RM | REZA MONSHIZADEH
AI · TECHNOLOGY · GOVERNANCE

BOARD BRIEFING REPORT
BANCA EUROPEA & MERCADOS FINANCIEROS

Tenemos una política, una norma y un certificado — ¿qué demuestran?

Un Board Briefing Report sobre la arquitectura de gobernanza de la IA — EU AI Act, ISO/IEC 42001, NIST AI RMF, pruebas y evidencia.

Reza Monshizadeh · Monshizadeh.com · 7 min de lectura

01 SITUATION

Cada uno se describe como el marco. Ninguno responde a la misma pregunta.

SUPONGAMOS LA SIGUIENTE SITUACIÓN

La dirección presenta al consejo:

- una política de IA alineada con el EU AI Act,
- un programa de certificación ISO/IEC 42001,
- una metodología de riesgo basada en el NIST AI Risk Management Framework,
- y un proceso de pruebas técnicas.

Un certificado no sustituye una matriz de correspondencia regulatoria.

Una evaluación de riesgos no demuestra que un control funcione.

Un resultado de prueba no acredita que se hayan identificado las obligaciones jurídicas correctas.

LA PREGUNTA AL CONSEJO

¿Puede la dirección demostrar cómo se conectan las obligaciones jurídicas, la gobernanza organizativa, las decisiones de riesgo y las pruebas de los sistemas en un único modelo operativo trazable?

02 MANAGEMENT SUMMARY

Tres puntos de orientación para el consejo.

01

Un marco completo tiene cuatro capas conectadas

El derecho define las obligaciones. El sistema de gestión hace repetible la gobernanza. El método de riesgo estructura el juicio. Las pruebas y la evidencia muestran cómo funcionan sistemas y controles. Complementarias — no intercambiables.

02

Un certificado no es una matriz de correspondencia

ISO/IEC 42001 puede proporcionar un sistema de gestión de la IA certificable — no establece automáticamente el cumplimiento del EU AI Act. **EN 18286** se desarrolló específicamente para el requisito de gestión de la calidad del AI Act.

03

Un Framework Stack, no una única etiqueta

La prueba requerida es una línea trazable desde la obligación hasta el control, la prueba, el responsable y la evidencia conservada — una arquitectura gobernada que cubra toda la población de IA y su ciclo de vida.

Una entidad puede comprar un certificado. No puede comprar la matriz de correspondencia.

03 CALIBRACIÓN DE LA CALIDAD DE RESPUESTA

El estado RAG calibra la calidad de la respuesta. No juzga a la entidad.

DIMENSIÓN	VERDE	ÁMBAR	ROJO
Inventario	Una única población de IA gobernada y conciliada	Existe un inventario, pero parte de la IA de terceros o integrada queda fuera	*"Sabemos dónde está nuestra IA."*
Mapeo jurídico	Matriz de correspondencia de requisitos a controles por caso de uso	Existe un mapa jurídico, pero no está vinculado a los controles	*"Estamos alineados con el EU AI Act."*
Alcance de la certificación	Alcance, exclusiones y límites organizativos son explícitos	Existe un certificado, pero su alcance no está conciliado con el inventario de IA	*"Estamos en proceso de obtener una certificación ISO."*
Método de riesgo	La clasificación determina la ruta de gobernanza	Existen puntuaciones de riesgo, pero no modifican requisitos ni aprobaciones	*"Aplicamos el marco NIST."*
Pruebas	Los umbrales de aceptación están vinculados al uso previsto	Se realizan pruebas, pero están desconectadas del caso de uso o de la decisión	*"El proveedor ha probado el modelo."*
Responsabilidad	Un responsable identificado tiene autoridad para aprobar, detener y escalar	Intervienen comités, pero la autoridad personal no está clara	*"Pasa por el comité de IA."*
Terceros	Se definen evidencias, obligaciones de notificación de cambios y derechos de aseguramiento	Existen cláusulas contractuales, pero la evidencia operativa es incompleta	*"Es responsabilidad del proveedor."*
Información al consejo	Se informa de eficacia, excepciones y decisiones	Se informa del estado de ejecución, pero la eficacia de los controles no es visible	*"El programa avanza según lo previsto."*

VERDE no es un certificado. VERDE es una línea trazable desde la obligación hasta la evidencia.

