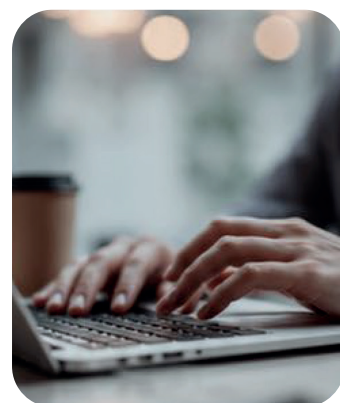


La nueva frontera europea de la IA B2B



Informe de Vigilancia estratégica

Activar la oportunidad

La nueva frontera europea de la IA B2B

Informe de Vigilancia estratégica

La nueva frontera europea de la IA B2B

Resumen ejecutivo 4

01 **Ecosistema científico, de innovación y talento** 8 *Del rigor investigador a la capacidad organizativa interna*

- **Ecosistema científico:** La huella global de la IA financiera, la velocidad de innovación y el mapa de competitividad institucional 9
- **Ecosistema innovador:** Los supernodos europeos de excelencia (París, DACH, Londres, España) y la transferencia Lab-to-Market 20
- **Transferencia, talento y gobernanza:** Nuevos perfiles híbridos (Analytics Translator), reestructuración operativa en Fusion Teams y retención estratégica 27

02 **Evolución tecnológica, modelos e infraestructura** 36 *De la IA de consumo a la eficiencia operativa y soberana*

- **De IA masiva a IA industrial:** La transición hacia IA industrial (SLMs), el análisis financiero Build vs. Buy y el control del Coste Total de Propiedad (TCO) 37
- **Arquitecturas de control y frontera agéntica:** El paradigma del RAG Soberano, redes Zero Egress, el salto al sistema 2 y la automatización mediante Agentes 45
- **Infraestructuras críticas y sostenibilidad:** Las Gigafactorías europeas, el Hub de supercomputación español (RES) y el imperativo de la Green AI 53

03 **Marco regulatorio y cumplimiento** 62 *El marco normativo como foso defensivo estratégico*

- **La regulación como producto:** El Compliance by Design y la ventaja competitiva frente a modelos no auditables 64
- **Gestión integrada y MRM:** La IA dentro del marco de Gestión de Riesgo de Modelo (MRM) para un escalado seguro 65
- **Caso de actualidad:** acceso a modelos frontera y soberanía operativa 66

Informe de Vigilancia Estratégica

La nueva frontera europea de la IA B2B

Resumen ejecutivo



El informe analiza el momento de madurez que atraviesa la inteligencia artificial (IA) fundacional en Europa y su impacto potencial en sectores críticos. La primera ola de adopción ha estado marcada por los grandes modelos generalistas y las aplicaciones de consumo, pero el debate estratégico empieza a concentrarse en usos más especializados, seguros y gobernables. Este cambio resulta especialmente relevante para los sectores críticos y regulados, donde cualquier despliegue tecnológico debe convivir con exigencias estrictas de trazabilidad, resiliencia, privacidad y control de riesgos.

Para la banca, la IA representa una oportunidad de transformación, aunque su valor dependerá de la capacidad para integrarla de forma ordenada en procesos reales de negocio. La prioridad debe estar en seleccionar los ámbitos donde puede generar eficiencia, mejorar la toma de decisiones, reforzar la resiliencia operativa y proteger la soberanía del dato. Esa priorización exige combinar ambición tecnológica con disciplina regulatoria, criterio económico y una arquitectura de gobierno preparada para escalar.

Del modelo generalista a la IA soberana en sectores críticos

La ventaja no está en el tamaño del modelo, sino en su integración segura en procesos críticos.

IA industrial, regulada y eficiente

El análisis confirma que Estados Unidos y China mantienen una ventaja estructural en inversión privada, modelos fundacionales de propósito general e infraestructura cloud. Frente a esa asimetría, Europa está configurando una tesis distinta, más orientada a la especialización vertical, la confianza regulatoria y el control de los datos industriales.

Esta posición encaja especialmente bien con la banca. En una actividad donde la confianza, la protección del dato y la gestión del riesgo forman parte del núcleo del negocio, la adopción de la IA no puede apoyarse en modelos opacos ni en arquitecturas que dejen información sensible fuera del perímetro de control. La prioridad debe ser una IA comprensible, auditable y gobernada desde el diseño, capaz de operar en entornos seguros y alineados con las exigencias regulatorias europeas.

El informe pone el foco en **tres ideas relevantes**. La primera es que los **modelos especializados** pueden ofrecer una relación mucho más favorable entre coste, latencia y control operativo. La segunda es que el **RAG soberano*** permite separar el motor de IA de la memoria corporativa, evitando que el conocimiento interno quede absorbido por proveedores externos. La tercera es que el **cumplimiento regulatorio**, lejos de ser solo una carga, puede convertirse en un estándar de calidad industrial y en una barrera competitiva frente a tecnologías menos transparentes o difíciles de auditar.



EE. UU. movilizó 109.000 millones de dólares de inversión privada en IA en 2024, frente a 19.420 millones en Europa. La respuesta europea no puede basarse en replicar esa escala, sino en combinar inversión selectiva, soberanía, confianza y especialización B2B.

* RAG soberano para conocimiento corporativo gobernado.

Principales tendencias

La lectura agregada del informe permite ordenar las tendencias en cinco grandes movimientos. No son líneas aisladas, sino piezas de una misma transición hacia una IA B2B más eficiente, más controlada y conectada con las exigencias regulatorias europeas.

1. La era del “One Model Fits All” empieza a agotarse

Los grandes modelos generalistas seguirán siendo relevantes, pero no son la respuesta óptima para todos los procesos empresariales regulados. En tareas recurrentes, documentales o altamente reguladas, los Small Language Models (SLMs) y modelos especializados ofrecen una alternativa más eficiente. Permiten reducir costes de inferencia, mejorar latencia y reforzar la ventaja competitiva mediante mayor dominio sobre datos, pesos y trazabilidad.

2. El RAG soberano se convierte en una arquitectura clave

La separación entre el modelo y la memoria corporativa será una decisión estructural. Una organización regulada no necesita reentrenar modelos con todo su conocimiento interno, sino conectar modelos controlados con repositorios documentales gobernados. Esta arquitectura permite usar IA generativa sin perder control sobre expedientes, políticas internas, documentación regulatoria o datos de cliente.

3. La regulación pasa de freno a ventaja competitiva

AI Act, DORA, RGPD y NIS2 elevan la exigencia operativa, pero también profesionalizan

el mercado. Las entidades capaces de demostrar trazabilidad, supervisión humana, control de riesgos, calidad de datos y resiliencia tecnológica estarán mejor posicionadas para escalar IA en procesos críticos. En banca, el cumplimiento riguroso puede actuar como sello de confianza.

4. El talento deja de ser un recurso de soporte y pasa a ser infraestructura

La ventaja competitiva no dependerá solo de contratar perfiles técnicos especializados. El informe apunta a una hibridación entre expertos de negocio, perfiles legales, equipos de riesgo, tecnólogos y redes científicas europeas. La IA diferencial en banca se construirá desde el conocimiento de dominio y negocio, no únicamente desde la ingeniería de modelos.

5. La madurez y el control deben orientar la priorización

El informe identifica como prioritarios los procesos de RegTech, fraude, AML, KYB, IA documental, datos sintéticos, gobernanza de modelos y agentes supervisados. Son ámbitos donde el Banco puede capturar eficiencia, reducir riesgo operativo y construir capacidades escalables sin asumir una dependencia excesiva de proveedores cerrados.

La pregunta directiva ya no es qué modelo usar. La pregunta relevante es qué procesos deben permanecer bajo control soberano, cuáles pueden apoyarse en proveedores externos y qué nivel de supervisión exige cada decisión automatizada.

Hoja de ruta ejecutiva

La estrategia que se desprende del análisis del informe no plantea una transformación masiva e indiferenciada. Propone una adopción progresiva, con prioridades distintas según horizonte temporal, nivel de madurez tecnológica y sensibilidad regulatoria en cada caso de uso.

1. Corto plazo, de 0 a 12 meses

RAG soberano, automatización documental y RegTech

La prioridad en la implementación debe centrarse en casos de impacto operativo inmediato. Asistentes documentales internos, búsqueda semántica gobernada, automatización de KYC/KYB, reducción de falsos positivos en AML y copilotos de cumplimiento ofrecen una combinación favorable de madurez, retorno y control. En esta fase conviene implantar el Sovereign Wrapper como capa transversal de accesos, auditoría, logs y control de salida de datos.

2. Medio plazo, de 1 a 3 años

Agentes supervisados y razonamiento trazable

La segunda fase debe avanzar hacia sistemas capaces de ayudar en procesos más complejos, no solo en la generación de texto. Estos agentes supervisados podrían apoyar tareas como el análisis crediticio, la gestión de alertas, la revisión de expedientes, la tesorería, la financiación comercial internacional (trade finance) o la prevención del fraude. Su uso debería mantenerse siempre bajo reglas claras de negocio, con validación humana (maker-checker) antes de cualquier decisión sensible y con registro completo de los pasos seguidos por el sistema. En paralelo,

Quantum AI, optimización y criptografía post-cuántica (PQC) deben mantenerse como línea de agenda técnica prioritaria, con vigilancia activa y preparación temprana de PQC.

3. Largo plazo, más de 3 años

IA híbrida, simulación financiera y tecnologías post-cuánticas

La tercera fase debe mantenerse en vigilancia activa y experimentación controlada. Incluye IA neuro-simbólica, gemelos digitales de liquidez, simulación de mercados, Quantum AI aplicada a optimización, distribución cuántica de claves y nuevas arquitecturas de seguridad. No son prioridades de despliegue masivo inmediato, pero sí líneas que pueden condicionar la ventaja competitiva futura.

Cierre ejecutivo

La banca no necesita competir en la carrera global por construir el modelo de IA más grande, sino en la capacidad de integrar una IA fiable en el núcleo de sus procesos financieros. La ventaja estará en combinar modelos eficientes, infraestructura soberana, gobernanza regulatoria, talento híbrido y una selección priorizada de casos de uso. La IA ganadora en sectores regulados será menos espectacular que la IA de consumo, pero más robusta, auditable y defendible.



La IA diferencial para sectores críticos será soberana por diseño, eficiente por arquitectura y regulada desde el origen.

01



Ecosistema científico, de innovación y talento



Activar la oportunidad

La nueva
frontera europea
de la IA B2B

Informe de Vigilancia estratégica



Ecosistema científico

La IA financiera se decide en la ciencia aplicada

- » **De un universo operativo de 10,3 millones de documentos sobre IA, el análisis aísla 326.000 publicaciones donde la IA converge con finanzas y banca.** Ese núcleo representa solo el 3,15% del total, pero concentra la señal estratégica relevante para el sector.
- » **La producción científica aplicada ha desbordado a la investigación teórica tradicional.** En 2024, la huella de adopción de IA en OpenAlex supera los 1,3 millones de documentos, aproximadamente cuatro veces más que la literatura fundamental recogida por los estándares académicos de referencia.
- » **La IA financiera no se está construyendo principalmente alrededor de chatbots, marketing o automatización de baja complejidad.** El peso científico se concentra en High-Trust AI, con algoritmos robustos, trazables y explicables para riesgo, fraude, solvencia y modelización matemática.
- » **La frontera de innovación ya no aparece primero en las revistas científicas tradicionales.** Los preprints funcionan como radar anticipado de tecnologías emergentes, mientras los journals consolidan conocimiento validado, auditable y más próximo a la industrialización bancaria.
- » **El menor volumen visible de FinTech y Digital Banking no apunta a una pérdida de relevancia, sino a una privatización de la I+D.** Parte del conocimiento crítico se desplaza hacia empresas, plataformas y silos corporativos protegidos.

Definición del universo analítico

Del océano IA al foco financiero

El análisis reduce la huella global de la IA hasta aislar la señal financiera aplicable, medible y comparable.

El bloque parte de **U0***, la huella global de IA en OpenAlex. La medición censal alcanza **15,6 millones de documentos**, mientras el corpus operativo consolidado suma **10,3 millones** para análisis de detalle entre **2022 y 2025**.

Sobre esa base se aplica un filtrado semántico específico para banca y finanzas. **U1** aísla la intersección entre IA, finanzas y banca, con **326.000 documentos**, equivalentes al **3,15%** de U0-operativo.

El zoom continúa con **U2**, centrado en aplicación vertical, con **50.748 documentos**. **U3** mide calidad e impacto con ventana madura de citación y **U4** reconstruye redes de colaboración geográfica.

El valor metodológico está en medir adopción financiera, no solo volumen académico.

De la huella global al núcleo financiero

U0 · IA global (operativo)

10,3M

OpenAlex 2022-2025



U1 · IA + Finanzas

326k

3,15% del total IA
Filtrado semántico contra un corpus sectorial (Banca & Finanzas)



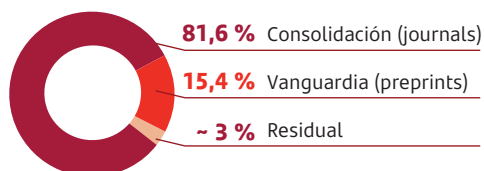
U2 · Aplicación vertical

50,7k

69,3% Riesgo + Seguros
excluye "General Finance"/"Banking"

Zoom cuantitativo: IA global → IA aplicada a finanzas (OpenAlex + AI Index)

Canales de comunicación (U1)



Traducción a banca: 3 palancas

- **Eficiencia (Opex)**
Industrializar Risk/Insurance (maduro)
- **Crecimiento (Alpha)**
Derivados y mercados (alta complejidad)
- **Confianza (cumplimiento)**
High-Trust AI (gobernanza + validación)

Señales de mercado (CAGR 2022-2024)

- **44,7 % Fraud Detection**
Explosión defensiva (urgencia)
- **22,7 % Derivates**
Renacimiento cuantitativo (banca inv)
- **~ 0 % Risk + Insurance**
Madurez: estándar/commodity

GenAI ≠ core bancario (señal bibliométrica)

En literatura especializada:
LSTM/RNN (2.610) > LLM (1.854)
→ foco en series temporales + robustez,
con capa semántica emergente

* "U" significa Universo analítico, es decir, el conjunto de documentos científicos usado para el análisis. U0 recoge la huella global de papers sobre IA; U1 filtra IA aplicada a finanzas y banca; U2 depura los aplicaciones verticales específicas; y U3 se usa para medir calidad e impacto con una ventana madura de citación.

La IA como motor de cálculo y solvencia

Algoritmia de alta confianza en riesgos y seguros

La producción científica sitúa la IA financiera en riesgos, seguros y capital regulatorio, por encima de usos conversacionales.

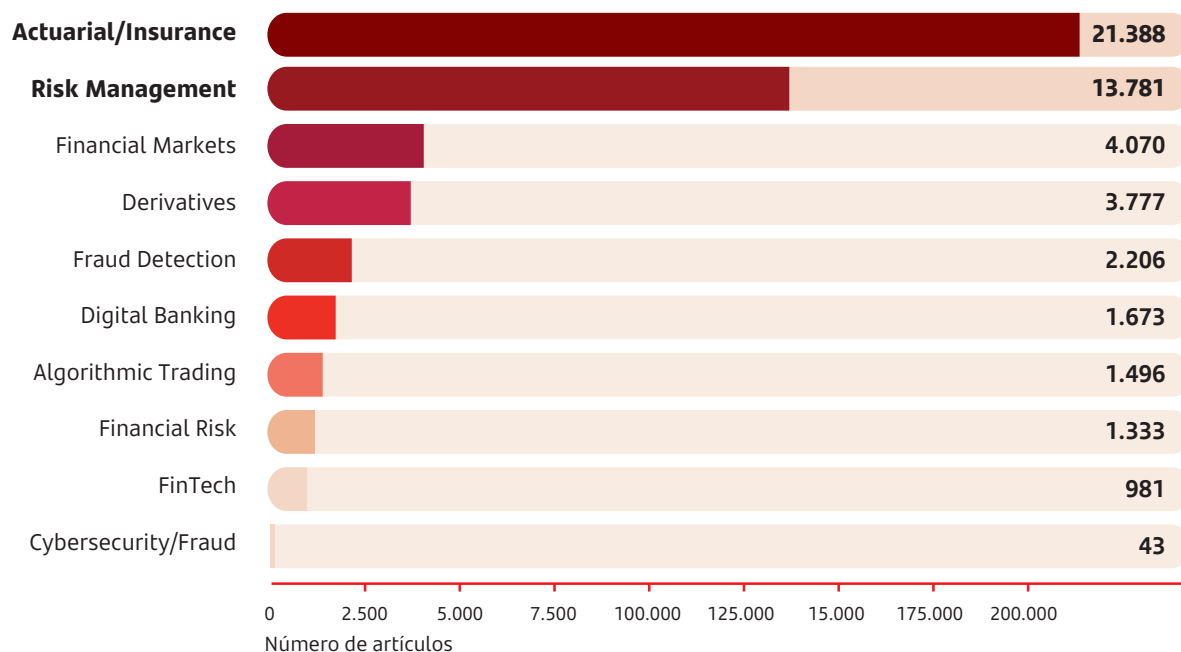
Al excluir la categoría general de banca y finanzas, el corpus **U2** revela la prioridad real de la investigación aplicada. **Actuarial/Insurance** suma **21.388 artículos** y **Risk Management** alcanza **13.781**.

Ambos dominios concentran el **69,3%** de la investigación especializada, confirmando que la IA actúa principalmente como un motor numérico de cálculo de capital y solvencia. Esta adopción prioriza la trazabilidad matemática y la auditoría exigida

por normativas estrictas como **Basilea o la Ley de IA europea**. Por ello, las menciones a la **IA explicable (XAI)** y el indicador de IA de alta confianza crecen de forma sostenida para garantizar la gestión del riesgo de los modelos y mitigar sesgos de género.

La gestión de riesgos y seguros adopta la IA como un estándar industrial auditable y maduro alejado de la sobreexpectación comercial.

