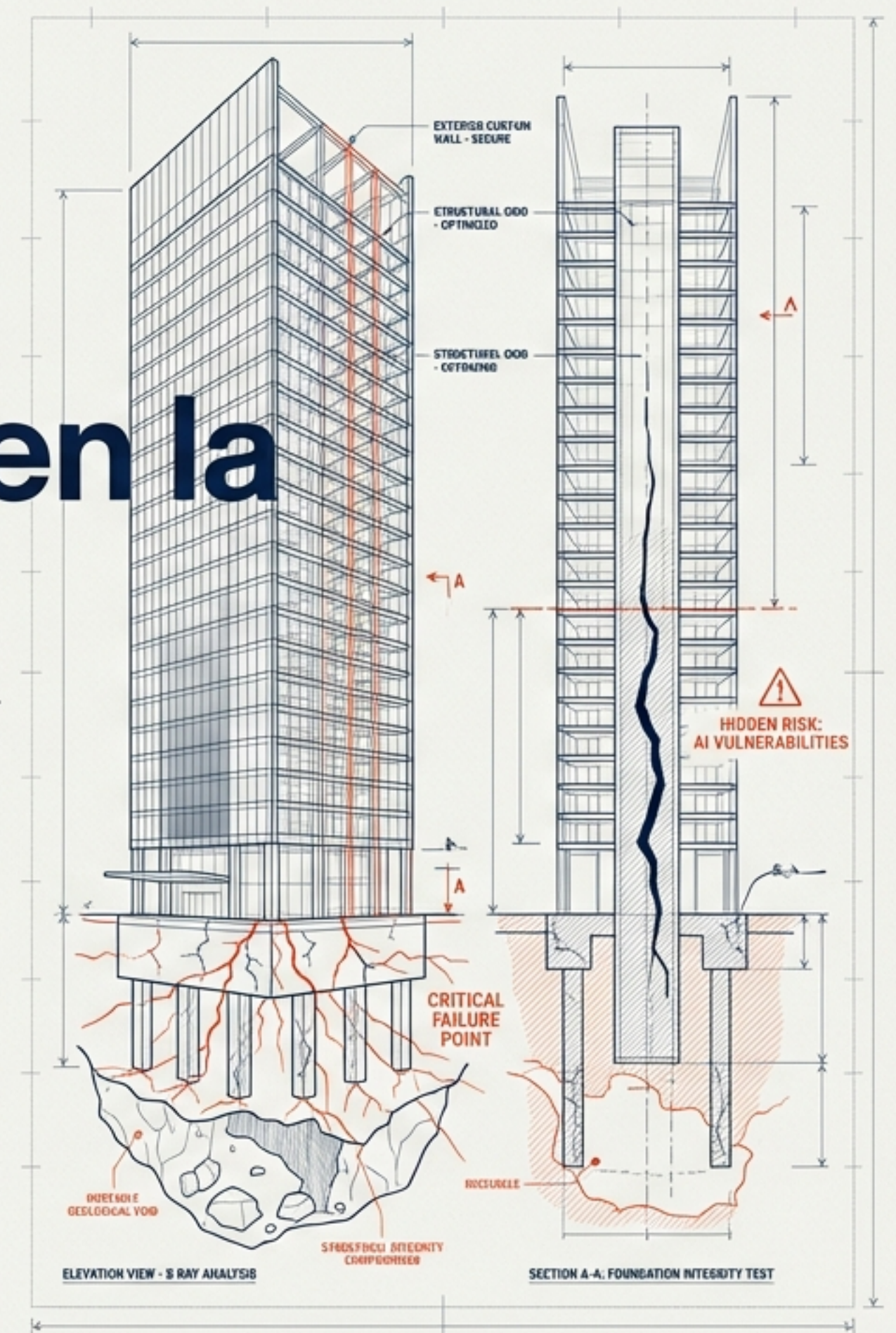


Riesgos de Seguridad en la Implementación de IA

Cuando la innovación introduce riesgos que el negocio no está viendo.

