = compliant".

14 · CONCLUSÃO

A IA empresarial como disciplina de governo contínuo

O Regulamento Europeu de Inteligência Artificial transforma a IA empresarial numa **disciplina de governo técnico, jurídico e operacional contínuo**. As organizações que desenvolvam, integrem ou utilizem sistemas de IA necessitarão de capacidades permanentes — não de projetos pontuais.

Capacidades permanentes que a empresa deve sustentar

- Controlar o uso de modelos de IA de uso geral
- Conservar registos
- Documentar configurações
- Supervisionar resultados
- Gerir riscos
- Aplicar políticas
- Monitorizar incidências
- Gerar evidências

A CLOUDFRAMEWORK posiciona-se como uma **camada de governo e operação** para sistemas de IA empresariais, desenhada para ajudar as organizações a implementar IA de forma **rastreável, segura, auditável e alinhada** com as exigências do quadro regulatório europeu. A LAWORATORY aporta a camada jurídica que complementa essa operação com a avaliação de cumprimento exigível em cada caso.

Calendário de aplicação do Regulamento

O Regulamento (UE) 2024/1689 entrou em vigor a 1 de agosto de 2024 e aplica-se em fases. Já estão em aplicação as proibições (fevereiro de 2025) e as obrigações para modelos de uso geral (agosto de 2025). Em agosto de 2026 aplicam-se as obrigações para sistemas de alto risco. E a partir de agosto de 2027 completa-se o resto.

✓ Fev 2025
Práticas **proibidas** (Art. 5) em aplicação

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

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

2027
Sistemas regulados setorialmente e restantes obrigações

Novo calendário para sistemas de alto risco — Regulamento Omnibus Digital

O **Regulamento Omnibus Digital em matéria de Inteligência Artificial** adia a aplicação das normas para sistemas de alto risco, com o objetivo de permitir uma melhor preparação técnica:

2 DEZ 2027

Sistemas autónomos de alto risco

Biometria, infraestruturas, educação, emprego. Aplicáveis a partir de **2 de dezembro de 2027**.

2 AGO 2028

Sistemas integrados em produtos

Brinquedos, elevadores, dispositivos médicos. Aplicáveis a partir de **2 de agosto de 2028**.

Leitura comercial. A extensão de prazos pelo Omnibus é uma oportunidade de preparação, não uma desculpa para adiar o governo da IA. As organizações que arranquem agora estarão prontas — com evidência e com critério — quando aplicar. As que esperarem pelo último trimestre chegarão com a documentação incompleta e sem substrato técnico.

Próximo passo: uma sessão conjunta CLOUDFRAMEWORK + LAWORATORY

Uma conversa de 60 minutos com a sua direção, o seu CTO/CISO e o seu DPO/legal counsel. Mapeamos os sistemas de IA em uso ou desenvolvimento, classificamos o papel provável da sua organização para cada um e propomos — se fizer sentido — um diagnóstico formal técnico-jurídico. Sem compromisso.

cloudframework.io/cloudia

A CLOUDFRAMEWORK aporta capacidades técnicas (governo, rastreabilidade, controlo operacional). A LAWORATORY aporta avaliação jurídica e classificação regulatória. Ambas as camadas trabalham sobre o mesmo perímetro.