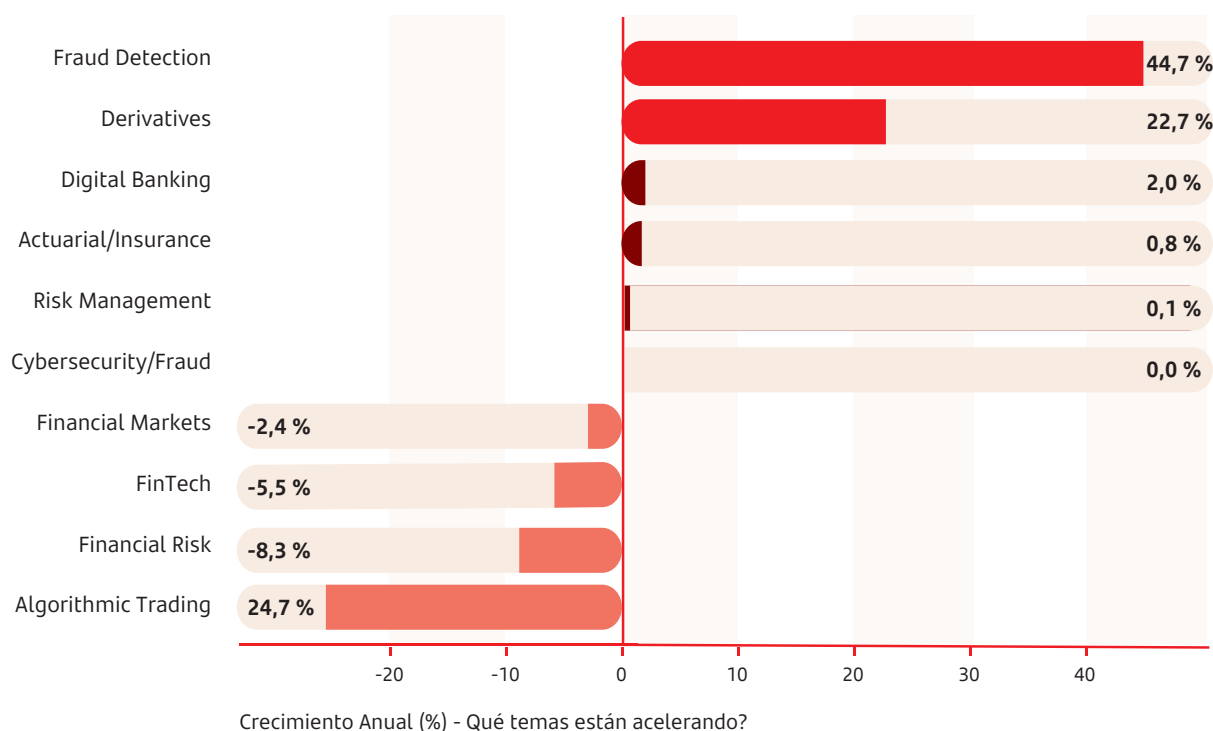
Detalle de aplicaciones específicas de IA en Finanzas (excluyendo general)



La innovación financiera avanza a dos velocidades

La velocidad de innovación en IA financiera no se distribuye de forma homogénea. La investigación se acelera en los ámbitos defensivos y de alta complejidad técnica, mientras algunas áreas más maduras o privatizadas pierden visibilidad en la producción científica abierta.

Velocidad de Innovación: Tasa de Crecimiento Anual (CAGR 2022-2024)



El cuadrante superior (alto crecimiento) señala las tendencias emergentes o de retorno ("Alpha"), mientras que el cuadrante inferior derecho (alto volumen, bajo crecimiento) identifica la tecnología "commodity" o estructural del sector.

El fuerte crecimiento de **Fraud Detection** y **Derivatives** apunta a dos prioridades claras: seguridad frente a nuevas amenazas y sofisticación cuantitativa.

En cambio, la caída de **Algorithmic Trading** y **FinTech** sugiere que parte de la innovación se está desplazando hacia entornos propietarios.

La doble velocidad de la innovación

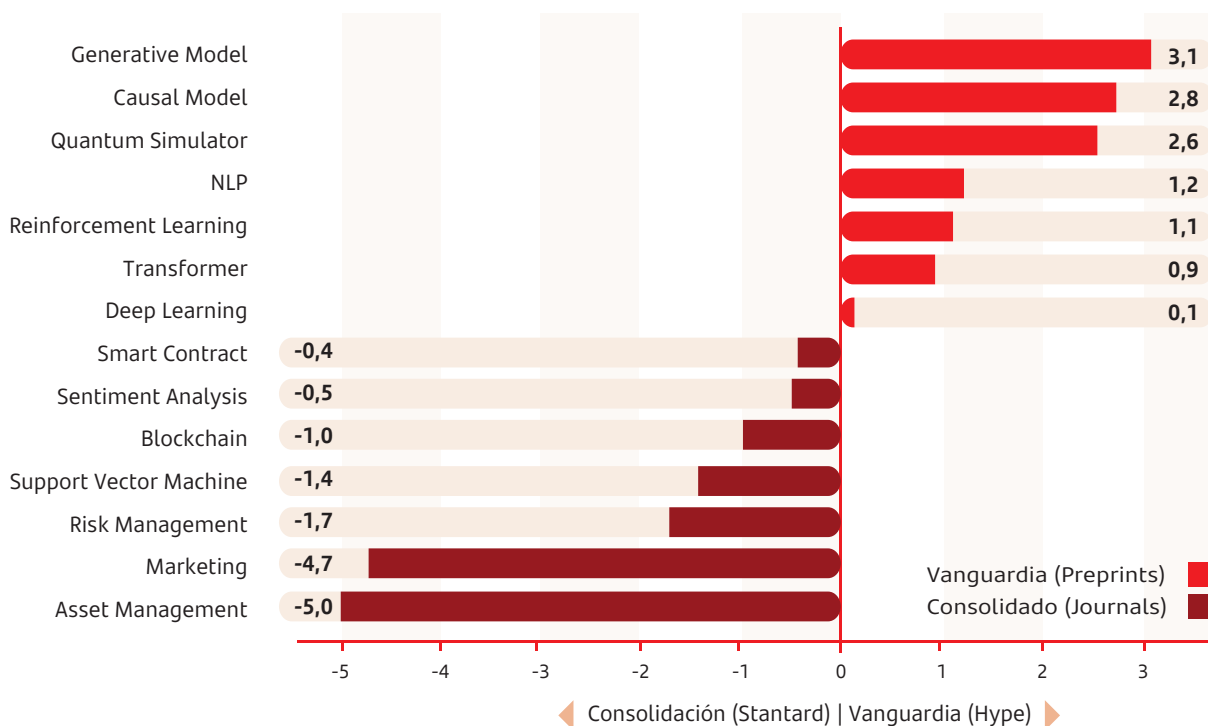
Validación científica y señal temprana

La IA financiera combina conocimiento auditable en journals y señal temprana en preprints, con tiempos de validación muy distintos.

La difusión de la innovación en IA aplicada a finanzas muestra una **asimetría crítica** en sus canales de comunicación científica. El **81,6%** del conocimiento se consolida en **revistas científicas tradicionales** o journals, las cuales aportan la validación por pares, la transparencia y la estabilidad metodológica exigidas por el supervisor bancario para modelos de producción.

Por el contrario, los **preprints** concentran el **15,4%** del corpus sectorial, superando ampliamente a las actas de conferencias, que en este corpus concreto apenas representan el 3%. Este ratio de cinco a uno sugiere que la **innovación financiera** busca autoría temprana, contraste rápido y menor exposición a ciclos editoriales largos.

Radar de innovación: Vanguardia (Preprints) vs. Consolidado (Journals)



Ignorar preprints puede ocultar señales tempranas, aunque no deben tomarse como evidencia definitiva.

El radar de anticipación tecnológica

Industrializar hoy, experimentar mañana

El cruce entre journals y preprints separa tecnologías listas para producción de líneas aún sujetas a validación.

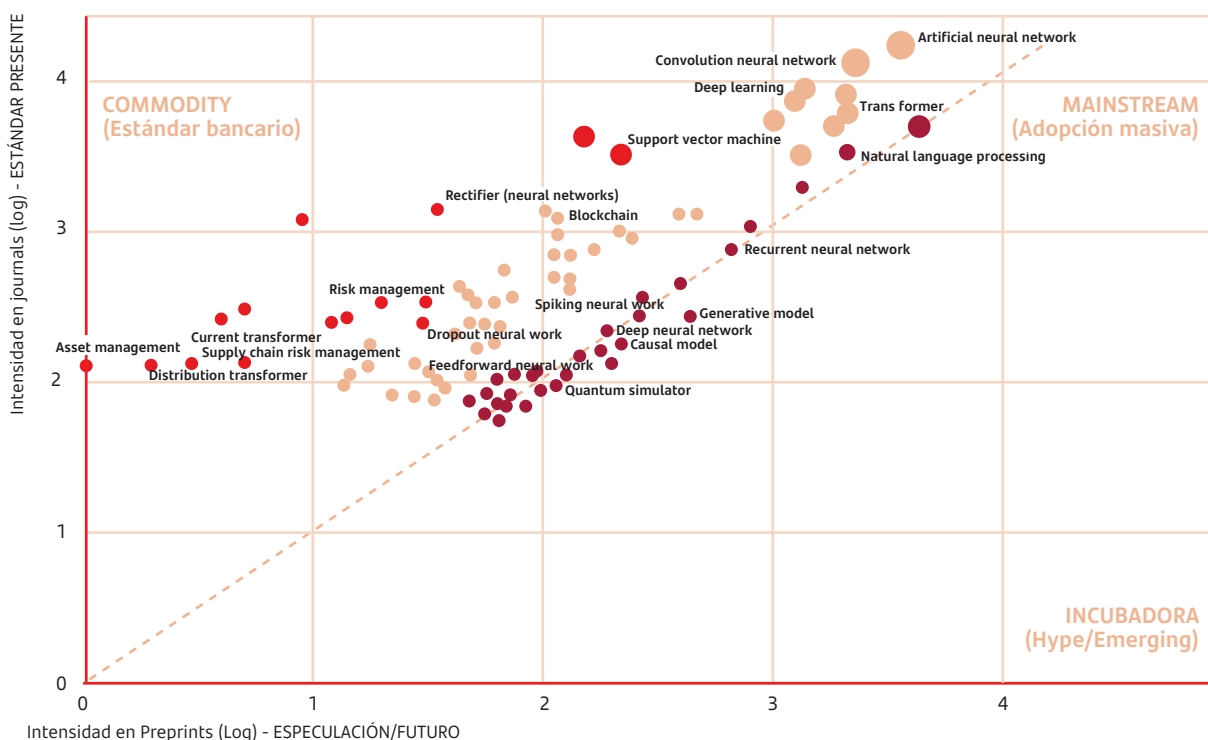
El radar distingue la zona de seguridad regulatoria. Allí aparecen **Risk Management, Credit Risk, Blockchain** y **Smart Contracts**, con mayor presencia en journals y uso más claro en eficiencia, auditoría y control.

En la zona emergente se sitúan **modelos generativos, IA causal** y **simulación cuántica**. Su mayor peso en preprints apunta a incertidumbre técnica, pero también a posibles ventajas tempranas.

Deep Learning queda en una posición intermedia. Ya opera como infraestructura transversal, conectando predicción, automatización documental y sistemas de decisión, sin sustituir los motores deterministas en procesos críticos.

La bibliometría ordena qué escalar, qué vigilar y dónde experimentar.

Matriz de Madurez. Del laboratorio (Preprints) a la Industria (Journals)



Clasificación de las tecnologías según su madurez de mercado.

La geopolítica del conocimiento

Asia gana escala científica

La producción mundial revela una especialización regional, con China dominando riesgos, Asia emergente liderando banca digital mientras EE.UU. retiene la soberanía disruptiva.

El mapa geopolítico muestra que **China** encabeza el volumen de investigación aplicada a finanzas. Su especialización se concentra en **Financial Risk**, con el **51,1%** de las publicaciones científicas a nivel mundial, y en **Algorithmic Trading**, con el **38,3%**.

El sudeste asiático domina la banca orientada a consumidor. **Indonesia** concentra el **48,6%** de la investigación en **Digital Banking** y el **30,6%** en **FinTech**.

India lidera **Fraud Detection** con el **43,6%**. **EE.UU.** conserva fortaleza defensiva en **Ciberseguridad** y **Actuarial/Insurance**,

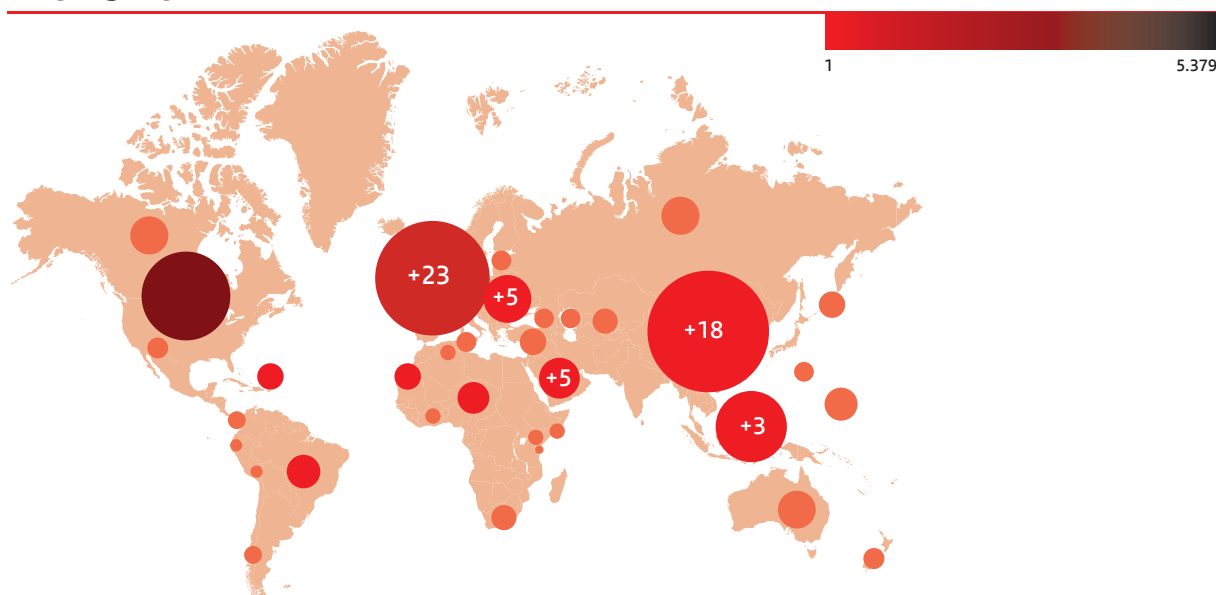
además de mayor capacidad industrial para modelos fundacionales.

Por el contrario, **Estados Unidos** sostiene una posición dominante basada en la creación de los grandes modelos fundacionales de frontera, respaldado por un ecosistema híbrido con fuerte inversión industrial.

Europa queda rezagada en volumen por país, evidenciando una preocupante fragmentación de la masa crítica investigadora.

China domina el cálculo financiero; Asia emergente domina la banca digital. EE.UU. monopoliza los modelos fundacionales de frontera y la inversión comercial.

Mapa geopolítico



El Efecto Boutique europeo

Europa gana por calidad

Europa no lidera por volumen, pero destaca en calidad, especialización y validación de tecnologías financieras críticas.

El análisis europeo utiliza **U3**, con datos de **2021** para evitar el sesgo de citación reciente. La matriz combina **RCA***, que mide especialización, y **Quality Ratio****, que mide impacto frente al promedio mundial.

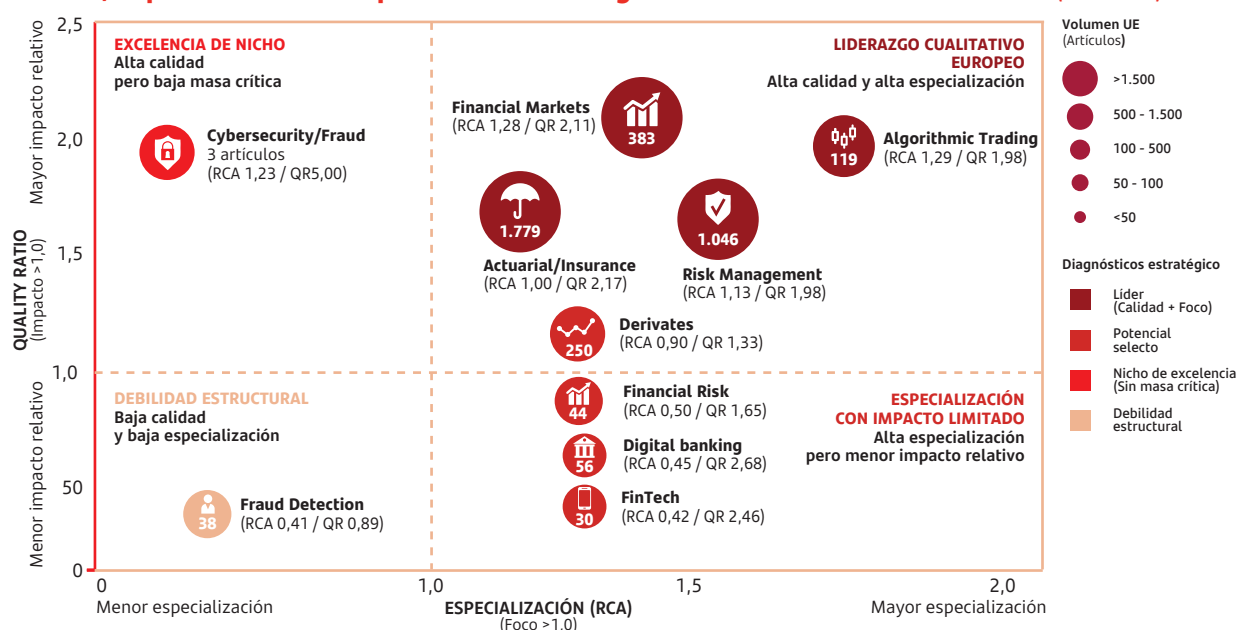
En **Algorithmic Trading**, Europa alcanza **RCA 1,29 y Quality Ratio 1,98**. En **Financial Markets**, registra **RCA 1,28 y Quality Ratio 2,11**, con una posición fuerte en mercados complejos.

La fortaleza se repite en **Risk Management** y **Actuarial/Insurance**, con ratios de calidad de **1,98 y 2,17**. Europa se posiciona así como una autoridad regulatoria global y garante técnico de la fase de validación, certificación y supervisión de sistemas financieros de alto riesgo normativo.

Europa compete mejor cuando la calidad pesa más que la escala.

Matriz de competitividad europea

Escala, especialización e impacto de la investigación en IA financiera. Universo: U3 (Año 2021)



Lectura: Europa no lidera por volumen, pero presenta ventajas cualitativas claras en verticales de alta complejidad científica y financiera. El "Efecto Boutique" europeo no se concentra en mercados, trading, riesgos y seguros.

* RCA, o ventaja comparativa revelada, mide si Europa está más especializada en un área que el promedio mundial. Un valor superior a 1 indica especialización relativa.

** Quality Ratio mide el impacto relativo de las publicaciones europeas frente al promedio mundial. Un valor superior a 1 indica mayor impacto científico comparado.

La privatización de la I+D

Privatización de la ciencia y brechas de colaboración

La innovación digital se desplaza a entornos propietarios.

La baja presencia de **FinTech** y **Digital Banking** en publicaciones científicas no implica menor innovación. Indica que una parte relevante de la I+D se desplaza hacia empresas, plataformas y laboratorios propietarios, donde el conocimiento se protege por ventaja competitiva y no siempre queda visible en la ciencia abierta.

En **Risk/Insurance**, la industria participa en el **6,6%** de los artículos, porque la validación pública refuerza aceptación supervisora. En **FinTech/Digital**, la participación empresarial cae al **2%**.

La brecha es más amplia en Europa.

