

IA Y GOBERNANZA...*cuando el riesgo ya no es opcional*



**De la experimentación a la
responsabilidad**

Una pregunta para el Comité de Riesgos

Si mañana una IA toma una
decisión equivocada que genera
una pérdida,

¿quién responde?



01

EL RIESGO CAMBIÓ

La IA no solo cambia
cómo trabajamos.
Cambia cómo debemos
gobernar.



¿Qué pasa cuando la IA se equivoca... y nadie se da cuenta?

- Una decisión puede ser incorrecta.
- Una respuesta puede ser falsa.
- Un dato puede ser confidencial.



Y todo puede ocurrir en segundos.



El riesgo ya no está confinado a tecnología

La IA ya no automatiza solamente tareas



La IA no solo hace más.
Lo hace mucho más rápido.



A mayor autonomía, mayor necesidad de gobierno.

La IA no crea el riesgo desde cero

Muchos riesgos ya existían.

La IA cambia su velocidad, escala y alcance.



**IA =
velocidad + escala +
autonomía + opacidad**

**El riesgo no desaparece
porque cambie la tecnología.**

Lo que la IA puede construir... y destruir en segundos



El riesgo no está solo en el algoritmo

El riesgo aparece en todo el ciclo de vida, no solamente cuando construimos el modelo.



Gobernar IA significa gobernar todo su ciclo de vida.

02

CUANDO EL RIESGO SE MATERIALIZA

Un error puede ser pequeño.
Su escala, no.



4362

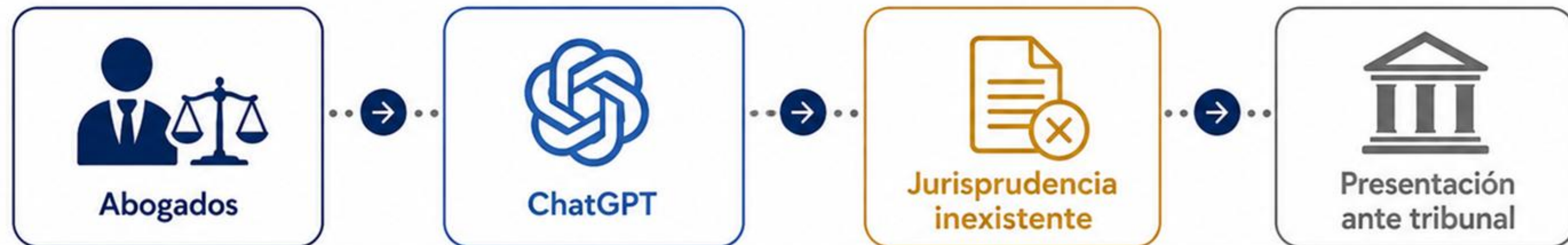
Incidentes de IA documentados en 2025*

↑ **56% vs. año anterior**

* *AI Index Report 2025, Stanford*

Roberto Mata vs. Avianca: cuando la IA inventa lo que nunca existió

Un caso real que expone un problema mucho mayor **que ChatGPT.**



La IA puede generar el contenido. La responsabilidad no se genera con él.

La IA generó la información.

¿Quién era responsable de verificarla?



**Human oversight no es tener un humano en el proceso.
Es tener un humano que pueda cuestionar y detener**

El problema no era solamente la IA.

- ✗ Confianza excesiva en la herramienta
- ✗ Ausencia de validación
- ✗ Falta de supervisión
- ✗ Confusión entre velocidad y calidad
- ✗ Responsabilidad mal definida



GOBERNANZA

El fallo tecnológico se convirtió en incidente porque falló la gobernanza.

Cuando el dato confidencial entra en la IA



SAMSUNG

2023- Ingenieros cargaron código fuente, procesos internos y **notas confidenciales** en ChatGPT



La mayor amenaza de seguridad no siempre viene de afuera



Documento confidencial



Empleado



IA generativa (ChatGPT)



Fuga de información



Información fuera de control

El dato que entra en una IA también entra en su ecosistema de riesgo.

RIESGO:



Confidencialidad



Propiedad intelectual



Fuga de información

Cuando el chatbot dice algo que la empresa no quería decir



2024- El chatbot brindó información falsa sobre tarifas; la empresa intentó desligarse.

