

FIONA

Governança de trajectòria per a agents d'IA.

FIONA és una capa externa i independent del model que avalua cada acció proposada amb l'estat acumulat de la tasca abans de l'execució.

NUCLI PRIVAT

CLIENT HTTPS RESTRINGIT

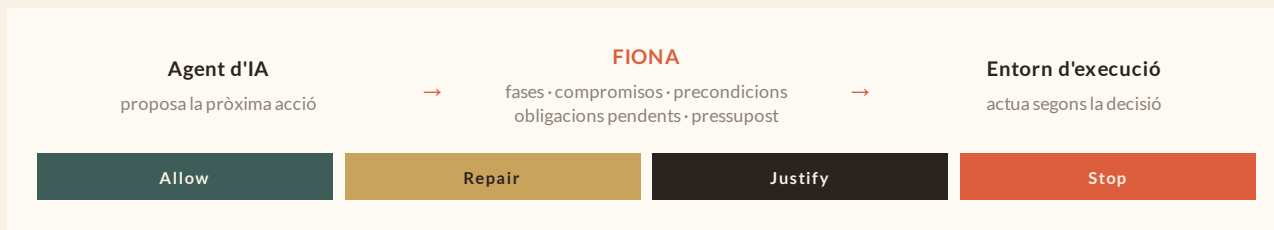
MODEL-AGNOSTIC

PROTOTIP INTERN

EL PROBLEMA QUE ABORDA

En tasques llargues, cada pas pot semblar raonable i, tanmateix, la seqüència pot perdre compromisos, repetir accions, esgotar pressupost o acabar sense un resultat utilitzable.

PATRO DE GOVERNANÇA



L'agent proposa una acció; FIONA l'avalua contra l'estat acumulat i retorna una de quatre decisions; l'entorn actua en conseqüència.

QUÈ EXISTEIX AVUI

- SDK privat **0.7.0b1** amb contractes d'acció i trajectòria.
- Client restringit **0.1.0b1** amb contractes tipats i transport HTTPS.
- **659 proves superades, 2 omeses**, més controls de tipus, build i empaquetat.

QUÈ ENCARA S'HA DE DEMOSTRAR

- Eficàcia en fluxos reals: completitud, qualitat, cost i no-interferència.
- Servei de producció: autenticació, aïllament entre clients, exportació de traça i rendiment.
- Validació independent i preparació per al desplegament.

LECTURA CORRECTA DE L'EVIDÈNCIA

Els resultats controlats mostren **potencial del mecanisme, no validació del producte**. Un pilot experimental sobre un benchmark extern va ser mixt i va revelar un defecte de control de termini. Això orienta la pròxima validació; **no prova superioritat general**.

Objectius de treball, no certificacions.

La taula següent **no declara compliment**. Situa on el mecanisme de FIONA *podria* contribuir a obligacions del [Reglament \(UE\) 2024/1689](#) i a riscos del [MIT AI Risk Repository](#), i indica l'estat real de cada hipòtesi. **Cap fila ha estat validada per un tercer independent.**

Calendari. El Reglament és aplicable amb caràcter general des del 2 d'agost de 2026. Les regles aplicables als sistemes d'alt risc de l'annex III ho seran des del 2 de desembre de 2027 i les relatives als sistemes integrats en productes regulats de l'annex I, des del 2 d'agost de 2028, segons el [Reglament \(UE\) 2026/1744](#).

Hipòtesis d'encaix normatiu i estat actual de validació de cadascuna.

OBLIGACIÓ O RISC	QUÈ EXIGEIX	HIPÒTESI D'ENCAIX DE FIONA	ESTAT ACTUAL
EU AI Act · Art. 9	Sistema de gestió de riscos documentat i continuat.	L'avaluació prèvia a l'acció <i>podria</i> aportar un punt de control documentat.	PER VALIDAR EN PILOT
EU AI Act · Art. 12	Registre automàtic d'esdeveniments reconstruïble.	La traça de decisions <i>podria</i> cobrir part del requisit.	FORMAT D'EXPORTACIÓ NO TANCAT
EU AI Act · Art. 14	Supervisió humana efectiva sobre decisions rellevants.	El mode Justify <i>podria</i> materialitzar el punt d'intervenció humana.	NO PROVAT AMB OPERADORS REALS
EU AI Act · Art. 15	Robustesa i ciberseguretat davant errors i manipulació.	Separar la decisió del prompt <i>podria</i> reduir alguns riscos de manipulació, però l'efecte net de seguretat i la nova superfície API i de servei encara s'han d'auditar.	SENSE AUDITORIA DE SEGURETAT
MIT AIRI · 7.3	Manca de capacitat o robustesa.	Validació determinista de precondicions sobre l'estat acumulat.	RESULTATS CONTROLATS, NO EN FLUX REAL
MIT AIRI · 7.4	Manca de transparència o interpretabilitat.	Regla i estat citables per decisió; depèn de la qualitat de l'ontologia del client.	DEPENDENT DE L'ONTOLOGIA

L'encaix normatiu real d'un sistema d'alt risc requereix avaluació de conformitat pels procediments que estableix el propi Reglament. FIONA pot aportar-hi evidència tècnica; no la substitueix ni la garanteix.

PRIMER PILOT PROPOSAT

Un agent. Un flux d'alt valor. Una línia base fixada abans de començar. Mesurem **completitud, qualitat, no-interferència, latència i cost** per arribar a una decisió tècnica **go/no-go** sobre el desplegament. Si els resultats no superen la línia base, el resultat correcte del pilot és *no desplegar*.

EXPLOREM EL CAS D'ÚS

pere@fiona-labs.com

fiona-labs.com

FIONA facilita governança i evidència tècnica. No és assessorament jurídic, certificació de compliment ni garantia de resultats. Les xifres de versió i de proves corresponen al codi intern a setembre de 2026 i no han estat auditades externament.