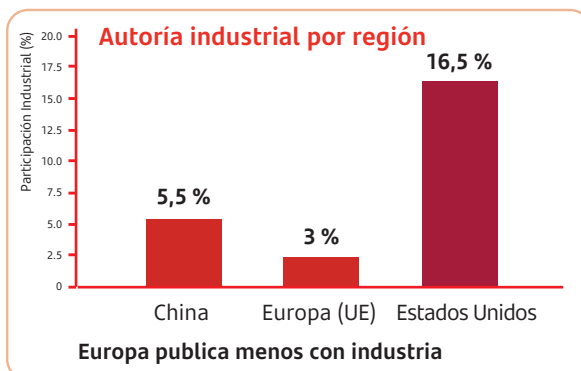
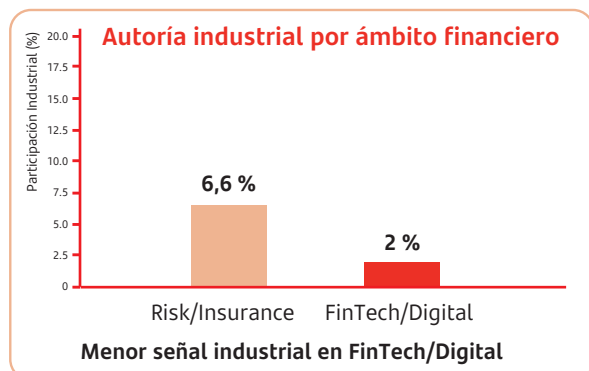
La producción científica procede en un **92%** de la academia y solo un **3%** de la industria, frente al **16,5%** industrial observado en EE.UU, lo que acelera la transferencia real al mercado financiero.

Asimismo, la ciberseguridad aparece aislada de la solvencia, configurando un peligroso punto ciego operativo frente a exigencias sistémicas como la regulación DORA o de resiliencia operativa.

El menor volumen de publicaciones refleja innovación propietaria, no ausencia de innovación.

Privatización de la ciencia y brechas de colaboración

La innovación digital se desplaza a entornos propietarios



Lectura: Una menor autoría industrial no implica menor innovación, sino menor presencia de esa innovación en publicaciones científicas abiertas.

Privatización de la I+D en FinTech.

% de papers con afiliación empresarial/Industrial (2025)
FinTech/Digital muestra menor señal industrial visible que Risk/Insurance.

Asimetría Institucional.

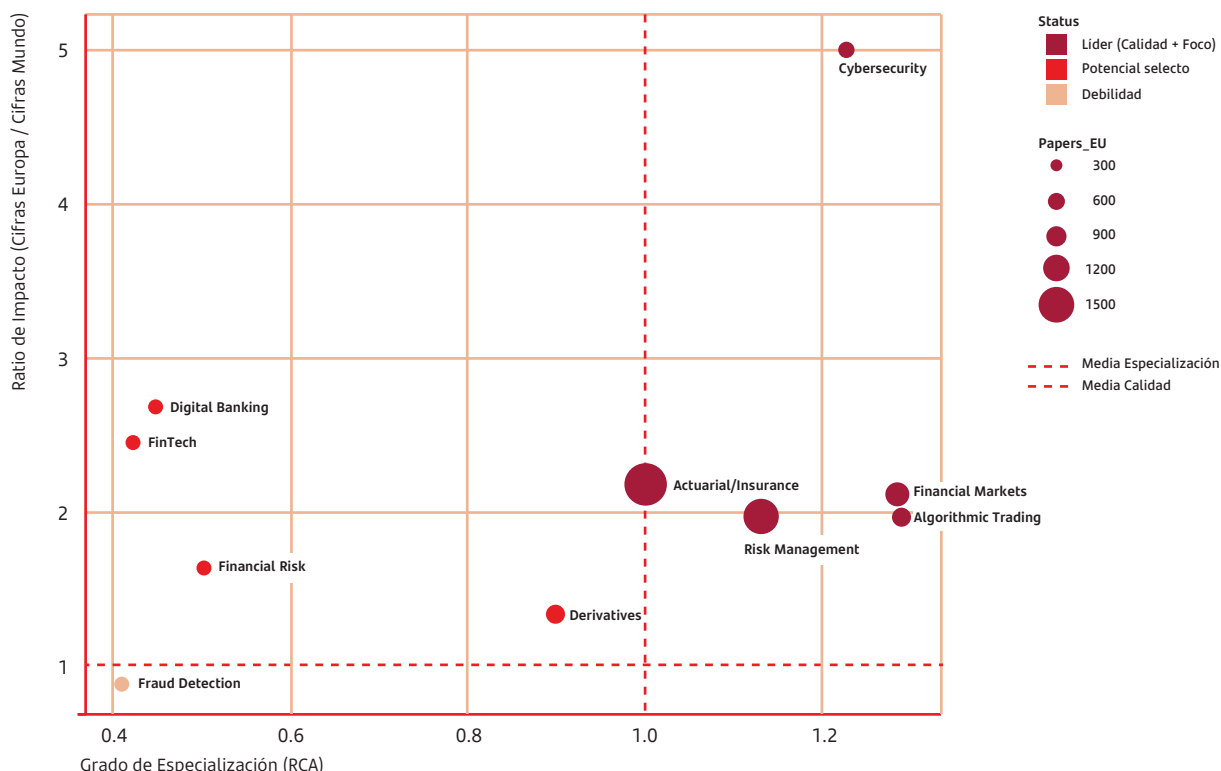
Composición de la autoría científica.
Fuente: Elaboración propia a partir de OpenAlex y AI Index Report (2025).

La ciberseguridad europea, excelencia sin escalas

La investigación europea en ciberseguridad financiera presenta una anomalía destacable.

El vector **Cybersecurity/Fraud** alcanza el mayor impacto relativo de la matriz, pero lo hace con una producción mínima, lo que revela una excelencia altamente concentrada y difícil de escalar.

Mapa de competencia Europea 2021: Especialización vs. Calidad Real



Se puede observar el punto azul oscuro en la esquina superior derecha (Ciberseguridad). Su posición aislada revela excelencia concentrada, pero difícil de escalar operativamente.

El resultado apunta a una vulnerabilidad sistémica. Europa cuenta con grupos de investigación capaces de producir ciencia de impacto mundial, pero la baja masa crítica limita su capacidad para cubrir el perímetro real de amenazas financieras, operativas y digitales.

El mapa de competitividad nacional

España articula ciencia aplicada

España combina masa crítica y volumen científico en universidad, especialización regulatoria, conexión latinoamericana y un CSIC orientado a IA simbólica y lógica.

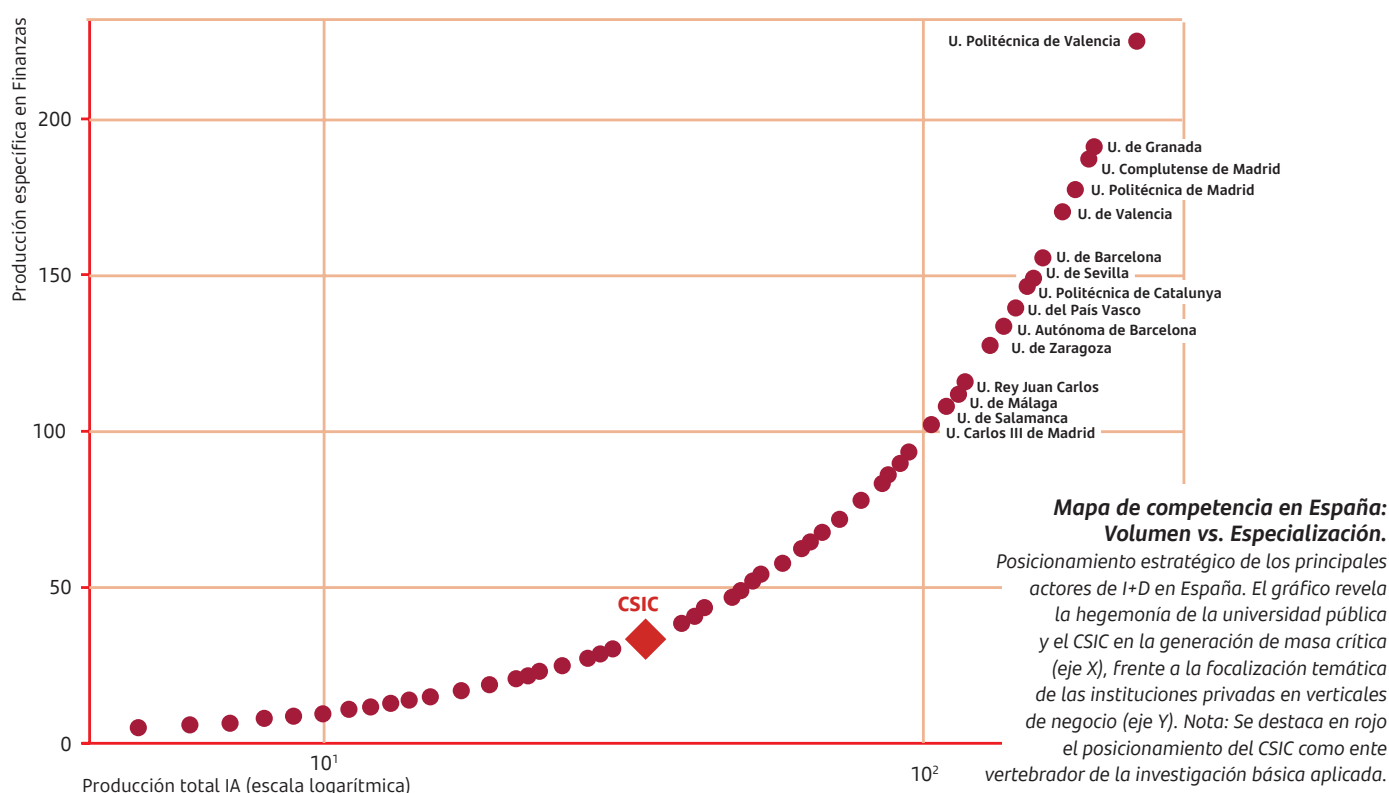
Las universidades públicas lideran de forma clara la generación de masa crítica y volumen bruto de producción científica, centrando su especialización en aprendizaje automático y modelos de deep learning avanzado. El mapa nacional sitúa a **UPV, UGR** y **UCM** entre los motores de producción en IA financiera. España muestra una fuerte penetración en espacios híbridos entre tecnología, economía, regulación y mercados.

El análisis temático detecta un peso relevante de **Law, Regulation** y microestructura de mercados. Esta señal sugiere posición natural en **RegTech**, supervisión algorítmica y lectura jurídica de la IA financiera.

Por el contrario, el **CSIC** actúa como el pilar vertebrador de la **IA simbólica**, el diseño de sistemas multiagente y el razonamiento lógico formal. Esta especialización metodológica es indispensable para el cumplimiento normativo financiero, aportando la interpretabilidad matemática, ética y auditoría necesarias exigidas para certificar modelos de alto riesgo bajo la nueva regulación de la UE.

La universidad aporta escala; el CSIC aporta lógica, interpretabilidad y profundidad técnica.

Mapa de competencia en España: Volumen vs. Especialización



Ecosistema de innovación

Supernodos europeos de excelencia

- » **Europa no opera como un ecosistema homogéneo de IA, sino como una red policéntrica de nodos especializados.** Cada hub o supernodo aporta una capacidad distinta para el sector financiero: eficiencia algorítmica, confianza industrial, razonamiento agéntico o validación regulatoria.
- » **El análisis cambia de escala.** Tras medir la producción científica, el foco se desplaza hacia la transferencia tecnológica, las spin-offs, los laboratorios frontera y los proveedores B2B capaces de convertir conocimiento en producto B2B regulado.
- » **París** aporta modelos **frugales y soberanía** de ejecución. El nodo **Alemania-Suiza** (DACH) conecta **IA industrial**, explicabilidad y seguridad crítica. **Londres** lidera razonamiento avanzado e **IA agéntica**. **España** refuerza **cómputo soberano, supervisión y confianza**.
- » **Las spin-offs universitarias son el puente entre excelencia científica y ventaja competitiva.** Permiten retener propiedad intelectual, acelerar proyectos piloto y nuevos casos de uso, atraer talento especializado y testar soluciones antes de que el mercado las consolide.
- » **Para una entidad financiera, este radar no es una cartografía académica, sino una herramienta de decisión** para priorizar alianzas, proyectos piloto y vigilancia estratégica en los ámbitos donde la IA europea puede aportar soberanía, eficiencia y cumplimiento.

Nodo París

El epicentro matemático y la arquitectura de modelos

El nodo francés combina tradición matemática, modelos frugales y pesos abiertos para reducir dependencia tecnológica y costes de inferencia.

París se consolida como el epicentro europeo de la eficiencia algorítmica. Su ventaja no está en competir por fuerza bruta computacional, sino en desacoplar rendimiento y tamaño mediante **SLMs**, arquitecturas **MoE** y curación avanzada de datos.

Los modelos **MoE**, o *mixture of experts*, activan solo una parte especializada del modelo en cada tarea. Esto permite mejorar eficiencia, coste de inferencia y rendimiento sin multiplicar de forma lineal el consumo computacional.

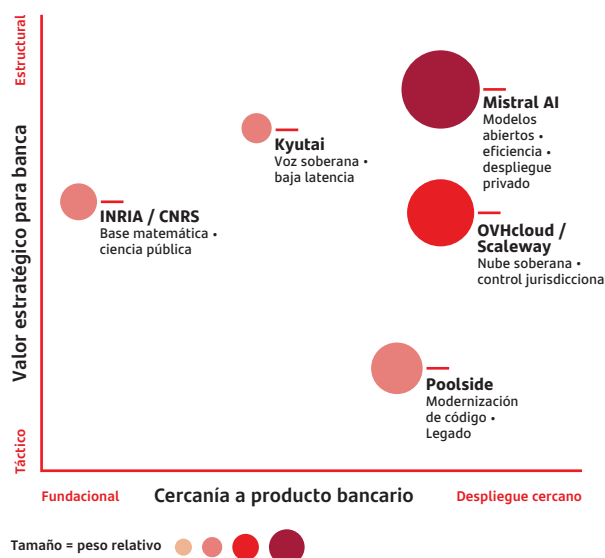
Mistral AI representa la capa empresarial del nodo, con modelos de pesos abiertos y opciones de despliegue controlado en entornos privados. Para sectores regulados como la banca, esto habilita soberanía de datos, reducción de exposición a nubes externas y control operativo sobre modelos sensibles.

Kyutai, junto con **INRIA** y **CNRS**, refuerza la dimensión de ciencia abierta, voz soberana, privacidad biométrica y transferencia matemática hacia aplicaciones bancarias de alto control. El SODA valida **Scikit-learn** en fraude y riesgos con socios como **AXA** y **Allianz**.

Nodo París

Mapa de capacidades del nodo

París articula un ecosistema de IA soberana apoyado en ciencia pública, modelos frugales y despliegue privado para entornos regulados.



Lectura: posicionamiento cualitativo del ecosistema París para banca sistémica.

Claves del modelo



La ventaja diferencial está en la eficiencia algorítmica.



Los pesos abiertos reducen dependencia tecnológica.



La nube soberana refuerza control y privacidad

París permite escalar IA bancaria sin hipotecar soberanía, margen operativo ni secreto bancario.

Nodo Múnich y eje DACH

IA industrial, soberanía y confianza técnica

Alemania y Suiza aportan IA industrial, explicabilidad, seguridad crítica y tecnologías post-cuánticas aplicables a banca corporativa.

El eje **Múnich-Zúrich-Stuttgart** actúa como el gran nodo europeo de IA industrial. Su foco es B2B, trazable y robusto, con capacidad para llevar modelos a procesos físicos, cadenas de suministro y activos productivos financiados.

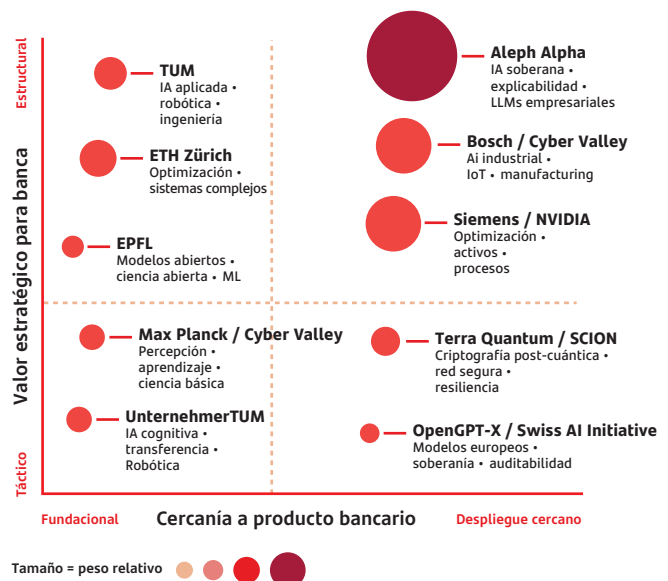
La primera capa es científica. **TUM, ETH Zürich, EPFL y Max Planck** aportan excelencia en causalidad, grafos, aprendizaje robusto y sistemas confiables. La segunda capa es de transferencia, con **UnternehmerTUM y Cyber Valley** como puentes entre investigación avanzada, industria y emprendimiento tecnológico.

La tercera capa refuerza la soberanía y la confianza. **Aleph Alpha, OpenGPT-X** y la **Swiss AI Initiative** impulsan modelos explicables y controlables, mientras **Terra Quantum** añade resiliencia, seguridad crítica y capacidades post-cuánticas. Para banca, el valor diferencial está en convertir activos físicos y procesos industriales en datos verificables para crédito corporativo, seguros y pagos.

Nodo DACH

Mapa de capacidades del nodo

DACH convierte la IA en infraestructura confiable para banca e industria, combinando explicabilidad, seguridad crítica y transferencia aplicada al tejido productivo.



Lectura: posicionamiento cualitativo del ecosistema DACH para banca sistémica.

Claves del nodo



La fortaleza diferencial está en la IA industrial confiable.



La explicabilidad y la soberanía refuerzan el control.



La seguridad post-cuántica amplía la resiliencia bancaria.

DACH permite evaluar activos industriales con datos operativos, no solo con balances históricos.

Nodo Londres

La convergencia entre Bio-Fintech y agéntica

El nodo británico concentra razonamiento avanzado, sistemas multiagente, grafos financieros y validación comercial en fintech B2B.

Londres combina la City, **Google DeepMind**, el **Alan Turing Institute** y el triángulo **Oxford-UCL-Cambridge**. Su ventaja no está solo en generar modelos, sino en trasladar ciencia de sistemas complejos hacia mercados, riesgo, cumplimiento y decisión financiera.

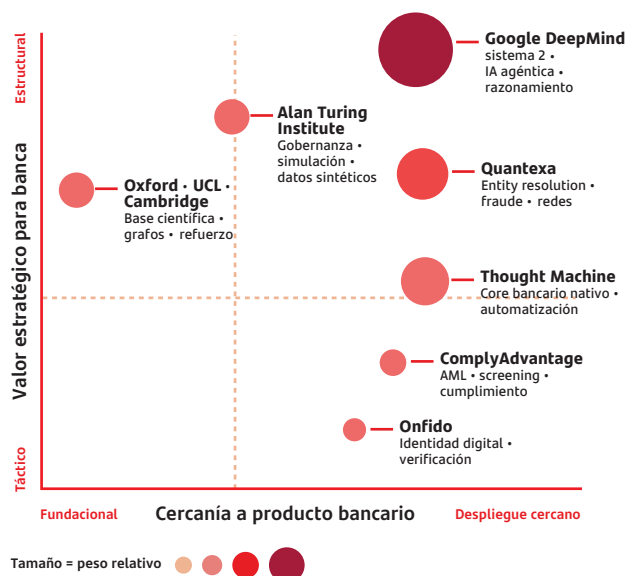
El nodo concentra capacidades de **sistema 2**, aprendizaje por refuerzo, redes de grafos, datos sintéticos e **IA agéntica**. DeepMind acelera esta agenda con enfoques como **Finance-Agent**, mientras Isomorphic Labs proyecta la bio-IA hacia la modelización de riesgos sistémicos complejos.