← — Risk Alert Orange →

Canal: Generando Cultura de Riesgos
ALGERisk Corporation

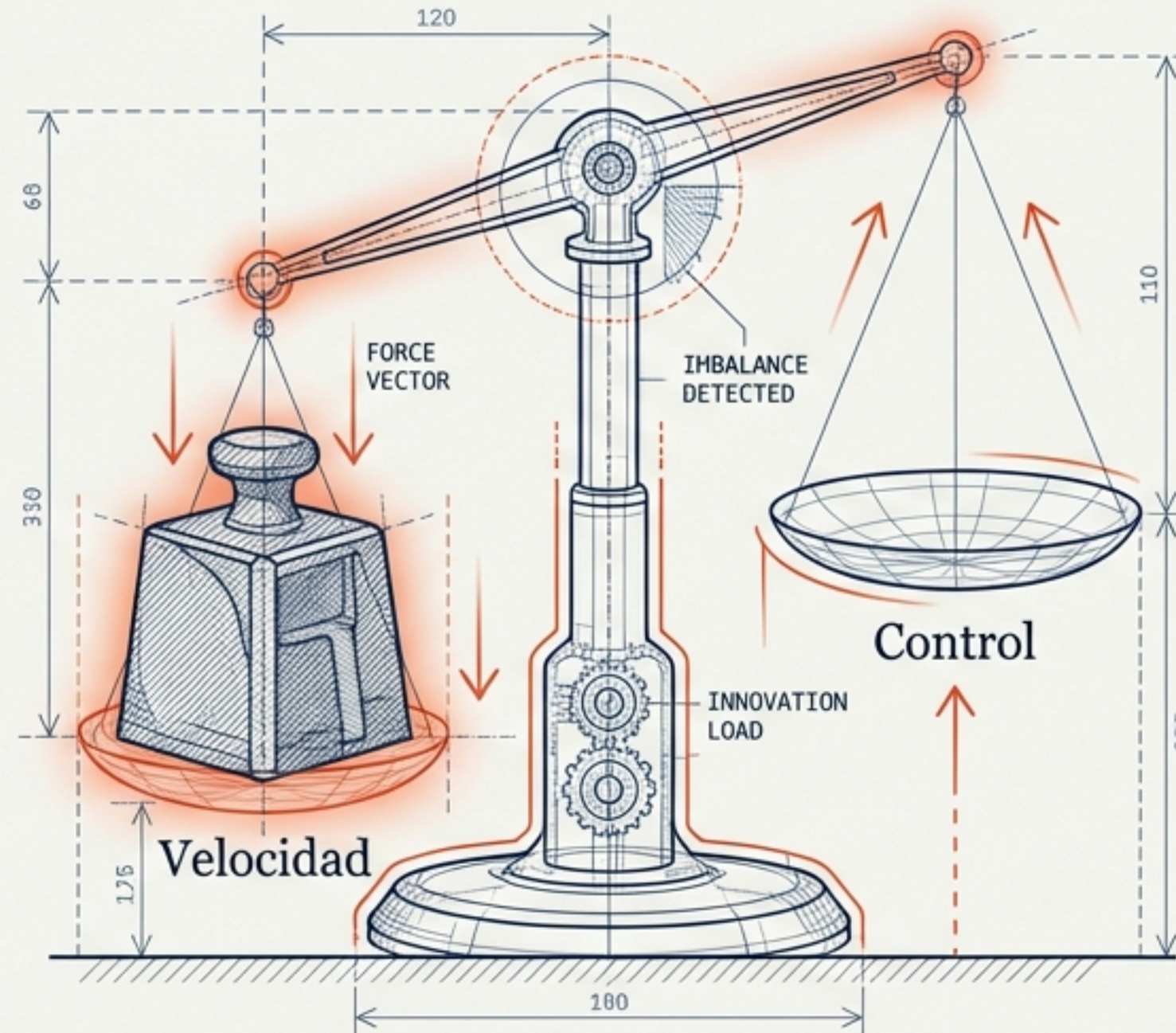


El Nuevo Vector de Riesgo: Innovación vs. Seguridad

El Contexto

La Inteligencia Artificial ya está entrando en procesos críticos de negocio:

- Decisiones crediticias.
- Atención al cliente.
- Detección de fraude y automatización operativa.