04 EL FRAMEWORK STACK

Cuatro capas. Cuatro preguntas distintas. Un modelo operativo.

01 MARCO JURÍDICO

¿Qué debe hacer la entidad?

EU AI Act, RGPD, DORA, regulación financiera y requisitos aplicables en materia de productos, empleo y protección de los consumidores.

LO QUE ESTA CAPA NO DEMUESTRA POR SÍ SOLA
Que la entidad haya traducido las obligaciones en controles operativos.

02 SISTEMA DE GESTIÓN

¿Quién gobierna la IA y mediante qué responsabilidades y procesos?

ISO/IEC 42001, ISO/IEC 38507 y, para el requisito de gestión de la calidad del AI Act, EN 18286.

LO QUE ESTA CAPA NO DEMUESTRA POR SÍ SOLA
Que cada sistema de IA esté correctamente clasificado, sea jurídicamente conforme o técnicamente fiable.

03 MÉTODO DE RIESGO

¿Cómo se identifican, evalúan, aceptan y tratan los riesgos de la IA?

NIST AI RMF, ISO/IEC 23894, metodologías de riesgo de modelo y procesos de clasificación de riesgos empresariales.

LO QUE ESTA CAPA NO DEMUESTRA POR SÍ SOLA
Que los controles seleccionados funcionen eficazmente.

04 PRUEBAS & EVIDENCIA

¿Qué demuestra que el sistema y sus controles funcionan como se afirma?

AI Verify, evaluaciones de impacto, validación, pruebas de robustez y seguridad, pruebas de controles y aseguramiento independiente.

LO QUE ESTA CAPA NO DEMUESTRA POR SÍ SOLA
Que todas las obligaciones aplicables hayan sido identificadas y asignadas.

Cada capa responde a una pregunta distinta. Ninguna responde a la siguiente.

05 QUIÉN DEBE RESPONDER

Una respuesta integrada de la dirección — liderada por el directivo responsable de la IA empresarial, la tecnología o los datos, junto con el directivo responsable de riesgos o cumplimiento.

PARTICIPANTES NECESARIOS

■ Responsabilidad de negocio	■ Legal	■ Cumplimiento	■ Riesgos
■ Riesgo de modelo	■ Tecnología	■ Datos	■ Ciberseguridad
■ Protección de datos	■ Riesgo de terceros	■ Compras	■ Auditoría interna

NOTA DE RESPONSABILIDAD

Pertenecer a un comité no equivale a asumir responsabilidad personal. El responsable identificado debe tener la autoridad necesaria para aprobar, limitar, suspender o escalar el uso de IA correspondiente.

AUDITORÍA INTERNA

La Auditoría Interna puede evaluar el diseño y la eficacia operativa. No debe convertirse en propietaria de la gobernanza de IA de primera línea.

06 EVIDENCIA QUE EL CONSEJO DEBE SOLICITAR

Diez artefactos que hacen verificable la arquitectura.

01 **Inventario empresarial de IA**
Una población gobernada que cubra la IA desarrollada internamente, adquirida, integrada y proporcionada por terceros.

02 **Mapa de arquitectura de marcos**
La relación entre derecho, sistemas de gestión, métodos de riesgo, pruebas y aseguramiento.

03 **Matriz de correspondencia regulatoria**
Requisitos aplicables conectados con políticas, controles, responsables, pruebas y evidencias.

04 **Responsabilidades y derechos de decisión**
Autoridad de aprobación, aceptación del riesgo residual, intervención, suspensión y escalado.

05 **Metodología de clasificación**
Clasificación jurídica, materialidad, impacto en clientes, criticidad operativa y reversibilidad.