El **Alan Turing Institute** aporta gobernanza ética, simulación de mercados y datos sintéticos junto a actores como **HSBC** y la **FCA**. En paralelo, fintechs B2B como **Thought Machine**, **Quantexa**, **OakNorth**, **Onfido** y **ComplyAdvantage** validan estas arquitecturas en procesos financieros reales.

Nodo Londres

Mapa de capacidades del nodo

Londres combina ciencia de sistema 2, IA agéntica y fintech B2B para trasladar modelos complejos a riesgo, cumplimiento y modernización bancaria.



Lectura: posicionamiento cualitativo del ecosistema Londres para banca sistémica.

Claves del nodo



La ventaja diferencial está en el razonamiento avanzado.



La fintech B2B acelera la aplicación financiera.



Gobernanza y datos sintéticos refuerzan el control.

Londres transforma la IA de análisis en IA de ejecución controlada.

Nodo España

El pilar de infraestructura y confianza

España aporta infraestructura soberana, supervisión temprana y ética aplicada para escalar IA bancaria bajo seguridad jurídica.

España no compite principalmente por grandes modelos comerciales. Su posición diferencial está en cómputo soberano, validación regulatoria y confianza.

MareNostrum 5, el **BSC-CNS** y la **AI Factory** ofrecen capacidad pública para entrenar y auditar modelos sensibles.

La **AESIA** añade un activo regulatorio singular. Su sandbox permite probar modelos de scoring, fraude o decisión automatizada antes de su despliegue, reduciendo contingencias bajo el **AI Act**.

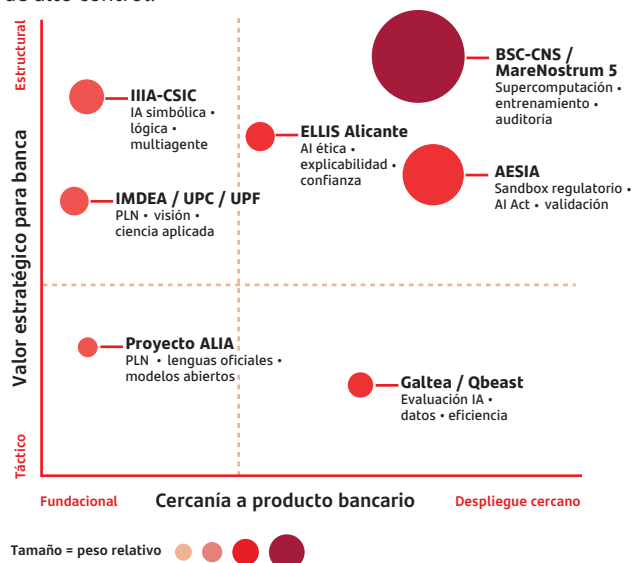
La red **ELLIS Alicante**, junto con **IMDEA**, **UPC**, **UPF** e **IIIA-CSIC**, completa el nodo con ética algorítmica, privacidad, IA explicable, PLN y sistemas autónomos.

Las spin-offs **Galtea** y **Qbeast** conectan esa base científica con herramientas aplicables a evaluación de modelos, control de sesgos y eficiencia en la gestión de datos.

Nodo España

Mapa de capacidades del nodo

España articula un ecosistema de IA confiable en supercomputación soberana, validación regulatoria y redes abiertas de investigación para entornos bancarios de alto control.



Lectura: posicionamiento cualitativo del ecosistema España para banca sistémica.

Claves del nodo

- La infraestructura soberana acelera entrenamiento y auditoría.
- La validación regulatoria reduce riesgo de despliegue.
- La IA ética y simbólica refuerza la confianza.

España puede ser el entorno europeo de prueba para IA financiera de alto riesgo.

El salto del laboratorio al mercado

Del radar a la adopción B2B regulada

El ecosistema europeo de startups y spin-offs transforma investigación, datos e infraestructura en capacidades aplicables a los servicios financieros y sectores regulados.

La innovación europea en IA no se concentra en una única tecnología ni en un único actor. El radar muestra un ecosistema compuesto por capacidades complementarias que responden a desafíos concretos del sector financiero: cumplimiento normativo, prevención del fraude, gestión del riesgo, automatización documental, privacidad de datos, modernización tecnológica y soberanía digital.

Para convertir este mapa tecnológico en decisiones operativas, el análisis se organiza mediante una matriz de priorización que cruza el horizonte de adopción bancaria con el impacto estructural sobre la arquitectura de la entidad. Esta lectura permite diferenciar soluciones de aplicación inmediata, capacidades escalables mediante colaboración, apuestas estratégicas de medio plazo y tecnologías que requieren seguimiento antes de alcanzar madurez suficiente.

Las áreas con mayor proximidad a adopción se concentran en RegTech, AML, KYC, fraude e inteligencia documental, donde ya existen soluciones capaces de reducir costes operativos, acelerar procesos y reforzar el cumplimiento regulatorio.

Más allá de la eficiencia operativa, el radar identifica una segunda capa de tecnologías habilitadoras centradas en privacidad, datos sintéticos, aprendizaje federado y gobernanza de modelos. Estas capacidades permiten desarrollar IA sobre información sensible sin comprometer confidencialidad, secreto bancario o requisitos regulatorios.

La dimensión documental constituye otro de los principales vectores de retorno. Contratos, expedientes, informes regulatorios y documentación financiera siguen concentrando una parte significativa de la carga operativa de las entidades. Las nuevas soluciones de procesamiento documental, grafos semánticos y razonamiento sobre conocimiento permiten transformar información no estructurada en activos gobernables y reutilizables.

Finalmente, el ecosistema incorpora apuestas de mayor alcance vinculadas a modelos fundacionales, infraestructura avanzada, ciberseguridad, computación cuántica y plataformas financieras de nueva generación. Aunque su adopción será progresiva, estas capacidades pueden redefinir la arquitectura tecnológica de la banca durante la próxima década.

La ventaja competitiva no vendrá de incorporar más IA, sino de desplegar IA gobernada, segura y alineada con la arquitectura regulatoria de la entidad.

Radar europeo de IA B2B para servicios financieros

Madurez tecnológica, horizonte de adopción e impacto estratégico para empresas reguladas

Matriz de madurez, impacto estratégico y capacidades tecnológicas del ecosistema innovador



Lectura: El ecosistema europeo combina soluciones de adopción inmediata en cumplimiento, fraude y documentación con apuestas estratégicas en datos, GenAI, cuántica e infraestructura.



Patrón dominante: la adopción cercana se concentra en procesos regulados y operativos. Las capacidades más estructurales exigen colaboración segura y construcción de plataforma.

Tipologías Tecnológicas



RegTech / AML / KYC / fraude



Riesgo / scoring / analítica financiera



Banca abierta / core / plataformas financieras



IA fundacional / GenAI / automatización



Privacidad / datos sintéticos / aprendizaje federado



IA documental / PLN / inteligencia textual



Ciberseguridad / identidad digital



Cuántica / infraestructura avanzada



NOTA: Empresas seleccionadas representativas del ecosistema europeo de IA para servicios financieros.

Horizontes: H1 = 0-12 meses | H2 = 12-24 meses | H3 = 24-36 meses | PoC = Prueba de concepto

Transferencia, talento y gobernanza

De la innovación externa a la capacidad interna

- » La ventaja no está solo en detectar ciencia, startups, spin-offs o nodos europeos de excelencia. **El factor diferencial es construir una arquitectura interna capaz de detectar y absorber ese conocimiento, convertirlo en pilotos útiles y escalarlo con control dentro de una entidad regulada.**
- » **La transferencia Lab to Market exige elegir el vehículo adecuado según el reto.** Co-ubicación industrial, venture building científico, spin-offs soberanas, licencias, consorcios B2B y coinversión no responden al mismo problema ni generan el mismo tipo de ventaja.
- » **La batalla del talento no se resuelve solo contratando perfiles técnicos en el mercado.** La banca necesita combinar captación externa, formación interna, alianzas científicas y retención académica para crear perfiles híbridos capaces de operar IA en entornos complejos.
- » **El perfil crítico es el profesional que traduce entre negocio, datos, tecnología y control.** Sin el perfil del Analytics Translator, equipos integrados y roles específicos de gobierno, la IA puede funcionar en piloto, pero bloquearse al pasar a producción.
- » **El AI Act convierte la gobernanza en una capacidad operativa.** La entidad deberá clasificar sistemas, asignar responsabilidades, documentar modelos, validar cambios, supervisar el comportamiento y conservar evidencias durante todo el ciclo de vida.

Modelos de transferencia a mercado

Transferir ciencia exige arquitectura

La ventaja no está solo en detectar innovación, sino en absorberla mediante vehículos estables de transferencia, propiedad intelectual y escalado B2B.

Europa ha desarrollado distintas arquitecturas para convertir ciencia, talento y propiedad intelectual en soluciones empresariales. Una primera vía son los **ecosistemas de co-ubicación corporativa**, es decir, entornos donde universidades, centros científicos, laboratorios industriales y grandes empresas trabajan cerca desde fases tempranas. **Cyber Valley** y **UnternehmerTUM** son dos ejemplos de este modelo.

Una segunda vía son los **programas de maduración y venture building científico**. No son una empresa concreta, sino instrumentos creados por centros de investigación para transformar una tecnología prometedora en una compañía, licencia o producto invertible. **INRIA Startup Studio**, **Fraunhofer AHEAD**, **Helmholtz Enterprise** y **VTT LaunchPad** operan en esta lógica, reduciendo el riesgo entre descubrimiento, equipo, propiedad intelectual y salida comercial.

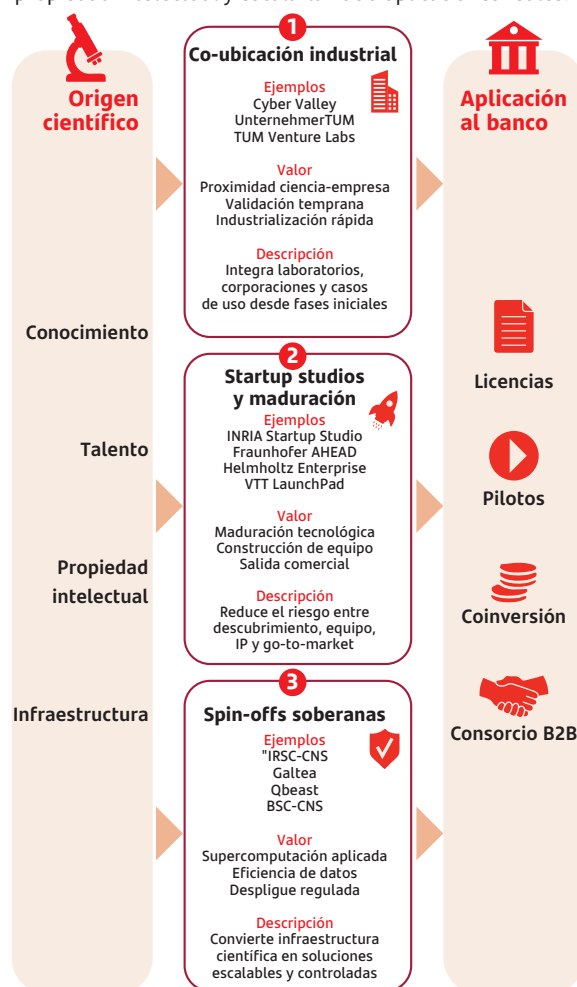
Una tercera vía son las **spin-offs nacidas de infraestructuras científicas soberanas**, como el **BSC-CNS**, con casos como **Galtea** o **Qbeast**. Para la banca, el interés está en elegir el canal adecuado según el reto, ya sea explorar IA de frontera, licenciar tecnología madura, coinvertir o participar en consorcios de aprendizaje federado.

La transferencia eficaz no compra innovación, construye canales para absorberla.

Modelos de transferencia

Tres vías para capturar ciencia, talento e IP

Europa convierte investigación en soluciones empresariales mediante arquitecturas estables de transferencia. Para banca, el reto no es detectar innovación, sino absorberla, proteger su propiedad intelectual y escalarla hacia aplicaciones reales.



Lectura: la transferencia eficaz no compra innovación, construye canales para absorberla.

Claves del modelo



Cada reto exige un vehículo de transferencia distinto.



La IP y el talento deben capturarse antes del escalado.



El valor bancario surge al conectar ciencia con despliegue regulado.

La batalla del talento

El talento limita la escala

La escasez de perfiles técnicos e híbridos convierte la industrialización de IA en una restricción estructural para la banca.

España muestra una paradoja relevante. Existe una base digital generalista relativamente sólida, pero la masa crítica avanzada sigue siendo insuficiente para desplegar **IA**, datos, arquitectura y operación en entornos complejos.

La brecha se vuelve visible dentro de las empresas. Se observa una baja presencia de especialistas TIC y una penetración todavía menor de especialistas en IA, lo que limita el salto desde pruebas piloto hacia capacidades estables.

El problema no se corrige solo contratando fuera. La competencia europea por los mismos perfiles, la concentración territorial del talento y la fuga hacia las Big Tech obligan a combinar captación, retención, formación interna y colaboración con redes científicas.

La brecha crítica no es digitalizar, sino sostener IA avanzada en producción.

Embudo de restricciones de talento

Cómo se estrecha la oferta efectiva de perfiles TIC e IA para banca e industria



Resultado



Dificultad para industrializar IA avanzada en banca

La restricción no es solo captar talento, sino sostenerlo, combinarlo y escalarlo

Claves



La escasez no empieza en la contratación, empieza en la base disponible.



La formación avanzada no crece al ritmo de la demanda empresarial.



Sin perfiles híbridos, la IA se queda en piloto y no escala a producción.

El perfil crítico: Analytics Translator

El traductor convierte IA en valor

El perfil de **Analytics Translator*** conecta negocio, tecnología y control para que los casos de IA sean viables, medibles y desplegables.

En la industrialización de la IA bancaria, el perfil más crítico no siempre es el científico de datos más especializado, sino el profesional capaz de traducir entre áreas que normalmente trabajan con lenguajes distintos. Este rol se conoce habitualmente como **Analytics Translator** o **traductor de valor operativo**.

Su función consiste en conectar las necesidades del negocio con las posibilidades reales de los datos, los modelos y la arquitectura tecnológica. En banca, además, debe incorporar desde el inicio restricciones de **riesgo, cumplimiento, auditoría, privacidad y trazabilidad**, porque una solución de IA no puede evaluarse solo por su precisión técnica.

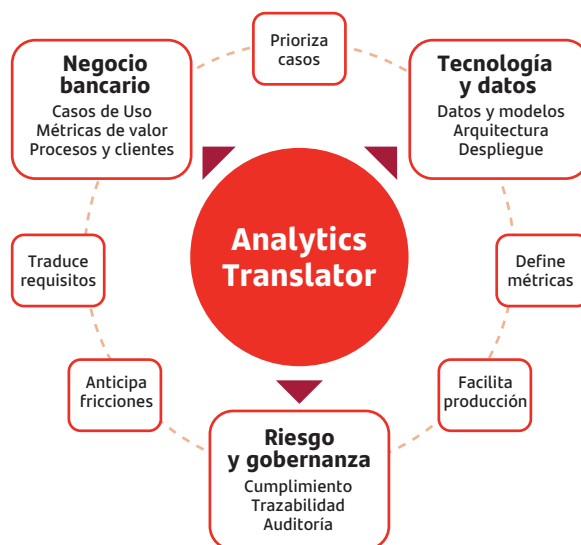
Por eso, un **experto de negocio con competencias avanzadas en IA** puede generar más valor inmediato que un perfil técnico sin contexto regulatorio. Su aportación está en priorizar casos, definir métricas, anticipar fricciones y convertir una prueba funcional en una solución gobernada, operable y defendible.

Sin traducción operativa, la IA funciona en piloto y se bloquea en producción.

Analytics Translator

Perfil puente entre tres dominios

Conecta negocio, tecnología y control para convertir un caso de IA en una solución bancaria viable, desplegable y gobernada.



Lectura: el valor del perfil está en traducir necesidades operativas, capacidades analíticas y exigencias de control en decisiones desplegables.

Claves



No sustituye el negocio ni el dato; conecta ambos mundos.



Integra valor, viabilidad y exigencia regulatoria.



Evita que la IA se quede en piloto y acelera su paso a producción.

* Analytics Translator es el perfil puente que convierte necesidades de negocio en casos de IA viables, medibles y gobernables.

Del silo funcional al equipo de IA

Equipos integrados para industrializar IA

Los pilotos no escalan cuando negocio, tecnología, riesgo y cumplimiento intervienen de forma secuencial. La producción exige equipos compartidos desde el diseño.

El modelo organizativo tradicional separa las funciones por especialidad. Negocio define la necesidad, tecnología construye la solución, riesgo y cumplimiento revisan después, y operaciones recibe el sistema al final. Esta secuencia puede funcionar en proyectos convencionales, pero en IA suele generar bloqueos, retrabajos y pilotos que no llegan a producción.

La alternativa son **equipos multidisciplinares de IA**, también conocidos como **Fusion Teams**. No son comités de coordinación, sino grupos de trabajo con perfiles de negocio, datos, arquitectura, riesgo, cumplimiento, seguridad, privacidad y operación participando desde el inicio del caso.

Su valor está en anticipar las condiciones reales de despliegue. El equipo no solo pregunta si el modelo funciona, sino si puede integrarse con los datos disponibles, operar con trazabilidad, superar validación independiente, mantenerse en producción y generar evidencias suficientes para auditoría y supervisión.

La IA exige equipos integrados

Del flujo secuencial por silos al Fusion Team capaz de llevar un caso IA hasta producción gobernada.

Modelo secuencial por silos



❌ **Resultado:**
Trabajo duplicado, bloqueos y pilotos que no escalan



Lectura: La IA no escala cuando cada área valida tarde lo que debería haber diseñado desde el inicio.

Fusion Team de la IA



✅ **Resultado:**
Diseño viable, controles desde el inicio y paso a producción

Claves

1. Anticipa riesgos antes del despliegue.
2. Integra datos, arquitectura y control.
3. Convierte pilotos en capacidades operativas.

La IA no escala cuando cada área valida tarde lo que debería haber diseñado desde el inicio.

Gobernar la IA requiere nuevos roles

Roles para industrializar IA

El control de la IA debe diseñarse antes del despliegue, no añadirse al final.

La banca necesita funciones específicas para integrar arquitectura, riesgo, cumplimiento y evidencia durante todo el ciclo de vida de la IA.

Cuando un caso de IA pasa de piloto a producción, deja de ser solo un desarrollo tecnológico. Debe integrarse en sistemas reales, usar datos gobernados, cumplir requisitos regulatorios, resistir auditorías y mantenerse bajo supervisión durante todo su ciclo de vida.