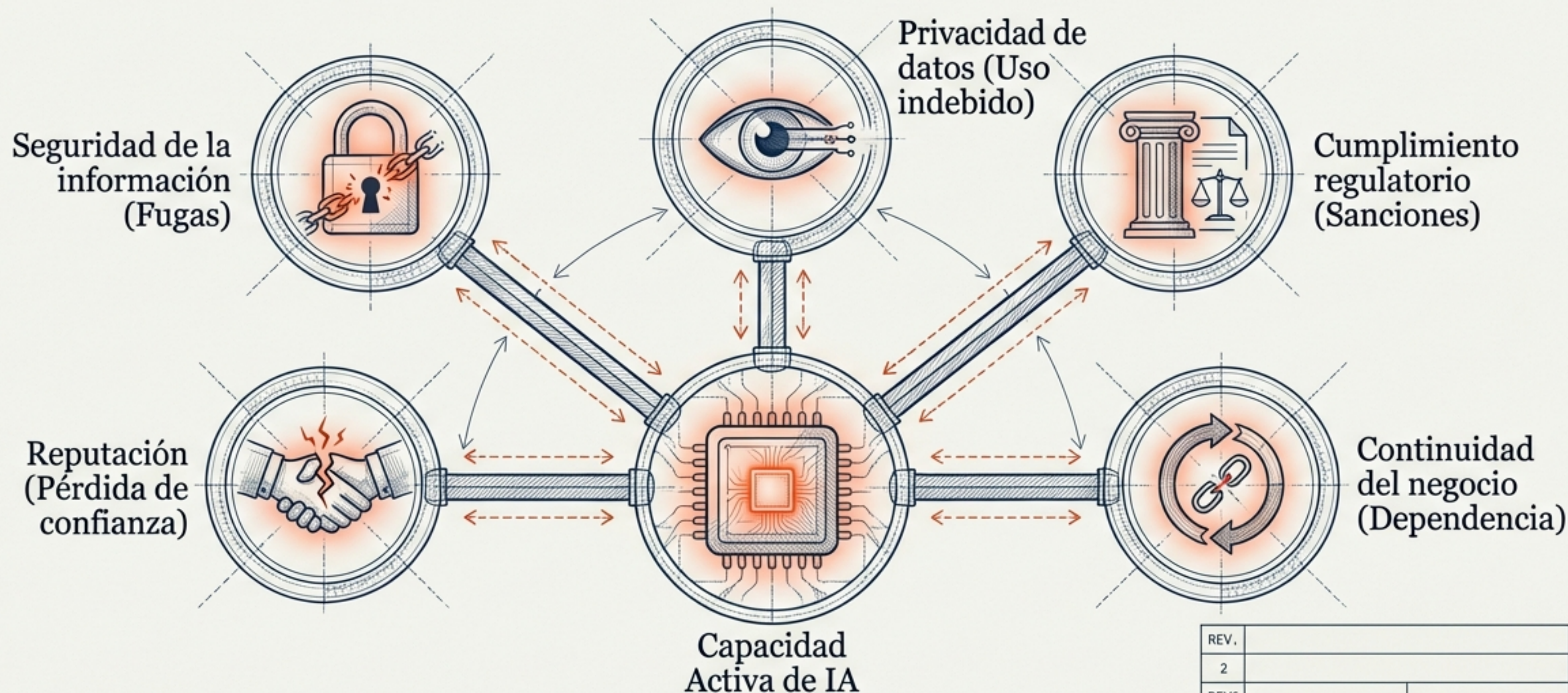


El Conflicto

Sin embargo, las organizaciones están operando bajo una “Lógica de Innovación” (velocidad, capacidad) en lugar de una “Lógica de Riesgo” (seguridad, control).

Tratar a la IA como un “riesgo tecnológico más” es un error estratégico.