La responsabilidad legal no puede delegarse a la IA.

● **Ausencia de accountability**



¿Puede una empresa decir “fue la IA” para evitar una responsabilidad?

Tres casos... Tres riesgos... Una misma pregunta.

Avianca

Decisión
Supervisión
Validación

SAMSUNG

Información
Confidencialidad
Uso permitido



AIR CANADA

Cliente
Responsabilidad
Control



¿Quién gobierna el uso de IA?

03

DEL INCIDENTE A LA GESTIÓN

El incidente es visible.
La vulnerabilidad que
lo hizo posible,
no siempre.



La IA puede amplificar errores existentes



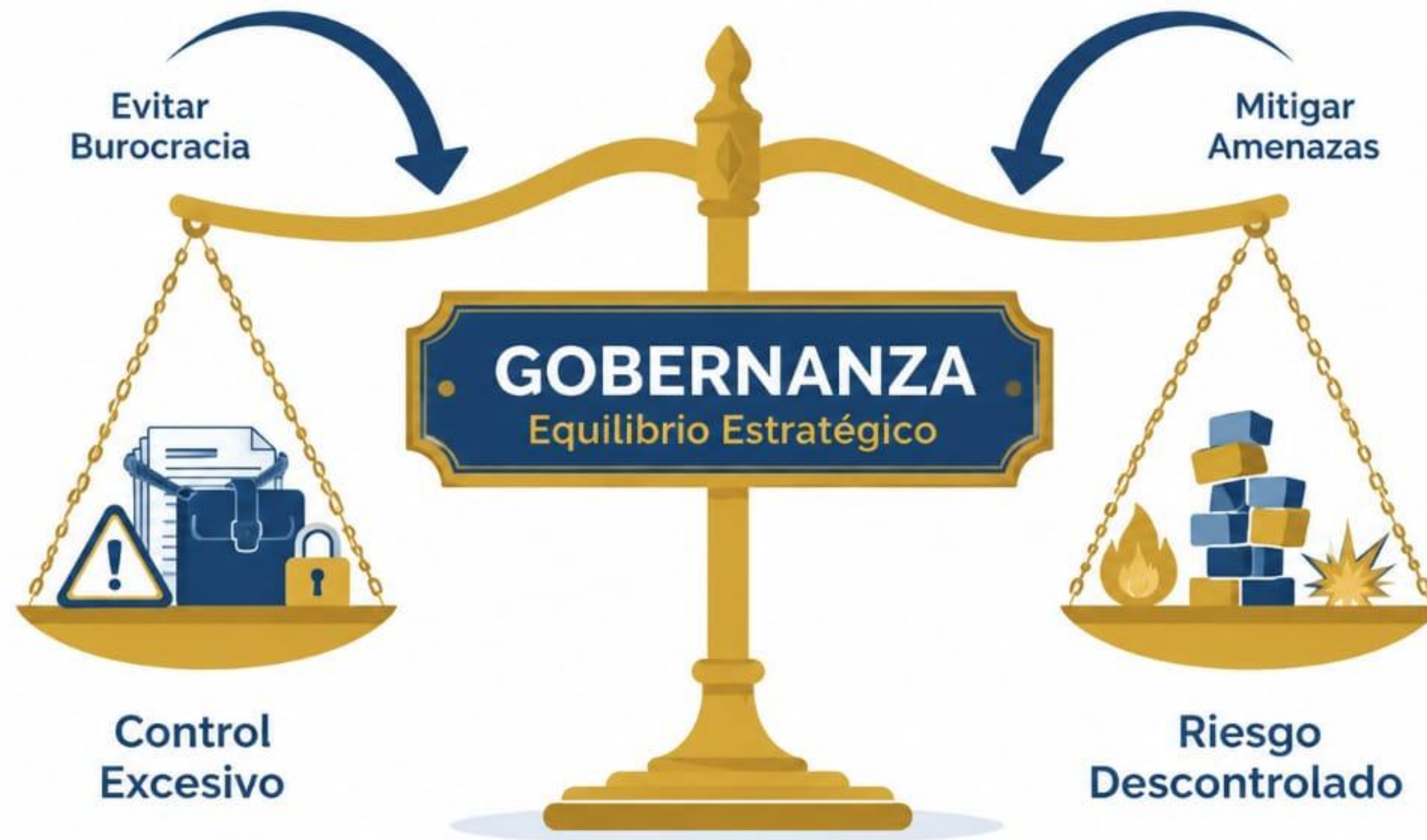
La escala cambia la naturaleza del riesgo.