Por eso hacen falta nuevos roles de gobierno. El **arquitecto de IA empresarial** asegura que la solución encaje con la arquitectura del banco, los sistemas heredados, la seguridad, la resiliencia

y la operación diaria. Su función es evitar que un buen prototipo se convierta en una solución imposible de desplegar o mantener.

Los perfiles de **gestión de IA** traducen riesgo, cumplimiento, validación y auditabilidad en controles verificables. Junto al responsable de dato, validación independiente, seguridad, privacidad y MLOps, convierte la IA en una capacidad operativa gobernada, no en una colección de pilotos aislados.

Roles para industrializar IA

La IA no escala solo con científicos de datos. Necesita funciones que conecten arquitectura, validación, cumplimiento, operación y evidencia.

Cuando un caso de IA pasa de piloto a producción, deja de ser solo un desarrollo tecnológico. Debe integrarse en sistemas reales, usar datos gobernados, cumplir requisitos regulatorios, resistir auditorías y mantenerse bajo supervisión durante su ciclo de vida.

Por eso hacen falta nuevos roles de gestión. Cada función aporta una pieza crítica para que la solución sea desplegable, controlable y defendible en el tiempo. Sin estas funciones, la entidad acumula pilotos, pero no capacidades gobernadas.

“ IDEA CLAVE Gobernar IA no es documentar al final, sino diseñar controles desde el inicio **”**

ESTRUCTURA DE GOBIERNO IA



Objetivo común: Convertir la IA en una capacidad operativa, gobernada, segura y sostenible, que genera valor y cumple con las exigencias regulatorias.

Responsabilidades compartidas a lo largo del ciclo de vida

Diseño

Definición del caso, datos, modelo, métricas y límites de uso

Desarrollo y prueba

Construcción de modelo, validación técnica y prueba de calidad

Validación y aprobación

Revisión independiente, riesgo de modelo y cumplimiento

Despliegue

Integración, controles previos y paso a producción



Operación y monitoreo

Supervisión continua, revalidación, auditoría y mejora continua

Hibridación organizativa

Capacitar en tres capas

El upskilling debe convertir expertos de negocio en perfiles híbridos mediante itinerarios diferenciados por responsabilidad, riesgo y capacidad técnica.

La hibridación organizativa no consiste en formar a toda la plantilla con el mismo nivel técnico. Una entidad financiera necesita una capacitación escalonada, donde cada colectivo entienda la IA en función de su exposición al riesgo, su capacidad de decisión y su papel en el despliegue.

La primera capa crea una base común de **alfabetización segura**. Debe ayudar a usar herramientas de IA con criterio, entender sus límites, proteger información sensible y reconocer riesgos de privacidad, sesgo, seguridad o uso indebido. Es la condición mínima para una adopción amplia sin elevar el riesgo operativo.

La segunda capa desarrolla **perfiles híbridos** en áreas de negocio, riesgo, compliance, operaciones, pagos, finanzas o producto. Aquí se forman profesionales capaces de traducir necesidades reales en casos de uso, trabajar con equipos de datos y valorar si una solución puede desplegarse con controles suficientes.

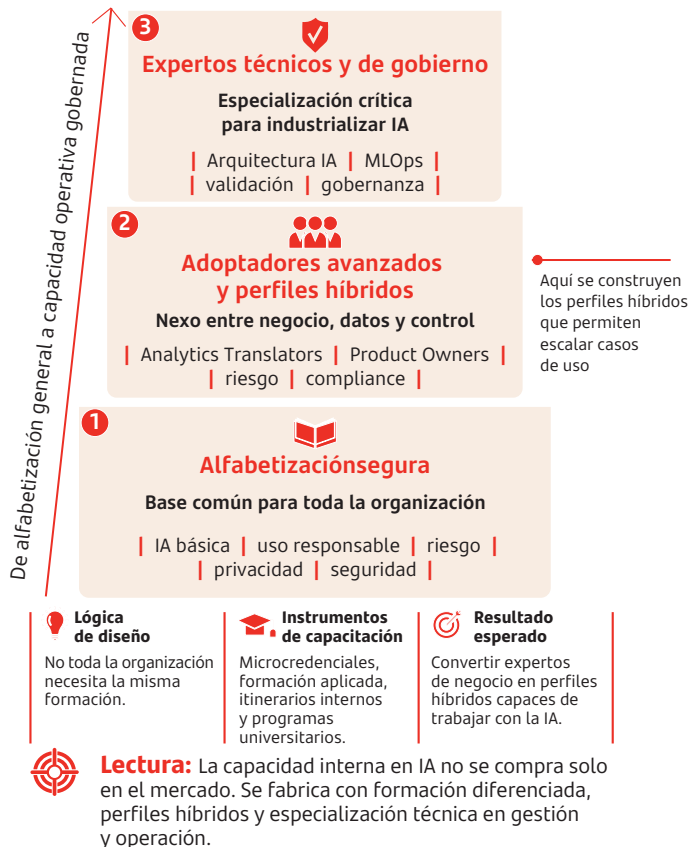
La tercera capa se reserva a especialistas avanzados en **arquitectura de IA, MLOps, validación, privacidad, seguridad y gobernanza**. Su función es asegurar que los modelos no solo funcionen, sino que puedan mantenerse, auditarse y evolucionar durante todo su ciclo de vida.

La capacidad interna se fabrica por capas, no con formación genérica masiva.

Las microcredenciales, los itinerarios internos y los programas universitarios aplicados permiten acelerar esta transición con formación breve, certificable y conectada a problemas reales del banco.

Capacitar en tres capas

La capacidad interna en IA se construye con itinerarios diferenciados por nivel de responsabilidad, riesgo y especialización.



Claves

- La alfabetización segura crea una base común.
- Los perfiles híbridos conectan negocio y tecnología.
- Los expertos avanzados garantizan despliegue y gobernanza.

Instrumentos de retención académica

La retención de talento científico no se resuelve con una única palanca

Doctorados industriales, cátedras y redes de excelencia permiten fidelizar talento y capturar propiedad intelectual aplicada.

La respuesta al **déficit de talento** no puede depender solo del mercado laboral. Instrumentos como los **doctorados industriales, las cátedras ENIA o cátedras Chip**, las redes **ELLIS** y alianzas con centros como el **CSIC** permiten anclar conocimiento científico a retos bancarios concretos.

El doctorado industrial convierte un problema complejo en investigación aplicada con supervisión académica y empresarial.

Las cátedras ofrecen continuidad, reputación y agenda compartida en IA responsable, datos, ciberseguridad o hardware.

Para banca, estos instrumentos cumplen una doble función. Reducen dependencia del outsourcing y crean una cantera estable de perfiles con conocimiento científico, contexto operativo y potencial de generación de propiedad intelectual.

Matriz de instrumentos de retención

Formación, investigación aplicada y captura de propiedad intelectual para fidelizar talento científico

La retención ya no depende solo del salario. Requiere combinar formación, investigación aplicada, financiación pública, redes científicas y captura de propiedad intelectual

Instrumento	Uso principal	Horizonte	Compromiso
 Microcredenciales / Upskilling	Reconvertir perfiles funcionales en perfiles híbridos	6-12 meses	Bajo
 Doctorados industriales	Resolver problemas complejos con I+D aplicada	3-4 años	Medio
 Cátedras ENIA / Chip	Crear líneas estables de IA, dato o hardware	2-4 años	Medio-alto
 Choose Europe / SpAIn Hub	Atraer talento senior internacional o repatriado	Medio-largo plazo	Medio
 Redes ELLIS / Max Planck	Acceder a investigadores top tier y ciencia frontera	Continuo	Alto
 Spin-offs / KIBS	Capturar deep tech, IP y transferencia aplicada	3-5+ años	Variable



Lectura: La estrategia ganadora combina instrumentos de corto plazo para reconvertir talento interno con vehículos de medio y largo plazo para capturar ciencia, IP y capacidades diferenciales.

Lectura orientativa para priorizar mecanismos de retención académica y transferencia tecnológica en banca.

La mejor retención no compete en salario, ofrece misión, ciencia y recorrido profesional.

Alineación normativa interna

Prepararse para auditar algoritmos

El AI Act obliga a convertir gobernanza, documentación, validación y supervisión en capacidades operativas internas.

La regulación europea cambia la forma en que una entidad financiera debe desplegar IA. Ya no basta con aprobar un caso de uso desde el área jurídica o documentar el modelo al final del proyecto. En los sistemas de mayor riesgo, la entidad tendrá que demostrar que el modelo se ha diseñado, probado, supervisado y mantenido con controles verificables.

Esto convierte el cumplimiento en una tarea operativa y técnica. Cada modelo deberá poder clasificarse, vincularse a un responsable, registrar sus datos de entrenamiento o uso, justificar sus cambios y conservar evidencias sobre rendimiento, sesgos, supervisión humana y gestión de incidencias. La pregunta ya no será solo si el modelo cumple, sino si la entidad puede demostrarlo durante todo su ciclo de vida.

Para lograrlo, la organización debe conectar **gobernanza de IA**, riesgo de modelo, protección de datos, seguridad, auditoría interna y responsables de negocio. El objetivo es pasar de políticas generales a una **trazabilidad real del sistema**, donde cada decisión relevante pueda explicarse, revisarse y sostenerse ante auditoría o supervisión.

Ciclo de control AI Act

Del riesgo a la evidencia continua durante todo el ciclo de vida



Lectura: el AI Act convierte la gobernanza de IA en una capacidad operativa. No basta con declarar cumplimiento; hay que demostrarlo con evidencia continua.

Claves

1. Clasificar antes de construir
2. Controlar antes de desplegar
3. Evidenciar durante la vida útil

Cumplir el AI Act exige evidencia operativa, no solo políticas corporativas.

02



Evolución tecnológica, modelos e infraestructura



Activar la oportunidad

La nueva
frontera europea
de la IA B2B

Informe de Vigilancia estratégica



De IA masiva a IA industrial

La evolución de la IA en sectores regulados desplaza el foco desde la potencia máxima hacia la eficiencia económica, el control operativo y la especialización por tarea.

- » **El criterio deja de ser la potencia bruta.** La adopción de modelos fundacionales ya no se decide por elegir el modelo más capaz, sino por identificar el modelo suficiente para cada proceso, con la infraestructura adecuada, la latencia exigida y el nivel de control que requiere el dato.
- » **Los LLMs pierden el rol de opción por defecto.** Siguen siendo relevantes en tareas complejas, abiertas o de alto valor unitario, pero dejan de justificar su uso indiscriminado en procesos regulados y repetitivos, donde el sobre coste no siempre se traduce en una mejora operativa proporcional.
- » **Los SLM pasan a ocupar una capa industrial.** Su menor coste de inferencia, capacidad de despliegue local y adaptación a tareas concretas los convierte en una opción natural para flujos de alto volumen, como clasificación documental, RAG interno, validaciones preliminares o soporte al middle-office.
- » **El análisis financiero reordena la arquitectura.** Cuando la inferencia escala, el consumo vía API transforma la IA en OpEx variable. Frente a ello, el despliegue controlado reduce Vendor Lock-in, mejora previsibilidad presupuestaria y permite amortizar infraestructura en cargas recurrentes. El ecosistema europeo, con iniciativas como ALIA y Salamandra, aporta capacidades multilingües, transparencia y mayor soberanía tecnológica.
- » **La siguiente fase será multimodal.** La adopción ya no se limitará al texto. Voz, visión y modelos multimodales permitirán automatizar procesos documentales, análisis de llamadas, atención al cliente y tratamiento de documentos escaneados con criterios de trazabilidad, seguridad y control operativo.

El fin del *One Model Fits All*

Un solo modelo ya no basta para todas las tareas

Las organizaciones reguladas necesitan una arquitectura multicapa que asigne capacidad, coste y control según criticidad del proceso.

El enfoque **One Model Fits All** pierde sentido cuando la IA pasa del piloto a la operación. Un modelo gigante puede resolver muchas tareas, pero no siempre con el coste, la latencia o el nivel de control que exige un proceso bancario recurrente.

La alternativa no es sustituir todos los **LLMs**, sino reservarlos para usos donde su capacidad adicional justifique el sobrecoste como son el razonamiento complejo, tareas abiertas o decisiones de alto valor unitario. Para procesos acotados, los **SLM** ofrecen

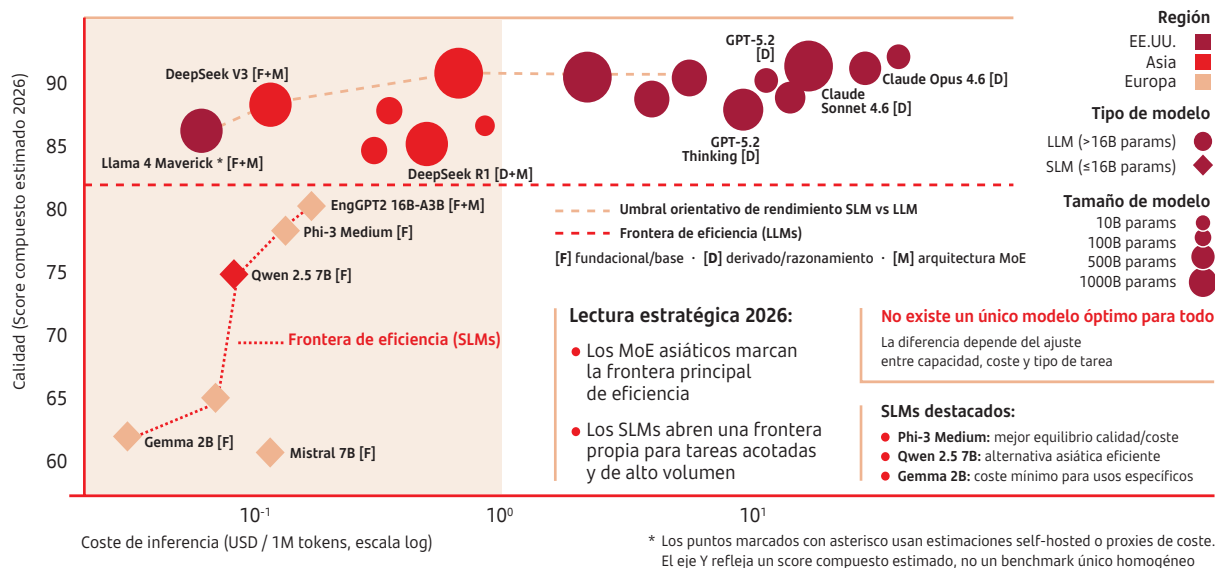
una relación más eficiente entre rendimiento útil y coste operativo.

Con este enfoque, la arquitectura se segmenta por criticidad, volumen y sensibilidad del dato. El resultado es menor **Vendor Lock-in**, mejor reconstrucción del proceso y una asignación más disciplinada del gasto, donde cada modelo ocupa la capa que mejor encaja con el proceso.

La arquitectura empresarial debe adaptar el modelo al proceso, no el proceso al modelo.

Frontera de eficiencia en modelos fundacionales y derivados (2026)

Estimación estratégica: LLMs, arquitecturas MoE y SLMs especializados



Nota metodológica: la clasificación SLM/LLM es orientativa y no responde a un umbral universal. En modelos MoE debe distinguirse entre parámetros totales y activos. El gráfico combina precios API y estimaciones de despliegue, por lo que debe leerse como orientación estratégica, no como benchmark exacto.

La figura distingue modelos fundacionales, modelos derivados y arquitecturas MoE dentro del universo de modelos de propósito general.

Modelos de Lenguaje Pequeños / SLMs

SLMs para volumen bancario

Los SLMs convierten tareas repetitivas en inferencia más económica, rápida y desplegable cerca del dato.

Un **SLM** no debe interpretarse como una versión menor de un LLM, sino como una arquitectura diseñada para tareas acotadas, repetibles y medibles. Su valor aparece cuando la capacidad necesaria está bien definida y el rendimiento suficiente pesa más que la amplitud generalista.

En banca, esta lógica encaja con procesos de alto volumen, como son la clasificación documental, extracción de campos, RAG interno, validaciones preliminares, traducción operativa o apoyo al *middle-office*. En estos casos, el diferencial de calidad frente a un modelo mayor puede no compensar el sobre coste de inferencia.

La ventaja operativa se refuerza cuando el modelo puede desplegarse en entornos propios o privados, cerca del dato o en infraestructura privada. Esto reduce latencia, estabiliza costes, mejora trazabilidad y limita la exposición de información sensible frente a arquitecturas dependientes de APIs externas.

El despliegue local o autoalojado reduce exposición del dato, estabiliza latencia y convierte parte del gasto recurrente en capacidad amortizable. El resultado es una IA menos visible, pero más industrializable.

Por qué un SLM escala mejor en banca

Cinco claves operativas para procesos masivos, recurrentes y sensibles al dato



LECTURA: el SLM gana relevancia cuando la tarea está acotada, el volumen es alto y el control operativo condiciona el caso de negocio.

Un SLM rentable supera a un LLM sobredimensionado en producción masiva.

Ecosistema europeo y multilingüe

Soberanía lingüística operativa

ALIA, Salamandra y modelos europeos permiten cubrir lenguas cooficiales con mayor trazabilidad, apertura y control regulatorio.

Europa empieza a construir una capa propia de modelos abiertos y multilingües para reducir dependencia tecnológica y adaptar la IA a contextos regulados. En España, **ALIA** aporta recursos lingüísticos y multimodales en castellano y lenguas cooficiales, con foco en transparencia, control y despliegue empresarial.

Dentro de ese marco, **Salamandra*** funciona como una familia de modelos compactos orientados a usos prácticos: clasificación,

resumen, extracción documental, traducción y pilotos multimodales. Su valor no está en competir con los LLMs globales, sino en habilitar capacidades ajustables, trazables y cercanas al dato.

En el contexto bancario, estas iniciativas ofrecen una base útil para **explorar IA soberana** en procesos documentales, regulatorios y de atención multilingüe, reduciendo dependencias opacas y mejorando la gobernanza.

Ecosistema europeo de modelos para banca

Base lingüística, modelos controlables y aplicaciones bancarias



* Salamandra es una familia de modelos abiertos de IA desarrollada en el entorno del BSC, orientada a lenguas ibéricas y cooficiales. Incluye modelos de lenguaje y capacidades multimodales, con especial interés para usos donde se requiere mayor transparencia, adaptación local y control del dato.

La soberanía útil es la que reduce riesgo operativo, no solo dependencia tecnológica.

Análisis financiero B2B Build vs. Buy

Comprar agilidad, construir escala

Build ya no significa entrenar desde cero, significa orquestar modelos abiertos bajo control propio cuando el volumen lo justifica.

El debate financiero debe abandonar la falsa dicotomía entre crear modelos desde cero o consumir APIs. En banca, **Build** significa integrar, ajustar y operar modelos abiertos o compactos en infraestructura propia o privada, con foco en control, amortización y estabilidad del coste.

Buy sigue siendo útil cuando la entidad necesita velocidad, elasticidad o acceso inmediato a modelos de frontera. Encaja bien en pilotos, pruebas de concepto y procesos aún poco

estabilizados. Su límite aparece cuando esos usos dejan de ser puntuales y cada nueva automatización incrementa el gasto recurrente.

El criterio de decisión debe apoyarse en el comportamiento económico del proceso. Si el volumen es estable, el dato es sensible y existe capacidad interna para operar el modelo, el despliegue propio gana peso. La estrategia más robusta será híbrida, pero con una regla clara sobre qué se compra y qué se internaliza.