La IA no es solo software: Es un Riesgo Transversal

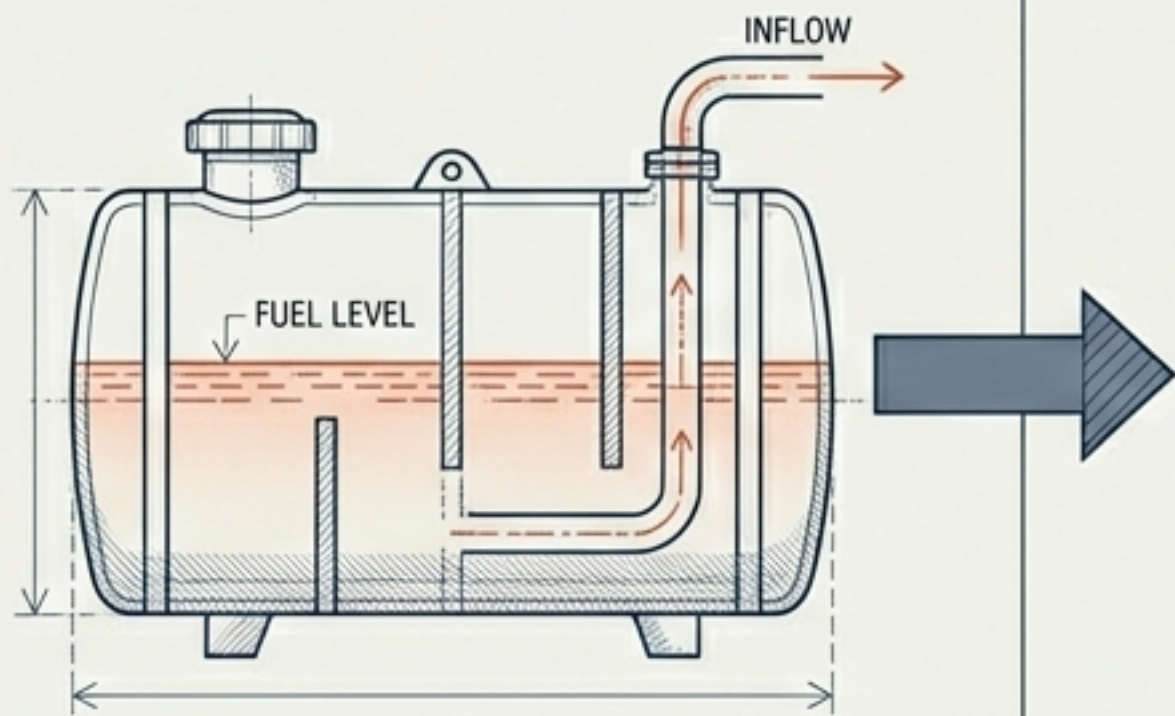


“El *riesgo* no está solo en el ataque, sino en *cómo se usa y gobierna la IA.*”

Los 3 Vectores de Riesgo Crítico

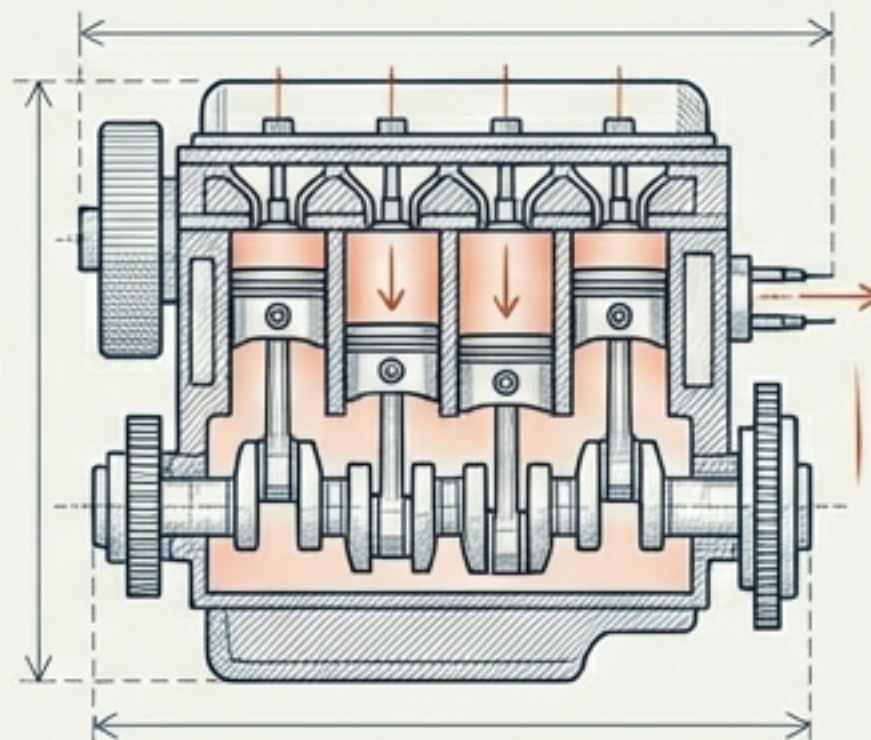
Un diagnóstico de las exposiciones ocultas.