¿Qué estamos permitiendo que la IA haga?



No todos los usos de IA tienen el mismo nivel de riesgo.

Gobernar la IA no significa decir "NO"



Gobernanza = innovación con límites claros.

La gobernanza de IA empieza mucho antes del modelo



No gobernamos solamente el modelo; gobernamos para qué, cómo y dónde se utiliza.

04

¿QUIÉN GOBIERNA LA IA?

La IA puede ejecutar.
La responsabilidad sigue teniendo dueño.



Tres estándares, una estructura de gestión.



SISTEMA

ISO/IEC 42001 / SISTEMA DE GESTIÓN DE IA



ESPECIALIZACIÓN

ISO/IEC 23894 / GESTIÓN DE RIESGO DE IA



FUNDACIÓN

ISO 31000 / GESTIÓN INTEGRAL DE RIESGOS

La norma no sustituye al gobierno.
Lo estructura



Marco integral de gobernanza de IA

PRINCIPIOS

CAPAS



Los principios marcan el rumbo... las capas convierten la gobernanza en acción.

Perú: el reloj regulatorio ya está corriendo



22 DÍAS
para el hito regulatorio

¿Qué debería estar haciendo una entidad financiera?

01 — INVENTARIAR

¿Dónde utilizamos IA?

02 — CLASIFICAR

¿Qué nivel de riesgo tiene cada uso?

03 — CONTROLAR

¿Qué medidas aplican sobre riesgos, datos, seguridad, transparencia y supervisión?

04 — EVIDENCIAR

¿Podemos demostrar quién responde y cómo se controla?

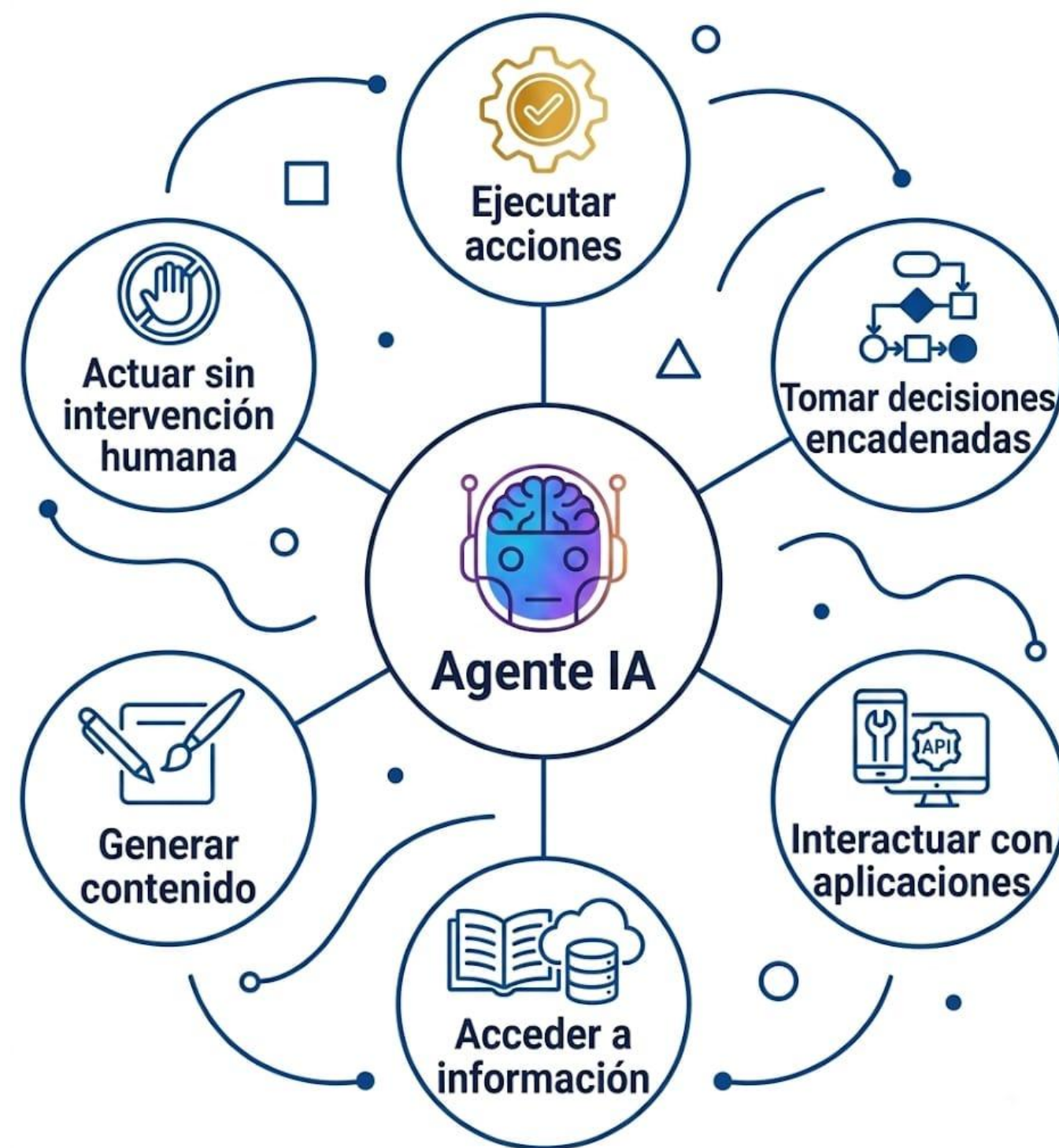
Para el sector financiero, el desafío es demostrar que el gobierno está funcionando