Build vs. Buy en banca

Cómo decidir entre API externa y despliegue propio según coste, control y escala

 BUY API externa		 BUILD SLM local
Adecuado cuando prima la velocidad, la elasticidad y el acceso inmediato a capacidades de frontera.		Adecuado cuando el proceso es estable, recurrente, sensible al dato y requiere control presupuestario.
 OpEx variable	Naturaleza del gasto	 CAPEX inicial amortizable
 Crece con cada automatización	Comportamiento del coste	 Se modera al escalar
 Mayor exposición externa	Control del dato	 Perímetro controlado
 Mayor Vendor Lock-in	Dependencia del proveedor	 Mayor gobierno interno
 Pilotos y procesos variables	Uso recomendado	 Procesos recurrentes y estables
 Regla de decisión La decisión no depende del tamaño del modelo, sino de la estructura económica del proceso y del nivel de control requerido. 		

Comprar acelera el piloto; construir controla la escala.

El Coste Total de Propiedad / TCO

El token oculta el coste

El TCO* revela cuándo la API deja de ser flexible y se convierte en OpEx variable difícil de contener.

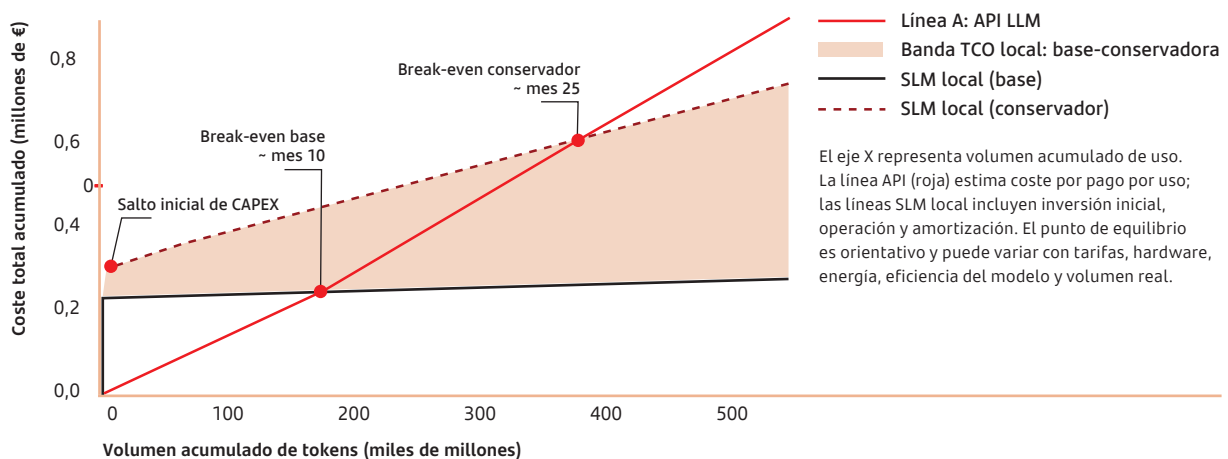
El precio por token es una métrica incompleta para decidir una arquitectura de IA en banca. Puede servir para comparar proveedores, pero no explica el coste real de sostener un proceso en producción, con millones de inferencias, controles de seguridad, monitorización y continuidad operativa.

En consumo vía API, cada incremento de uso se convierte en **OpEx variable**. La entidad gana rapidez inicial, pero el gasto acumulado queda ligado al volumen procesado,

a las tarifas del proveedor y a condiciones comerciales externas. Cuando el proceso escala, la flexibilidad inicial puede transformarse en presión presupuestaria recurrente.

El despliegue propio exige inversión, integración y operación, pero cambia la pendiente del coste. Al internalizar infraestructura y operar **SLM** en entornos controlados, el gasto se vuelve más previsible y amortizable. El TCO permite decidir cuándo esa inversión compensa por volumen, sensibilidad del dato y necesidad de gobierno.

TCO a 36 meses: API vs. SLM local (base y conservador)



* La comparativa de TCO debe interpretarse como una simulación orientativa, no como un resultado fijo. El punto de equilibrio entre API y despliegue propio puede cambiar con rapidez según tarifas de inferencia, precio del hardware, coste energético, volumen real de uso, eficiencia de los modelos y costes de operación. Por ello, el análisis debe revisarse periódicamente y mantener flexibilidad arquitectónica para combinar API, cloud privada y despliegues propios según evolucione cada caso de uso.

El coste relevante no es el token, sino la pendiente del gasto acumulado.

La especialización por tarea

Modelos pequeños, tareas críticas

Un modelo de 7B u 8B de parámetros puede ser suficiente cuando la tarea está acotada, documentada y supervisada.

En tareas bancarias bien delimitadas, un **SLM de 7B u 8B** de parámetros puede ser suficiente si opera sobre fuentes fiables, instrucciones claras y criterios de validación definidos.

seguimiento y cumplimiento son críticos, la calidad de la solución operativa suele pesar más que la capacidad aislada del motor lingüístico.

El rendimiento no depende solo del modelo elegido, sino de cómo se integra en el proceso de negocio. Un modelo puede tener buenas capacidades de base, pero su valor aumenta cuando trabaja sobre fuentes fiables, instrucciones claras y circuitos de decisión bien definidos. En banca, donde precisión,

Esta lógica encaja especialmente en *middle-office*, contratos, expedientes, normativa interna o traducción documental. Son procesos repetitivos, sensibles al coste y con suficiente estructura para industrializarse. Ahí la ganancia viene de asignar el modelo adecuado, no de sobredimensionar la arquitectura.

Qué modelo encaja con cada tarea bancaria

Mapa tarea-modelo para procesos especializados

 Tarea bancaria	 Modelo suficiente	 Por qué encaja	 Control operativo
 RAG interno	SLM 7B-8B	Consulta sobre fuentes controladas	Alto
 Traducción documental	SLM 7B-14B	Tarea acotada y repetible	Medio-alto
 Clasificación de contratos	SLM 7B-16B	Extracción y clasificación estructurada	Alto
 Middle-office documental	SLM 8B-14B	Alto volumen y baja variabilidad	Alto
 Validación humana	SLM + workflow	Supervisión en puntos críticos	Crítico



Principio de asignación

Tarea acotada + fuente controlada + validación definida = SLM suficiente

En procesos bancarios repetitivos, el rendimiento útil depende más del diseño operativo que del tamaño máximo del modelo.

Mapa conceptual orientativo basado en tareas documentales y de middle-office descritas en el informe.

La especialización convierte tamaño limitado en rendimiento suficiente.

IA multimodal y modelos de voz

Voz y documento bajo control

La multimodalidad específica automatiza llamadas, documentos escaneados y formularios sin recurrir siempre a modelos gigantes.

La siguiente capa de eficiencia no será solo textual. En banca, una parte relevante de la información operativa llega en formatos no estructurados, como llamadas, PDFs escaneados, formularios, justificantes o imágenes documentales. La **IA multimodal** trata esos materiales dentro de flujos trazables y supervisados.

Los modelos de voz y visión tienen valor cuando se aplican a tareas concretas. La identificación y separación de interlocutores en llamadas, la transcripción, el análisis de documentos escaneados o la extracción de campos no requieren siempre un modelo

generalista de máxima escala. Pueden resolverse con modelos especializados, integrados en procesos controlados.

La prioridad no es añadir más canales, sino gestionarlos. En atención al cliente, back-office documental o cumplimiento, la multimodalidad debe operar con seguridad, retención controlada, revisión humana y métricas de calidad.

Aquí modelos como **Salamandra-VL** o soluciones europeas de voz como **Whisper Large V3** desplegado en entornos propios pueden reducir latencia y **OpEx** sin perder control operativo.

Flujos multimodales bajo control

Voz y documento en procesos bancarios supervisados



Principio operativo: La multimodalidad aporta valor cuando se integra en flujos específicos, medibles y bajo control.

No se trata de añadir más canales, sino de gobernar voz, documento y revisión dentro del entorno bancario.

Arquitecturas de control y frontera agéntica

Del RAG soberano al razonamiento autónomo supervisado.

El valor operativo de la IA bancaria depende de optimizar despliegue, proteger memoria corporativa y gobernar razonamiento avanzado.

- » **La eficiencia ya no se decide únicamente por el tamaño del modelo.** Técnicas como MoE, destilación, LoRA y compresión permiten reducir cómputo, latencia y consumo de infraestructura, acercando capacidades avanzadas a entornos bancarios donde el coste, la escalabilidad y la gobernanza son factores determinantes.
- » **La arquitectura se convierte en el principal factor de diferenciación.** Dos organizaciones pueden utilizar modelos similares, pero obtener resultados muy distintos según cómo gestionen recuperación de información, seguridad, trazabilidad, integración con sistemas internos y control operativo.
- » **El RAG Soberano separa el motor de lenguaje de la memoria documental del banco.** Esta decisión evita que el conocimiento corporativo quede embebido en el modelo y mantiene políticas, procedimientos y documentación crítica bajo gestión directa de la entidad.
- » **La soberanía del dato exige algo más que repositorios privados.** Zero Egress, enclaves seguros y mecanismos de computación confidencial garantizan que la información sensible permanezca dentro de perímetros autorizados durante todo el ciclo de inferencia y uso.
- » **El salto hacia sistema 2 introduce una nueva generación de capacidades centradas en el razonamiento.** Los modelos dejan de limitarse a predecir respuestas y comienzan a verificar pasos, contrastar información y justificar procesos antes de emitir una recomendación.
- » **La IA Agéntica amplía este enfoque al permitir que los sistemas interactúen con herramientas, aplicaciones y flujos de trabajo.** Su adopción en banca dependerá menos de la autonomía tecnológica y más de la capacidad para imponer límites, registrar decisiones y mantener supervisión humana en los puntos críticos.

Arquitecturas de optimización

Inferencia más ligera y útil

Las técnicas de optimización reducen coste, latencia y consumo de infraestructura sin convertir cada despliegue en ingeniería pesada.

La optimización busca desacoplar capacidad funcional y coste operativo. No todas las tareas requieren activar la totalidad de un modelo ni mantener infraestructuras sobredimensionadas. Arquitecturas MoE activan únicamente los componentes necesarios para cada consulta, mientras la destilación y el afinado eficiente trasladan capacidades específicas a modelos más compactos y especializados.

En banca, este enfoque acerca la IA al dato y desplegarla sobre servidores estándar, nodos internos o entornos con restricciones

de infraestructura. Técnicas como **LoRA**, compresión y cuantización reducen memoria, consumo energético y latencia sin comprometer el rendimiento cuando el proceso está bien definido y dispone de fuentes controladas.

La decisión relevante no es elegir una técnica aislada, sino qué limitación condiciona el caso de uso. Si el reto es coste, velocidad de respuesta o capacidad de despliegue, la arquitectura debe optimizar primero la eficiencia del sistema antes de aumentar el tamaño del modelo.

Arquitecturas para una inferencia desplegable

Técnicas para reducir coste, latencia y fricción material del despliegue



Lectura: Cada técnica resuelve un cuello de botella distinto: coste, adaptación, latencia o despliegue local.

Optimizar no reduce ambición, reduce la fricción material del despliegue.

RAG Soberano*

Memoria fuera del modelo

El RAG soberano conecta IA y conocimiento corporativo sin incorporar documentación sensible a los pesos del modelo.

El RAG Soberano introduce una separación deliberada entre capacidad de razonamiento y conocimiento corporativo. En lugar de incorporar documentación interna mediante reentrenamientos continuos, el modelo consulta en tiempo real repositorios documentales gobernados por la entidad. La arquitectura reduce la dependencia de los pesos del modelo y permite que la información utilizada sea siempre la versión vigente y autorizada.

La ventaja no es únicamente técnica, sino operativa y regulatoria. Al mantener el conocimiento fuera del modelo, resulta posible actualizar políticas, retirar documentos obsoletos, segmentar accesos y reconstruir con precisión qué fuentes respaldaron cada respuesta. La memoria corporativa permanece bajo control documental, con criterios de gobierno equivalentes a los aplicados sobre cualquier otro activo crítico de la organización.

Para una organización regulada, esta aproximación permite utilizar normativa, contratos, procedimientos internos o criterios de riesgo sin exponerlos a procesos de entrenamiento ni perder trazabilidad sobre su uso. La calidad de la respuesta deja de depender exclusivamente del modelo y pasa a apoyarse en la combinación entre razonamiento, recuperación documental y control de las fuentes consultadas.

* RAG soberano para conocimiento corporativo gobernado.

Memoria corporativa fuera del modelo

Riesgo de entrenamiento directo frente a arquitectura de RAG soberano



Riesgo de incorporación al modelo



1 Documentación sensible



2 Ajuste/entrenamiento



3 Modelo con memoria implícita



4 Respuesta difícil de reconstruir

- Actualización más costosa
- Menor claridad sobre la base documental efectiva
- Reconstrucción posterior más difícil



RAG soberano



1 Consulta del usuario



2 Búsqueda semántica



3 Repositorio documental privado



4 Fragmentos recuperados



5 Modelos de IA



6 Respuesta trazable

- Mayor control sobre el dato
- Actualización documental más ágil
- Mejor trazabilidad de la respuesta



Lectura: Separar razonamiento y almacenamiento no elimina el riesgo, pero mejora control, actualización y trazabilidad documental.

El conocimiento sensible debe ser recuperado, no sedimentado en el modelo.

Arquitecturas de contención y protección del dato

El dato permanece dentro del perímetro

Zero Egress combina red, infraestructura y computación aislada para contener el dato durante todo el ciclo de inferencia.

El **RAG Soberano** solo alcanza todo su potencial cuando se apoya en una arquitectura capaz de controlar el recorrido completo de la información.

Zero Egress, una arquitectura de aislamiento de datos y comunicaciones, responde a esta necesidad estableciendo un principio simple, ya que los datos sensibles no deben abandonar el perímetro autorizado durante los procesos de recuperación, enriquecimiento contextual, inferencia o generación de respuestas.

Los enclaves seguros y la computación confidencial refuerzan esta protección durante el uso activo del dato. La arquitectura separa recuperación documental, almacenamiento e

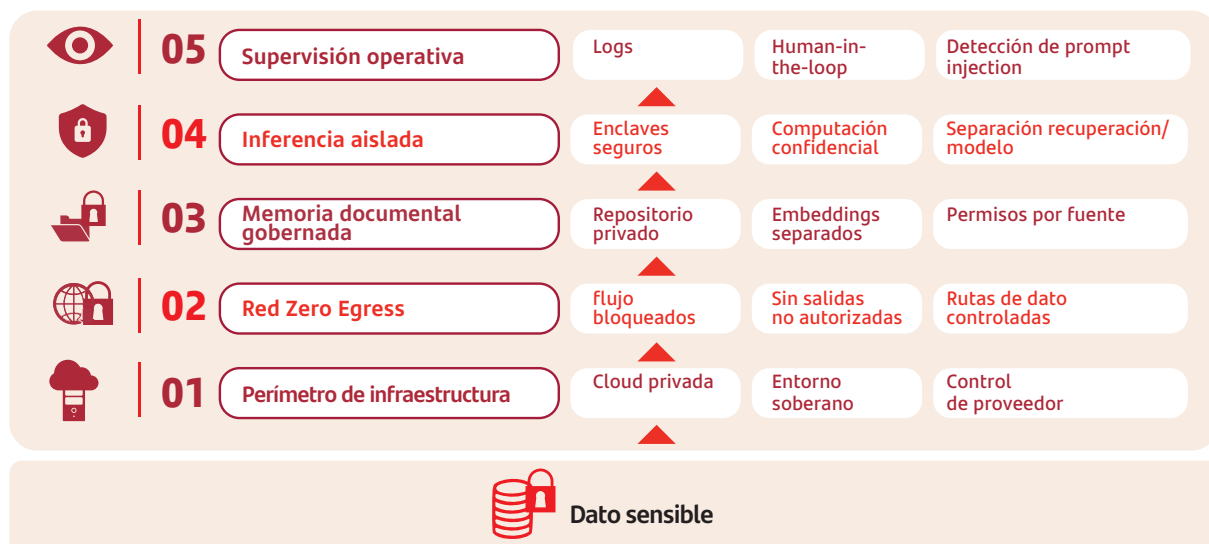
inferencia para reducir superficies de exposición, limitar movimientos innecesarios de información y facilitar el control granular de permisos, rutas de acceso y registros operativos.

En un entorno bancario, esta capa no es únicamente una medida de seguridad. Es un mecanismo de gestión que demuestra dónde ha estado el dato, quién ha accedido a él y bajo qué condiciones ha sido procesado. Cuando intervienen proveedores tecnológicos, infraestructuras híbridas o modelos especializados, la capacidad de mantener trazabilidad, segregación y supervisión técnica se convierte en un requisito operativo y regulatorio.

La soberanía del dato exige controlar también su recorrido técnico.

Capas de contención del dato sensible

Arquitectura de protección para operar IA sobre información confidencial



Lectura: La soberanía del dato no depende de una pieza aislada, sino de una arquitectura de red, memoria, inferencia y supervisión.

El salto al sistema 2*

Razonar antes de responder

El sistema 2 añade cómputo de inferencia, verificación y contraste para pasar de respuesta probable a una salida explicable.

El sistema 2 no supone sustituir los modelos actuales, sino añadir una capa de razonamiento más deliberativa sobre la generación probabilística. Frente a una respuesta inmediata basada en patrones estadísticos, estos sistemas pueden dedicar más capacidad de cómputo durante la inferencia para descomponer problemas, evaluar alternativas y verificar cada paso antes de emitir una conclusión.

Esta capacidad es especialmente útil en entornos donde existen reglas, procedimientos y criterios de validación explícitos. En banca, puede aportar valor en cumplimiento normativo, revisión de políticas internas, análisis

documental, gestión de expedientes o apoyo a procesos de riesgo, donde no basta con responder, sino que es necesario justificar cómo se ha llegado a una determinada recomendación.

Su aportación principal no es alcanzar una certeza absoluta, sino mejorar la calidad del proceso de decisión. Al incorporar mecanismos de contraste, evidencia documental y validación intermedia, el **sistema 2** reduce respuestas no fundamentadas, facilita la trazabilidad y mejora la capacidad de supervisión humana en contextos de elevada exigencia regulatoria.

De respuesta probable a salida verificable

Arquitectura generador-verificador para procesos bancarios con reglas, fuentes y supervisión



Lectura: El sistema 2 no elimina el riesgo, pero convierte la respuesta en un proceso más trazable, revisable y gobernable.

* El concepto de sistema 2 se inspira en la distinción popularizada por Daniel Kahneman entre pensamiento rápido y pensamiento deliberativo. En IA, se usa de forma análoga para describir arquitecturas que incorporan pasos de razonamiento, verificación y contraste antes de generar una salida final.

El sistema 2 convierte la respuesta en un proceso verificable.

IA Agéntica y automatización compleja

De responder a actuar

La IA agéntica convierte instrucciones en flujos operativos, siempre que herramientas, permisos y supervisión estén acotados.

La **IA Agéntica** supone un paso más allá de los asistentes conversacionales tradicionales. Mientras estos generan respuestas a partir de una petición, un agente puede planificar acciones, utilizar herramientas y coordinar distintos pasos para alcanzar un objetivo concreto. Su aportación no consiste solo en responder mejor, sino en transformar una instrucción en un proceso operativo ejecutable y verificable.