Vector 1: Los Datos



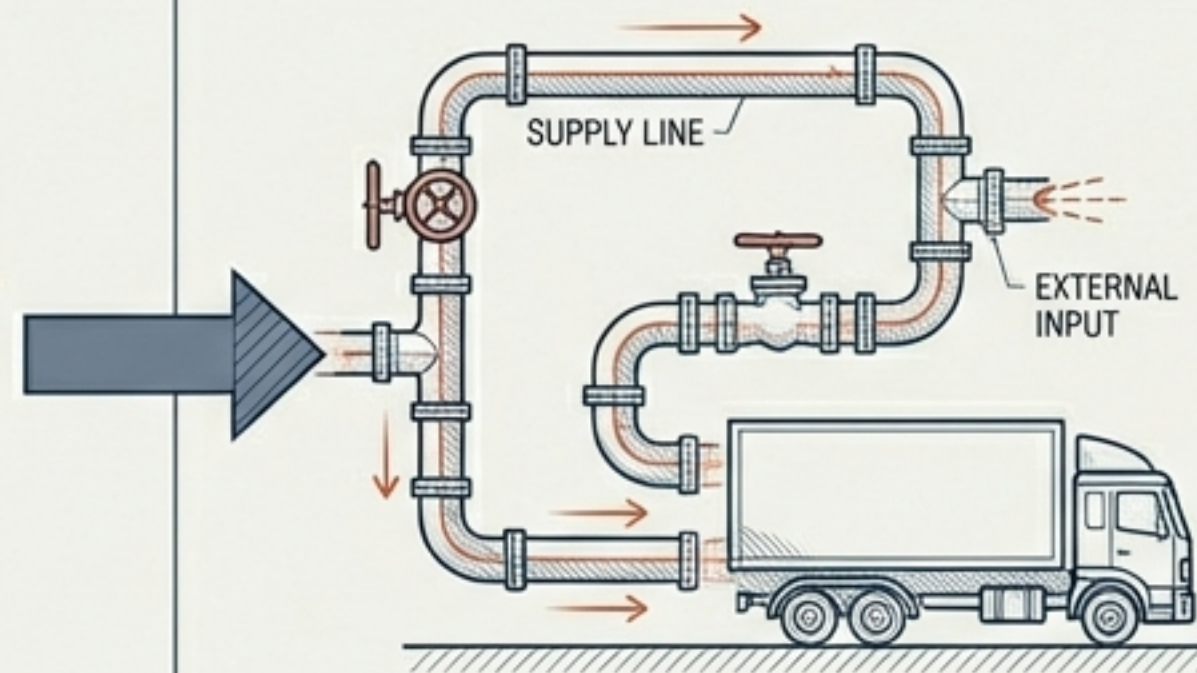
(El Combustible) – Riesgos de **privacidad**, **sesgo** y **fugas**.

Vector 2: La Caja Negra



(El Motor) – Falta de **explicabilidad** y **auditoría**.