La gestión del riesgo de IA se integra al ERM



IA no es una nueva isla de riesgo.

La siguiente frontera: cuando la IA actúa

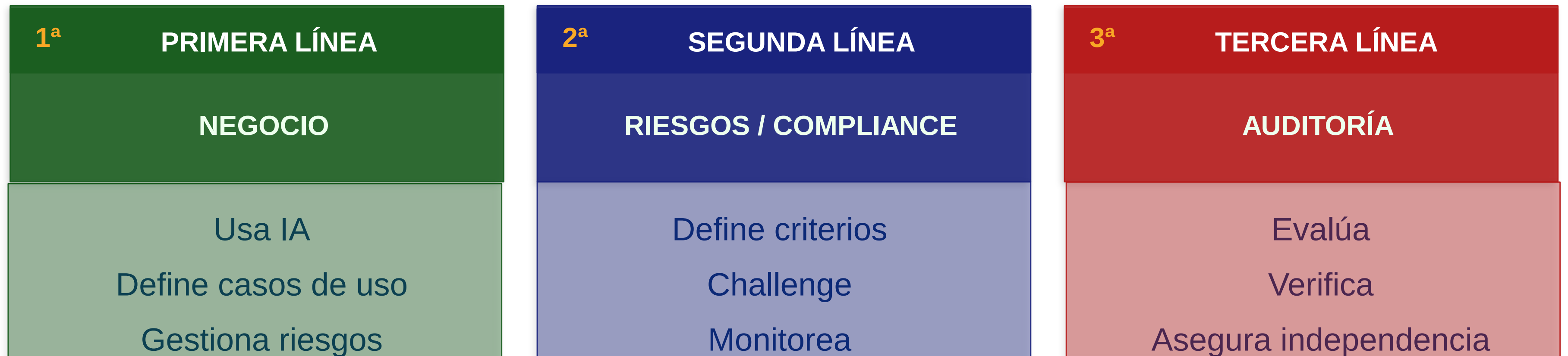


Ya no preguntamos solamente qué respondió la IA.

Preguntamos qué hizo.

¿Quién gobierna la IA?

Directorio / Alta Gerencia - define el tono y la responsabilidad



Tecnología habilita. El gobierno es empresarial.