06 **Mapa de controles del ciclo de vida**
Requisitos desde el inicio y la contratación hasta el despliegue, el cambio y la retirada.

07 **Evaluación de impacto y riesgo**
Una evaluación completada para un caso de uso con consecuencias relevantes.

08 **Registro de pruebas y validación**
Objetivos, métodos, umbrales de aceptación, excepciones y aprobación.

09 **Declaración del alcance de la certificación**
Entidades, procesos, sistemas, exclusiones y límites de certificación cubiertos.

10 **Paquete de información para el consejo**
Exposición al riesgo, excepciones, incidentes, cambios materiales, acciones vencidas y decisiones requeridas.

Un caso de uso debe poder seguirse desde su clasificación jurídica hasta su estado actual en producción — **sin cambiar poblaciones, definiciones o responsables entre documentos.**

07 GOVERNANCE CHECK

SEÑALES DE ALERTA

Estas respuestas pueden sonar tranquilizadoras en una reunión del consejo. Todavía no ofrecen una base suficiente para una decisión del consejo.

- ⚠ *“Aplicamos el marco NIST.”*
- ⚠ *“Una persona aprueba el resultado.”*
- ⚠ *“Estamos alineados con el EU AI Act.”*
- ⚠ *“Eso está cubierto por la política de IA.”*
- ⚠ *“Estamos en proceso de obtener una certificación ISO.”*
- ⚠ *“Es solo una herramienta interna.”*
- ⚠ *“El proveedor ha probado el modelo.”*
- ⚠ *“El marco se está implantando.”*

Ninguna de estas afirmaciones es necesariamente incorrecta. **Simplemente no constituye evidencia suficiente para que el consejo pueda confiar en ella.**

08 PATH TO GREEN

Seis condiciones para una arquitectura gobernada.

01 Arquitectura definida

Las cuatro capas están definidas y se utilizan de forma coherente.

02 Matriz de correspondencia construida

Las obligaciones se conectan con controles, responsables, pruebas y evidencias.

03 La clasificación determina la ruta

La materialidad y el estatus jurídico determinan la intensidad de la gobernanza.

04 Estándar de evidencia definido

Los registros necesarios se especifican antes de la aprobación para producción.

05 Terceros incluidos

Modelos, datos, herramientas e infraestructuras externos permanecen dentro del perímetro de gobernanza.

06 Eficacia supervisada

La información al consejo muestra el funcionamiento de los controles, las excepciones y las decisiones — no solo el avance del programa.

SIGUIENTE PREGUNTA PARA EL CONSEJO

Tomen un sistema de IA que pueda afectar materialmente a un cliente, un empleado, una transacción o un proceso crítico — ¿puede la dirección mostrar, en una única cadena de evidencias, el derecho aplicable, el responsable designado con autoridad decisoria, la decisión de riesgo aprobada, los controles operativos, los resultados de las pruebas, la vía de intervención humana, las dependencias de terceros y el estado actual en producción?

EXECUTIVE QUESTIONS FOR EUROPEAN BANKING & FINANCIAL MARKETS

Una entidad puede comprar un certificado. No puede comprar la matriz de correspondencia.

El consejo no debe preguntar qué marco aplica la entidad. Debe preguntar si un uso de IA con consecuencias relevantes puede trazarse desde la obligación hasta la evidencia operativa.

FUENTES SELECCIONADAS

Regulation (EU) 2024/1689 — Artificial Intelligence Act.

Regulation (EU) 2026/1744 — Digital Omnibus on AI.

CEN-CENELEC — EN 18286: Quality Management for EU AI Act Purposes.

ISO/IEC 42001:2023 — AI Management Systems.

ISO/IEC 42006:2025 — Certification of AI Management Systems.

NIST — AI Risk Management Framework & Generative AI Profile.

AI Verify Foundation — Testing Framework.

EBA — AI Act Implications for Banking and Payments.

Reza Monshizadeh · Senior Technology Executive · Frankfurt