Vector 3: Terceros



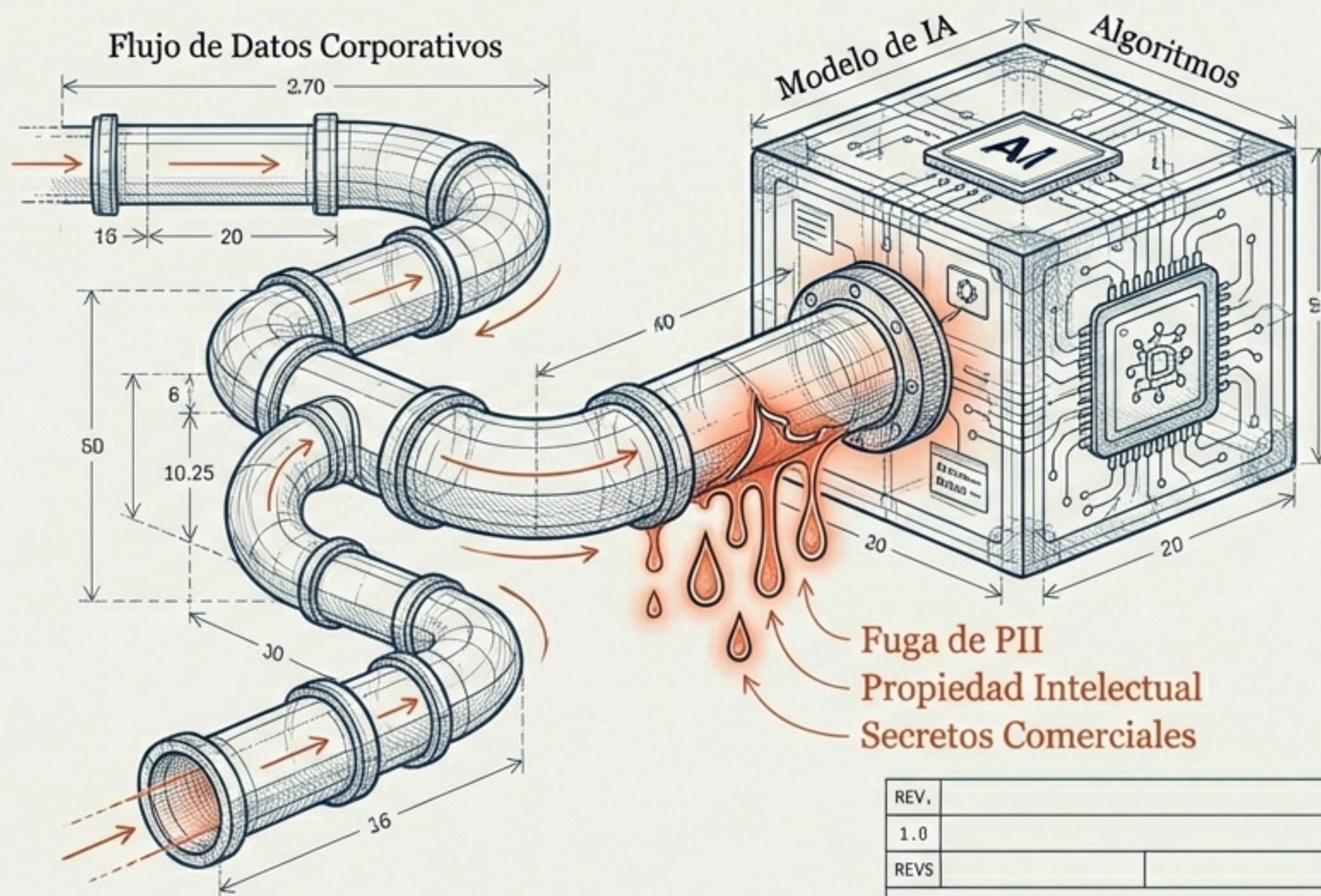
(La Cadena) – **Dependencia** de proveedores y modelos externos.

REV.		DATE
1.0		82/8/18
REVS		
PROJECT:		
AI RISK VECTORS		

Vector 1: Datos – El Activo Más Expuesto

La IA depende de datos, pero en muchos casos, la información no está preparada para este uso.

- **Datos Sensibles:** Uso de información confidencial sin controles.
- **Entrenamiento Deficiente:** Modelos alimentados con datos sesgados o incompletos.
- **Pérdida de Control:** Incertidumbre sobre el almacenamiento y procesamiento.



REV.		DATE
1.0		82/8/18
REVS		
PROJECT:		
AI RISK VECTORS		

Impacto de la Mala Gestión de Datos

La exposición de información confidencial en modelos externos es **irreversible**.

Incumplimientos Normativos



Violación de leyes de protección de datos locales e internacionales.

Sanciones Financieras



Multas financieras directas por negligencia en el manejo de datos.