Responsabilidad explícita



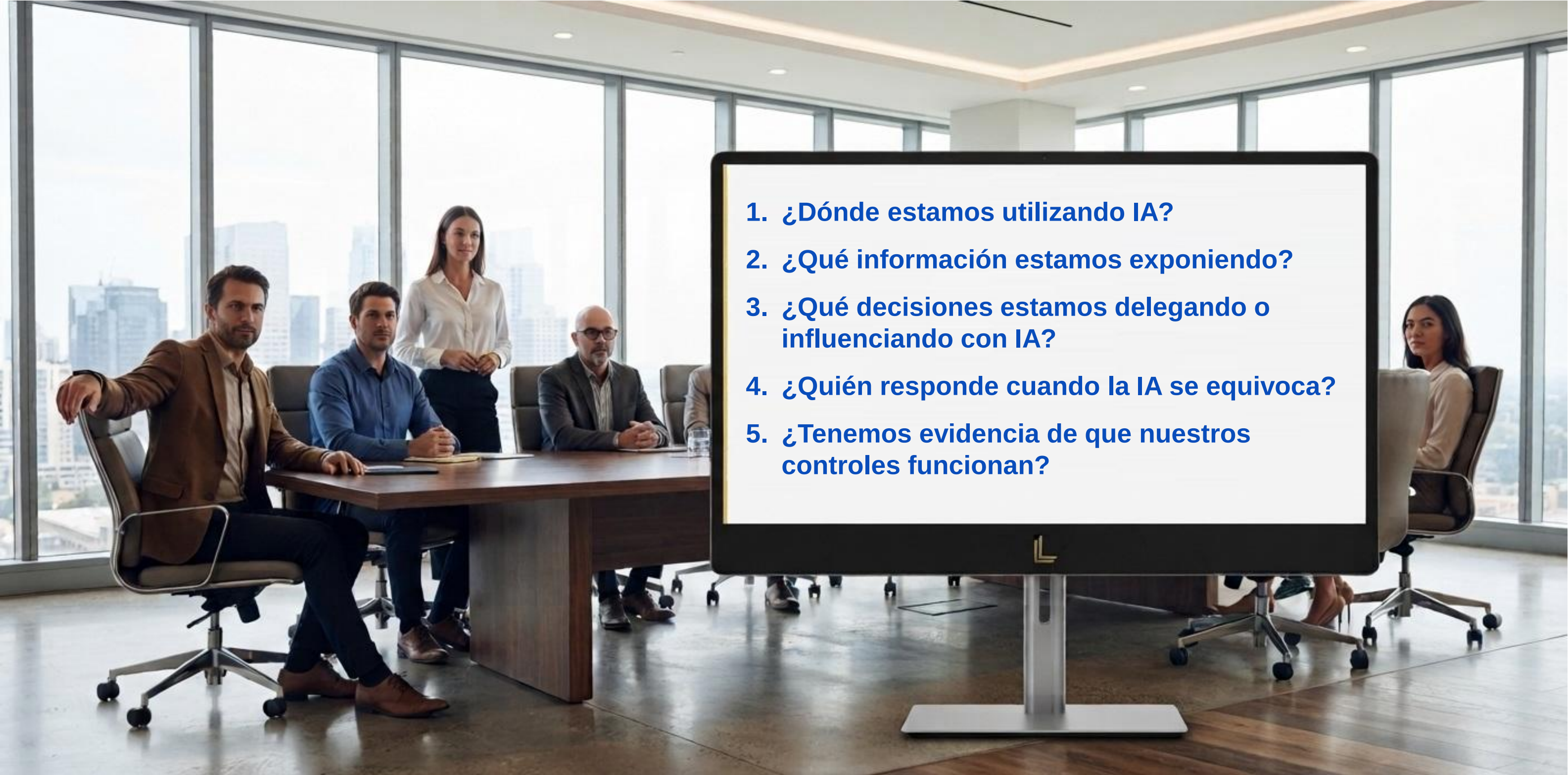
El accountability no se delega a la IA.

¿Dónde está hoy su organización?



**El objetivo no es controlar más.
Es poder escalar sin perder gobierno.**

5 decisiones que la Alta Dirección no debería delegar

- 
1. ¿Dónde estamos utilizando IA?
 2. ¿Qué información estamos exponiendo?
 3. ¿Qué decisiones estamos delegando o influenciando con IA?
 4. ¿Quién responde cuando la IA se equivoca?
 5. ¿Tenemos evidencia de que nuestros controles funcionan?

La Alta Dirección NO puede delegar estas decisiones.

Gracias



+51 993 576 943



Julissa.Vega@stamm.pe



www.stamm.pe