En banca, esta capacidad abre la puerta a abordar procesos que hoy requieren múltiples sistemas, consultas y validaciones. Actividades como el onboarding de clientes, la gestión hipotecaria, determinadas tareas de back office o el apoyo a funciones de riesgo y cumplimiento pueden beneficiarse de agentes capaces de consultar fuentes autorizadas, recopilar información y preparar evidencias para su revisión. El objetivo debe ser reducir fricción operativa sin sustituir los controles ni eliminar la supervisión necesaria.

La lógica se amplía con los sistemas multiagente, donde distintas funciones especializadas colaboran para resolver una tarea compleja. La división del trabajo puede mejorar eficiencia y escalabilidad, pero exige mecanismos sólidos de coordinación y trazabilidad para reconstruir cada paso realizado.

La adopción de IA Agéntica no debe entenderse como una búsqueda de autonomía total. Su valor reside en aumentar la capacidad operativa dentro de límites definidos, combinando automatización, control y puntos de intervención humana cuando la criticidad del proceso así lo requiera.

De instrucción a flujo operativo gobernado

Cómo la IA agéntica se acopla a herramientas, sistemas internos y controles bancarios



Qué aporta

- Menos fricción operativa
- Mayor coordinación entre sistemas
- Automatización multipaso

Qué no implica

- No sustituye sistemas core
- No elimina supervisión
- No autoriza acciones sin control



La autonomía solo aporta valor cuando cada herramienta, permiso y acción queda acotada, registrada y supervisada.

La autonomía útil es la que ejecuta bajo límites, no la que opera sin control.

Gestión de Agentes de IA

Agentes con perímetro operativo

Para que un agente opere de forma segura dentro de una organización, es necesario definir con claridad quién actúa, qué herramientas puede utilizar, cuáles son sus límites y cuándo debe intervenir una persona para supervisar o validar el proceso.

Cuando un **agente de IA** puede interactuar con sistemas, aplicaciones o procesos, el riesgo ya no está solo en la calidad de la respuesta, sino en **la acción que ejecuta**. Una recomendación puede revisarse, mientras que una operación mal autorizada puede afectar a clientes, controles internos o requisitos regulatorios.

Por eso, la gestión agéntica debe centrarse en el **runtime operativo**. Cada agente necesita una identidad verificable, un catálogo cerrado de herramientas, permisos mínimos por función y límites explícitos sobre qué puede consultar, modificar o escalar. La autonomía solo es aceptable si opera dentro de un **perímetro previamente definido**.

La **trazabilidad** es el segundo requisito. El banco debe poder **reconstruir qué hizo el agente**, qué fuente consultó, qué herramienta utilizó, qué decisión propuso y en qué punto intervino una persona. Sin logs completos y validación humana en procesos sensibles, el agente deja de ser gobernable.

En banca, la confianza no se basa en asumir que el agente actuará correctamente, sino en poder **comprobar cada paso**. La eficiencia procede de automatizar tareas, mientras que el control depende de acotar permisos y dejar rastro operativo.

Controles mínimos del runtime agéntico

Lista de gobierno operativo para agentes de IA en banca regulada

- 1  **Identidad del agente**
Quién actúa, con qué rol y bajo qué contexto.
- 2  **Herramientas autorizadas**
Catálogo cerrado de APIs, sistemas e interfaces permitidas.
- 3  **Límites de permisos**
Acceso mínimo necesario y acciones restringidas por criticidad.
- 4  **Logs de acción**
Registro completo de pasos, consultas, herramientas y resultados.
- 5  **Validación humana**
Aprobación obligatoria en operaciones sensibles o irreversibles.
- 6  **Interrupción y reversión**
Capacidad de detener, bloquear o revertir acciones no conformes.



Principio de gobierno

Todo agente debe operar con identidad, permisos y herramientas definidos antes de ejecutar una acción.



Un agente solo es gobernable si identidad, herramientas, permisos y acciones quedan acotados desde el diseño.

El agente solo es gobernable si identidad, permisos y acciones quedan registrados.

Radar Deep Tech - Mapa estratégico de capacidades emergentes

Buscar mejores soluciones

La IA evolutiva introduce ciclos de generación, evaluación y selección para optimizar soluciones bajo restricciones explícitas.

La siguiente frontera no consiste solo en responder mejor, sino en explorar soluciones que no habían sido consideradas inicialmente. A diferencia de los modelos generativos convencionales, los **enfoques evolutivos generan múltiples alternativas**, las evalúan mediante métricas o simulaciones y conservan las de mejor resultado para seguir refinándolas. Más que predecir, buscan, prueban y optimizan.

Proyectos como AlphaEvolve, FunSearch o GNoME muestran cómo esta aproximación permite recorrer espacios de solución muy amplios e identificar opciones que podrían pasar desapercibidas para métodos convencionales. Su valor no está solo en generar alternativas, sino en aprender de forma sistemática cuáles funcionan mejor y bajo qué condiciones.

En empresas reguladas, estas capacidades pueden ser relevantes pero requieren prudencia. La modelización de riesgo, la optimización de carteras, la detección de fraude o los ejercicios de stress testing podrían beneficiarse de mecanismos avanzados de exploración y simulación, siempre que mantengan criterios de evaluación transparentes, auditables y alineados con los marcos de control existentes.

El potencial aparece cuando existen datos fiables, objetivos bien definidos y mecanismos sólidos para evaluar resultados. En ese contexto, la IA evolutiva amplía la capacidad analítica de los equipos, explorando escenarios y estrategias difíciles de revisar manualmente, sin sustituir la responsabilidad ni el juicio experto.

Dentro de esta agenda técnica, Quantum AI, optimización y PQC deben mantenerse como líneas de vigilancia activa, con foco en simulación, optimización financiera, resiliencia criptográfica y preparación temprana de PQC.

Radar Deep Tech de IA evolutiva

De la predicción a la búsqueda controlada de soluciones bajo restricciones

Nivel 3 Exploración profunda



Búsqueda evolutiva



Optimización multiobjetivo
Quantum AI / optimización / PQC



Laboratorios internos de validación

Nivel 2 Vigilancia activa



Stress testing



Liquidez



Simulación de escenarios

Nivel 1 Señales cercanas



Modelado en grafos



Fraude / AML



Testing y modernización tecnológica

Nivel 0 Generar alternativas

Refinar
Evaluar
Seleccionar

Condiciones para avanzar



Evaluadores robustos



Restricciones explícitas



Validación fuera de muestra



Revisión experta



No es una hoja de ruta cerrada, sino un mapa de vigilancia para problemas con datos, restricciones y métricas suficientes.



Lectura: El valor no está en delegar la decisión final, sino en ampliar la capacidad del banco para explorar mejores opciones bajo control.

La IA evolutiva no automatiza la decisión. Amplía la búsqueda de mejores soluciones bajo control.

Infraestructuras soberanas y sostenibilidad

El soporte físico de la soberanía y la IA verde

- » **La IA deja de ser solo una cuestión de modelos.** Su despliegue depende de capacidad de cálculo, centros de datos, energía, refrigeración, almacenamiento y gobernanza del dato.
- » **Europa avanza con EuroHPC, AI Factories y las futuras Gigafactorías** para reducir dependencia tecnológica y convertir la supercomputación en capacidad accesible para industria, ciencia, administraciones públicas y sectores estratégicos.
- » **España gana peso como hub operativo** con la RES, **MareNostrum 5**, BSC AI Factory y la nueva AI Factory del CESGA, articulando escala europea, especialización sectorial y capilaridad territorial.
- » **La banca puede adoptar una estrategia de orquestación selectiva**, manteniendo la nube tradicional para operaciones cotidianas y recurriendo a infraestructuras soberanas de supercomputación para cargas críticas, simulaciones avanzadas y ajuste fino de modelos.
- » **La sostenibilidad entra en la decisión tecnológica.** El **TCO** de la IA debe incorporar electricidad, carbono, agua, inferencia masiva y reporting de **Alcance 3**, convirtiendo la eficiencia energética y la trazabilidad climática en factores clave de competitividad.

Fábricas, Gigafactorías y Data Labs

Cómputo europeo al servicio de la industria

Las AI Factories convierten supercomputación en acceso industrial, mientras los Data Labs preparan datos sensibles bajo control.

Las *AI Factories* impulsadas por **EuroHPC** representan un cambio de enfoque respecto a la supercomputación tradicional. No se limitan a ofrecer capacidad de cálculo, sino que crean un **entorno completo de adopción industrial** que combina infraestructura, soporte especializado, herramientas de desarrollo y acceso simplificado para acelerar proyectos de IA en sectores estratégicos.

Las Gigafactorías operan en una dimensión distinta. Están diseñadas para entrenar y desplegar modelos fundacionales de gran escala, concentrando enormes recursos de energía, almacenamiento y conectividad. Su función es dotar a Europa de capacidades comparables a las de los grandes polos tecnológicos globales y reforzar su autonomía tecnológica.

Para el sector financiero, el elemento más relevante son los **Data Labs**. Estos entornos permiten preparar, anonimizar, validar y gobernar datos sensibles dentro de perímetros controlados antes de acceder a recursos externos de supercomputación. El resultado es una combinación de escalabilidad, protección de la propiedad intelectual y cumplimiento regulatorio que facilita el uso seguro de capacidades avanzadas de IA.

La capacidad útil no empieza en la GPU, sino en el dato gobernado.

De infraestructura europea a capacidad bancaria útil

Cómo AI Factories, Data Labs y Data Spaces convierten supercomputación en capacidad operativa segura para banca

4



AI Gigafactory

Ultraescala para modelos de frontera y capacidad estratégica.

3



AI Factory

Cómputo, soporte técnico, pruebas, ajuste fino e inferencia avanzada.

2



Data Lab controlado

Preparación, anonimización, validación y gobierno del dato.

1



Data Space europeo

Marco común de intercambio e interoperabilidad.

Lectura para banca



Dato sensible bajo control



IP protegida



Acceso industrial seguro



Lectura: La soberanía útil no depende solo del cómputo disponible, sino de preparar y gobernar el dato antes de activarlo.

El Hub de Supercomputación Español

España como nodo soberano

La RES, MareNostrum 5 y CESGA sitúan a España en el mapa europeo de computación avanzado para IA.

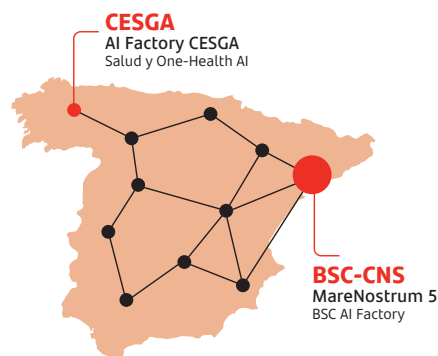
La Red Española de Supercomputación no es una instalación aislada ni un único centro de cálculo. Se trata de una infraestructura distribuida que conecta catorce nodos especializados bajo la coordinación del BSC. Esta arquitectura combina capacidades de supercomputación, IA, gestión avanzada de datos y experimentación tecnológica dentro de una estrategia nacional alineada con las prioridades europeas.

MareNostrum 5 constituye el principal activo de esta red por su capacidad para ejecutar cargas de trabajo de gran complejidad. Su evolución hacia una factoría de IA amplía el acceso a recursos de cálculo avanzados y facilita el entrenamiento, la validación y el despliegue de modelos en entornos controlados. Más allá de la potencia disponible, su valor reside en convertir la infraestructura científica en una capacidad utilizable por empresas e instituciones.

La adjudicación de una nueva factoría de IA al **CESGA** consolida esta posición y añade especialización en ámbitos estratégicos vinculados a la salud y One-Health AI. La combinación de una red distribuida, capacidades de referencia internacional y nuevos polos sectoriales sitúa a España como uno de los principales puntos de apoyo para la soberanía tecnológica europea.

España como nodo soberano

La **RES**, **Marenostrum 5** y **CESGA** refuerzan el papel español en la supercomputación europea para IA



Conexión con EuroHPC

Escala europea al servicio de la soberanía tecnológica



RES

Infraestructura distribuida que conecta capacidades de supercomputación, IA y datos a escala nacional.



MareNostrum 5

Principal activo de cálculo avanzado para entrenamiento, validación e inferencia en entornos controlados.



CESGA AI Factory

Añade una nueva capacidad sectorial y refuerza la especialización española en IA.



Soberanía computacional

España combina escala, capilaridad territorial y conexión operativa con las prioridades europeas.

España pasa de participar en EuroHPC a operar nodos críticos de IA.

La tercera vía para sectores regulados

Combinar nube, infraestructura propia y supercomputación europea

Las empresas reguladas no necesitan sustituir su infraestructura, sino activar supercomputación europea para procesos críticos y diferenciales.

La banca no necesita elegir entre depender por completo de grandes proveedores tecnológicos o reproducir internamente toda la capacidad de cálculo necesaria para la IA general. El enfoque más eficiente es **combinar distintas infraestructuras según el valor y las exigencias de cada proceso**. La nube y los entornos propios siguen siendo adecuados para operaciones habituales y de ejecución continua, mientras que la **supercomputación europea** puede reservarse para aquellos procesos que requieren una capacidad excepcional o un **mayor control estratégico**.

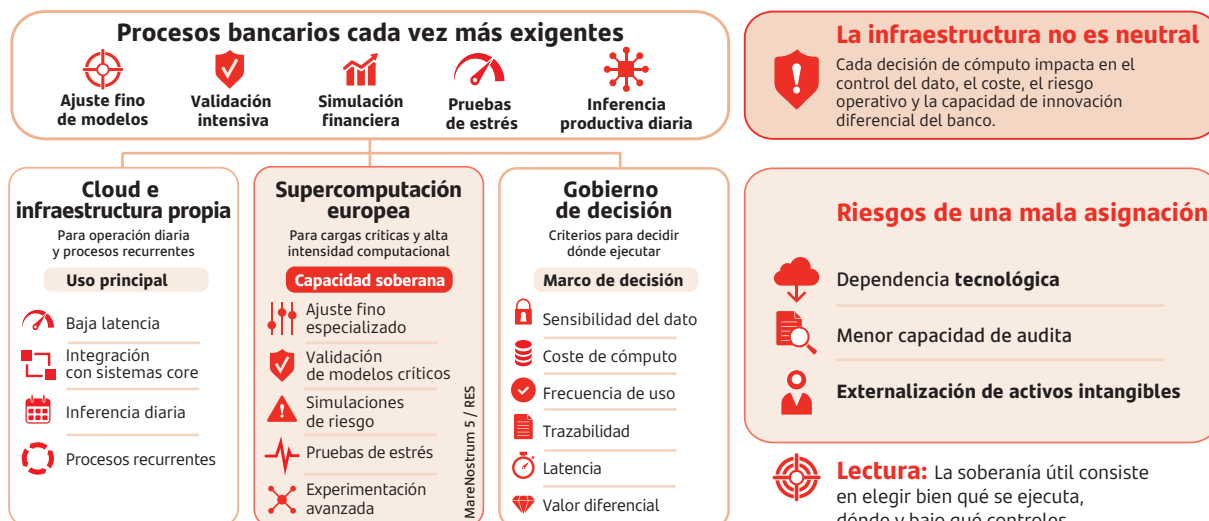
Esta **orquestación selectiva** accede a recursos avanzados cuando realmente aportan ventaja. Resulta especialmente útil para el ajuste fino de modelos especializados, la validación

intensiva de algoritmos, las simulaciones financieras complejas, las pruebas de estrés regulatorias o el análisis masivo de carteras. También facilita la **experimentación con modelos fundacionales** adaptados a necesidades concretas del sector financiero.

La decisión no debe responder únicamente a criterios tecnológicos. Cada caso de uso debe analizarse considerando la sensibilidad de los datos, el coste total de cálculo, la frecuencia de utilización, las necesidades de trazabilidad, los requisitos de latencia y el valor diferencial que genera para la entidad. El objetivo es asignar cada proceso al entorno que ofrezca el mejor equilibrio entre eficiencia, control y soberanía tecnológica.

Tercera vía para el cómputo bancario

La banca no sustituye su infraestructura. Decide qué procesos se ejecutan en cada capa según criticidad, coste y control.



El cuello de botella energético

La infraestructura invisible que sostiene la IA

La IA escala sobre electricidad, refrigeración y agua, no solo sobre algoritmos, datos y APIs.

La expansión de la IA desplaza el debate tecnológico hacia una realidad mucho más material. Detrás de cada modelo existen centros de procesamiento de datos (CPDs), redes de comunicaciones, sistemas de almacenamiento y mecanismos de refrigeración que requieren una cantidad creciente de recursos físicos. A medida que las organizaciones incorporan capacidades de IA en sus procesos, la presión sobre estas infraestructuras aumenta y convierte la **disponibilidad de energía** en un factor estratégico.

El **entrenamiento** de modelos avanzados concentra grandes necesidades de cálculo durante periodos concretos. Sin embargo, el **verdadero desafío** aparece cuando esos modelos pasan a **producción**. La **inferencia** desplegada sobre

millones de interacciones diarias genera una demanda continua asociada a procesos como la detección de fraude, la evaluación de riesgos, la atención al cliente o la automatización documental. Lo que parece una consulta individual de bajo impacto se transforma, a gran escala, en un consumo sostenido de recursos.

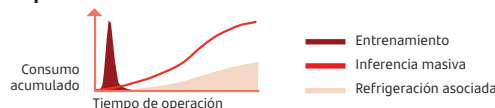
A esta dimensión energética se añaden otros factores relevantes como las emisiones asociadas al consumo eléctrico y el uso de agua necesario para la **refrigeración** de las instalaciones. Por eso, la **sostenibilidad** de la IA no depende únicamente del diseño del modelo. También está condicionada por la eficiencia de la infraestructura, la ubicación de los CPDs y la calidad del sistema energético que los alimenta.

El peaje físico de la IA bancaria

Del modelo al consumo continuo de infraestructura, energía y agua



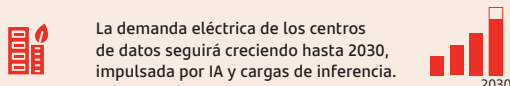
Impacto acumulativo de la inferencia en banca



Procesos bancarios que impulsan la inferencia masiva



Contexto de infraestructura



Lectura: La IA bancaria consume menos por grandes entrenamientos aislados y más por millones de inferencias repetidas cada día.

Green AI y gestión regulatoria

Modelos eficientes por obligación

Green AI conecta rendimiento, consumo y cumplimiento, convirtiendo la eficiencia energética y de recursos en criterio de gestión tecnológica.

La IA sostenible (**Green AI**) no implica renunciar a capacidades avanzadas ni limitar la innovación. Su planteamiento consiste en **utilizar la escala adecuada para cada necesidad** y evitar el uso de modelos sobredimensionados cuando existen alternativas más eficientes. En el sector bancario, una parte relevante de los procesos documentales, operativos y de soporte puede resolverse con modelos especializados de menor tamaño (SLMs) que ofrecen resultados comparables con un consumo significativamente inferior.

El enfoque combina distintas técnicas para optimizar recursos y mantener el rendimiento. Los SLMs, la destilación de modelos, la generación aumentada mediante recuperación de información, la compresión y las arquitecturas híbridas reducen el consumo energético, disminuir los tiempos de respuesta y contener los costes operativos. La eficiencia pasa a formar parte de la decisión de arquitectura, coste y gobierno tecnológico.

La regulación europea empuja en la misma dirección. Tanto el Reglamento Europeo de IA (AI Act) como las nuevas exigencias sobre CPDs impulsan una mayor transparencia sobre el impacto material de los modelos y de la infraestructura que los soporta. Medir, comparar y justificar el uso de recursos será cada vez más importante para demostrar sostenibilidad, cumplimiento normativo y creación de valor a largo plazo.

Cinco claves de Green AI en banca

De la eficiencia técnica a la obligación regulatoria y financiera

01

Elegir escala adecuada

No todos los procesos requieren modelos grandes.



Modelo

02

Priorizar SLMs especializados

Menor consumo, menor latencia y mejor control.



Computación

03

Optimizar arquitectura

RAG, destilación, compresión y despliegues híbridos.



Arquitectura

04

Medir impacto material

Electricidad, agua, hardware, CPD y ciclo de vida.



Infraestructura

05

Documentar cumplimiento

AI Act, métricas, trazabilidad y gobierno del modelo.



Gobernanza



De eficiencia técnica a obligación regulatoria

La eficiencia debe medirse, documentarse y explicarse ante gobierno interno y supervisores.

AI Act

Métricas CPD

Trazabilidad energética

Capas materiales consideradas

Modelo

Computación

Electricidad

Refrigeración / agua

Hardware

Centros de datos

Cadenas de suministro



Lectura: La Green AI convierte la eficiencia del modelo en una decisión de coste, cumplimiento y legitimidad operativa.

La Green AI será la que justifique su escala, no la que solo maximice rendimiento.

El reto de las emisiones financiadas

Alcance 3*, el gran reto

La mayor huella climática bancaria no está en oficinas o tecnología propia, sino en la actividad económica financiada.

El reporting climático bancario encuentra uno de sus mayores desafíos en las emisiones financiadas. Dentro del **Alcance 3**, la categoría 15 atribuye a las entidades una parte de las emisiones generadas por prestatarios, empresas participadas, emisores o proyectos que reciben financiación. Esta dimensión resulta especialmente relevante porque conecta la actividad financiera con el impacto climático de la economía real.

La complejidad va mucho más allá de una cuestión metodológica. Los bancos deben integrar información procedente de múltiples fuentes, con distintos niveles de calidad y madurez.

A ello se suman datos incompletos, documentación no estructurada y la necesidad de asignar factores de emisión de forma coherente a miles de exposiciones. En este contexto, la IA emerge como una herramienta capaz de mejorar la identificación, clasificación y estimación de información climática, reforzando la consistencia de los procesos de cálculo.

La presión supervisora también está aumentando. Ya no basta con anunciar objetivos o compromisos de descarbonización. Las entidades deben demostrar con evidencia verificable cómo delimitan sus perímetros de cálculo, qué calidad tienen los datos utilizados y qué evolución presentan sus carteras de crédito e inversión frente a los objetivos climáticos.

El reto de las emisiones financiadas

El mayor perímetro climático del banco está en la actividad económica que financia



“ El verdadero núcleo del reporting climático bancario está en lo que se financia, no solo en lo que se consume. ”



Dato crítico

Las emisiones financiadas pueden ser más de **700 veces** superiores a las emisiones directas reportadas por instituciones financieras.



Brecha de divulgación

Solo el **15 %** de los bancos analizados divulgaba emisiones financiadas. Datos incompletos, Perímetros heterogéneos, KPIs climáticos insuficientes



Lectura: La credibilidad climática bancaria depende menos de medir oficinas y más de demostrar qué emisiones se financian.

* El concepto Alcance 3 procede del GHG Protocol, marco internacional de contabilidad de emisiones que clasifica las emisiones indirectas de la cadena de valor. En banca incluye, entre otras, las emisiones asociadas a créditos, inversiones y proyectos financiados.

IA para la inteligencia climática

IA para cuantificar emisiones financiadas y riesgo climático

La propia IA puede cubrir vacíos de información climática, ordenar datos ESG y mejorar el reporting financiero.

La IA puede convertirse en una herramienta clave para abordar parte de los desafíos que el la misma contribuye a ampliar. A medida que aumentan las exigencias de transparencia climática, las entidades financieras deben gestionar grandes volúmenes de información procedente de fuentes heterogéneas y con distintos niveles de calidad. En este contexto, la IA facilita la identificación de datos relevantes, la clasificación de actividades económicas, la detección de vacíos de información y la transformación de documentos dispersos en métricas comparables y útiles para la toma de decisiones.

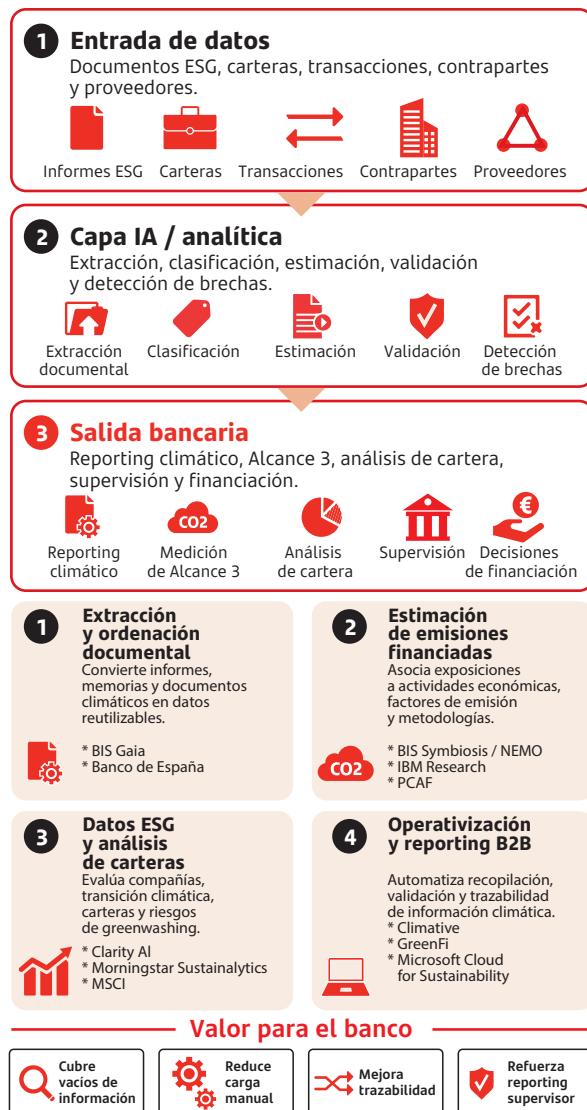
Experiencias como BIS Gaia, Symbiosis, NEMO, IBM Research o las iniciativas impulsadas por el Banco de España muestran que estas capacidades ya tienen aplicaciones prácticas. La IA extrae divulgaciones climáticas, estructurar información corporativa compleja, apoyar la aplicación de metodologías como PCAF y reforzar la trazabilidad necesaria para responder a requerimientos de supervisión y auditoría.

Su aportación resulta especialmente valiosa cuando se integra con datos externos, estándares reconocidos y procesos de validación experta. De este modo, las entidades pueden ampliar su capacidad analítica, mejorar la calidad del reporting y avanzar hacia una gestión más consistente de las emisiones financiadas y de los riesgos climáticos asociados.

La IA climática aporta valor cuando convierte datos incompletos en decisiones trazables.

Mapa de soluciones de inteligencia climática

De datos ESG incompletos a reporting, análisis de carteras y decisiones trazables



Control necesario

La IA ayuda a estimar y ordenar, pero requiere metodología, validación y revisión experta.

Agenda técnica prioritaria europea

De tendencias emergentes a líneas fundacionales de desarrollo

Las nuevas ramas de IA no solo deben estar en el foco de la vigilancia estratégica, sino que ya forman una agenda de capacidades fundacionales para competir en IA B2B regulada con soberanía, trazabilidad y aplicabilidad industrial.

No son solo tendencias. Son líneas fundacionales para desarrollar capacidades reguladas, trazables y menos dependientes de plataformas cerradas.



03



Marco regulatorio y cumplimiento



Activar la oportunidad

**La nueva
frontera europea
de la IA B2B**

Informe de Vigilancia estratégica



Cumplimiento y regulación

El marco normativo como ventaja defensiva para escalar IA bancaria con control, soberanía y capacidad de respuesta supervisora.

- » **AI Act y DORA elevan el listón de entrada para proveedores B2B.** La trazabilidad, la documentación técnica y la resiliencia operativa dejan de ser requisitos secundarios para convertirse en criterios clave de selección y contratación.
- » **El cumplimiento actúa como un filtro de calidad de mercado.** Las soluciones capaces de demostrar controles, evidencias y procesos auditables generan mayor confianza y reducen la incertidumbre regulatoria para la entidad.
- » **La explicabilidad y la supervisión humana exigidas por el AI Act fortalecen la adopción empresarial de la IA.** Los modelos que pueden justificar sus resultados son más fáciles de validar, escalar y defender ante auditorías y supervisores.
- » **La soberanía del dato reduce la exposición jurídica, la dependencia tecnológica y los riesgos asociados al acceso extraterritorial a información sensible.** La arquitectura debe preservar control, confidencialidad y continuidad operativa.
- » **Integrar la IA en la Gestión de Riesgo de Modelo (MRM) permite gobernar modelos, sesgos, cambios, proveedores y mecanismos de supervisión bajo un marco único de riesgo.** Esta aproximación protege la inversión del Banco y facilita una trazabilidad completa desde el diseño hasta la operación.

La regulación como producto

Compliance como ventaja comercial

El cumplimiento desde el diseño convierte trazabilidad, supervisión humana y documentación técnica en atributos que diferencian la solución.

El **AI Act** modifica los criterios con los que una entidad financiera evalúa y selecciona soluciones de IA. La capacidad técnica sigue siendo relevante, pero deja de ser suficiente para justificar una adopción a escala. Las organizaciones deben acreditar el origen de los datos, la trazabilidad de los procesos, la supervisión humana de las decisiones y la existencia de controles que permitan explicar el comportamiento del sistema ante clientes, auditores y supervisores. La transparencia deja así de ser solo una exigencia normativa y se convierte en un atributo de confianza y diferenciación.

Este cambio refuerza el principio de **Compliance by Design**, donde el cumplimiento se incorpora desde las primeras fases de diseño y contratación. La decisión de construir internamente, comprar una solución de mercado o combinar ambos enfoques debe evaluarse por el control que permite mantener durante todo el ciclo de vida. La capacidad para auditar proveedores, preservar el linaje de los datos, intervenir sobre los modelos y generar evidencias verificables determina la solidez regulatoria de la inversión y reduce riesgos futuros de adaptación, dependencia tecnológica o incumplimiento.

Compliance como ventaja comercial

El cumplimiento desde el diseño convierte trazabilidad, supervisión humana y documentación técnica en atributos de producto.

Compliance by Design como filtro de decisión tecnológica

CRITERIO REGULATORIO	BUY	BUILD
 Linaje de datos	 Dependencia del proveedor	 Mayor control interno
 Documentación y validación	 Evidencias heredadas	 Esfuerzo propio de compliance
 Tiempo de despliegue	 Más rápido	 Más condicionado por validación
 Control tecnológico	 Riesgo de dependencia	 Mayor soberanía y adaptabilidad

Factores claves para una decisión gobernable

 Linaje de datos	 Derechos de auditoría	 Supervisión humana	 Evidencias reutilizables	 Control del proveedor	 Ciclo de vida completo
---	---	--	--	---	--

 **No gana siempre la estrategia Build frente a Buy. Gana la opción más gobernable durante todo el ciclo de vida.**

En sectores regulados, una IA no gobernable deja de ser una solución y pasa a ser un riesgo.

Gestión integrada y MRM*

MRM para escalar IA segura

La IA en entornos regulados necesita un modelo único que integre regulación, resiliencia, ciberseguridad y control técnico.

Una entidad regulada no debe abordar el **AI Act**, **DORA** y **NIS2** como obligaciones independientes. En la práctica, una misma **solución de IA** puede activar exigencias simultáneas en materia de explicabilidad, resiliencia operativa, ciberseguridad, protección de datos y supervisión de terceros. Gestionarlos por separado aumenta el riesgo de duplicidades, controles inconsistentes y respuestas difíciles de coordinar ante supervisores y órganos de gobierno.

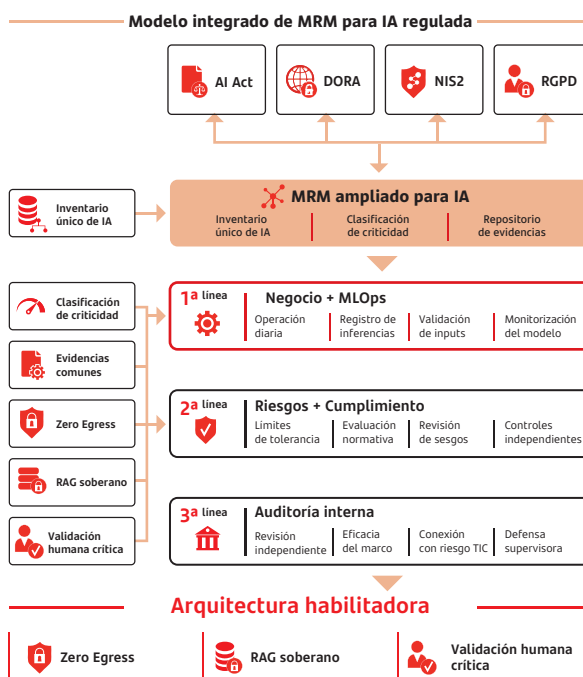
El siguiente paso es ampliar el marco de MRM hacia un modelo integrado de supervisión apoyado en tres líneas de defensa. Las áreas de negocio y los equipos operativos aplican controles continuos sobre el funcionamiento de los modelos. Las funciones de riesgos y cumplimiento verifican que se respeten los límites establecidos y evalúan el impacto regulatorio y ético de cada caso de uso. La auditoría interna aporta una revisión independiente sobre la eficacia del conjunto.

Este enfoque se refuerza mediante arquitecturas como **Zero Egress**, RAG soberano sobre repositorios documentales controlados por el banco y mecanismos de validación humana que refuerzan la trazabilidad y la capacidad de respuesta durante todo el ciclo de vida.

MRM para escalar IA segura

La IA bancaria necesita un modelo único que integre regulación, resiliencia, ciberseguridad y control técnico.

Un solo lenguaje de riesgo para tecnología, negocio, cumplimiento y auditoría



Escalar IA exige un solo lenguaje de riesgo para tecnología, negocio, cumplimiento y auditoría.

* MRM, o Gestión de Riesgo de Modelo, es el marco que permite identificar, validar, monitorizar y auditar los modelos utilizados por el Banco durante todo su ciclo de vida.

Caso de actualidad: acceso a modelos frontera y soberanía operativa

Cuando el acceso al modelo también
se convierte en riesgo geopolítico

El caso Fable 5 y Mythos 5 muestra que los modelos frontera empiezan a comportarse como infraestructura estratégica, no solo como software comercial.

En junio de 2026, **Anthropic** comunicó que el Gobierno de Estados Unidos había emitido una directiva de control de exportaciones para **suspender el acceso a sus modelos Fable 5 y Mythos 5** a cualquier persona sin nacionalidad estadounidense, dentro o fuera del país. Para asegurar el cumplimiento de la orden, la compañía indicó que debía desactivar ambos modelos para todos sus clientes, aunque el resto de modelos de Anthropic no se veía afectado.

Más allá del caso concreto, el episodio ilustra un **riesgo creciente para empresas reguladas** y sectores críticos. El acceso a modelos frontera puede quedar condicionado por decisiones externas de política industrial, seguridad nacional o control de exportaciones.

Para una entidad que integre IA en procesos críticos, la dependencia exclusiva de modelos cerrados sujetos a jurisdicciones externas puede introducir riesgos de continuidad, trazabilidad, cumplimiento y soberanía operativa.

Este tipo de situaciones refuerza la tesis central del informe. La soberanía en IA no implica aislarse de los modelos globales, sino **construir una arquitectura híbrida**, flexible y gobernable. Esto exige combinar proveedores externos, modelos abiertos o desplegables en entornos controlados, capacidades internas de evaluación, planes de contingencia y criterios claros sobre qué procesos pueden depender de servicios externos y cuáles requieren mayor control operativo.

La dependencia crítica no está solo en el dato o la infraestructura. También está en la continuidad de acceso a los modelos que sostienen procesos sensibles.



Términos de uso, propiedad y equipo de trabajo

Los contenidos, análisis, interpretaciones y conclusiones recogidos en este informe han sido elaborados en el marco del proyecto de vigilancia estratégica sobre IA desarrollado para Banco Santander. El documento tiene una finalidad exclusivamente informativa, estratégica y de apoyo a la reflexión interna, y no debe interpretarse como una recomendación definitiva de inversión, contratación, implantación tecnológica o adopción operativa.

La información incluida en el informe se basa en fuentes públicas, documentación técnica, análisis experto y materiales de trabajo recopilados durante el desarrollo del proyecto. Aunque se ha realizado un esfuerzo razonable por contrastar y ordenar la información disponible, el ámbito de la IA evoluciona con rapidez, por lo que los datos, referencias, tecnologías, empresas y conclusiones recogidas pueden quedar sujetos a actualización o revisión posterior.

Las menciones a empresas, tecnologías, instituciones, expertos o iniciativas externas tienen carácter descriptivo y analítico. Su inclusión no implica recomendación comercial, validación formal, relación contractual

ni posicionamiento oficial por parte de Banco Santander, salvo que así se indique expresamente.

El uso de este informe queda limitado al ámbito interno y profesional autorizado por Banco Santander. Cualquier reproducción, distribución, comunicación pública, adaptación o reutilización total o parcial de sus contenidos deberá contar con autorización previa, salvo en aquellos casos en los que se permita expresamente y siempre citando adecuadamente la fuente.

La titularidad de este informe y de los materiales desarrollados en el marco del proyecto corresponde a Banco Santander, sin perjuicio de los derechos que puedan corresponder a terceros sobre marcas, logotipos, fuentes, referencias, imágenes, gráficos o contenidos citados. Todas las marcas y nombres comerciales mencionados pertenecen a sus respectivos titulares.

Este documento ha sido elaborado por el equipo de trabajo del proyecto, integrado por profesionales de Banco Santander y de la Fundación General CSIC en las tareas de análisis, estructuración de contenidos, vigilancia estratégica y preparación documental.

Equipo de trabajo

Banco Santander: Equipo de AI Lab

Fundación General CSIC: Unidad de Vigilancia Estratégica (Dpto. Innovación)

Este informe está disponible bajo la licencia CC BY-NC 4.0:
<https://creativecommons.org/licenses/by-nc/4.0/?ref=chooser-v1>

Cómo citar este informe:

Banco Santander y Fundación General CSIC. (2026). *La nueva frontera europea de la IA B2B*. Banco Santander.

© Banco Santander, 2026. Todos los derechos reservados.

Sede corporativa: CGS Av. Cantabria s/n
28660 Boadilla del Monte, Madrid (España)