Pérdida de Confianza



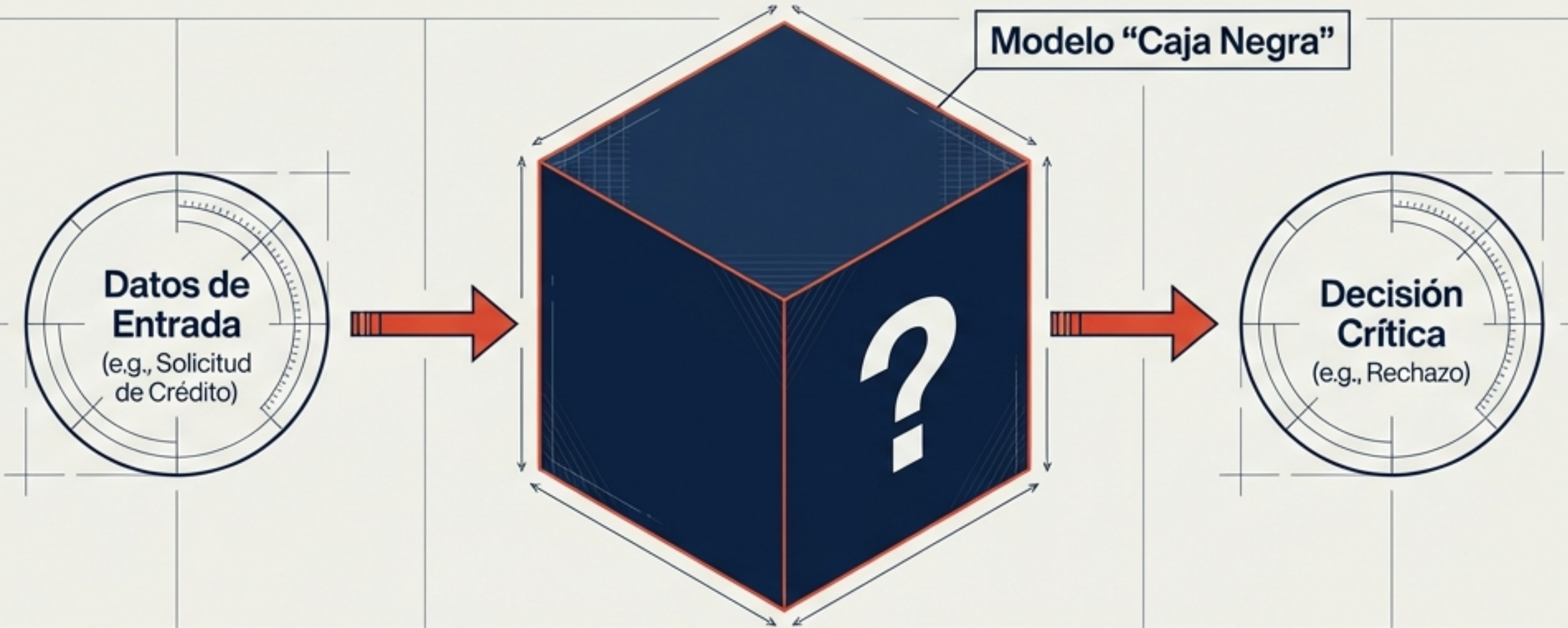
Daño reputacional cuando los clientes descubren que sus datos alimentaron una IA pública.

Consecuencia: Responsabilidad Civil y Penal.

REV.	DATE
1.0	82/8/18
REVS	

PROJECT: **AI RISK VECTORS**

Vector 2: Modelos No Explicables (Caja Negra)



Decisiones sin justificación.
A decisiones sin justificación. La decisión sin justificale, un arumerso de extunte explicar un ten. (e.g., Solicitud de Crédito).

Ausencia de trazabilidad lógica.
Ausencia de trazabilidad lógica. Lo contacte el maambia con prociones se habén; ausencia de crazabilidad lógica.

Imposibilidad de auditoría eficaz.
Imposibilidad de auditoría eficaz. Le auditoría desnes si no puedes explicalo, no puedes defenderlo legalmente.

“Si no puedes explicarlo, no puedes defenderlo legalmente.”

REV	DATE	PROJECT
		AI RISK VECTORS

El Dilema de la Auditoría y la Responsabilidad

Cuando la IA toma decisiones críticas, surgen preguntas que la tecnología no puede responder sola.



¿Quién responde?

(Responsabilidad legal y corporativa).

¿Cómo se explica el resultado?

(Transparencia ante el cliente/regulador).

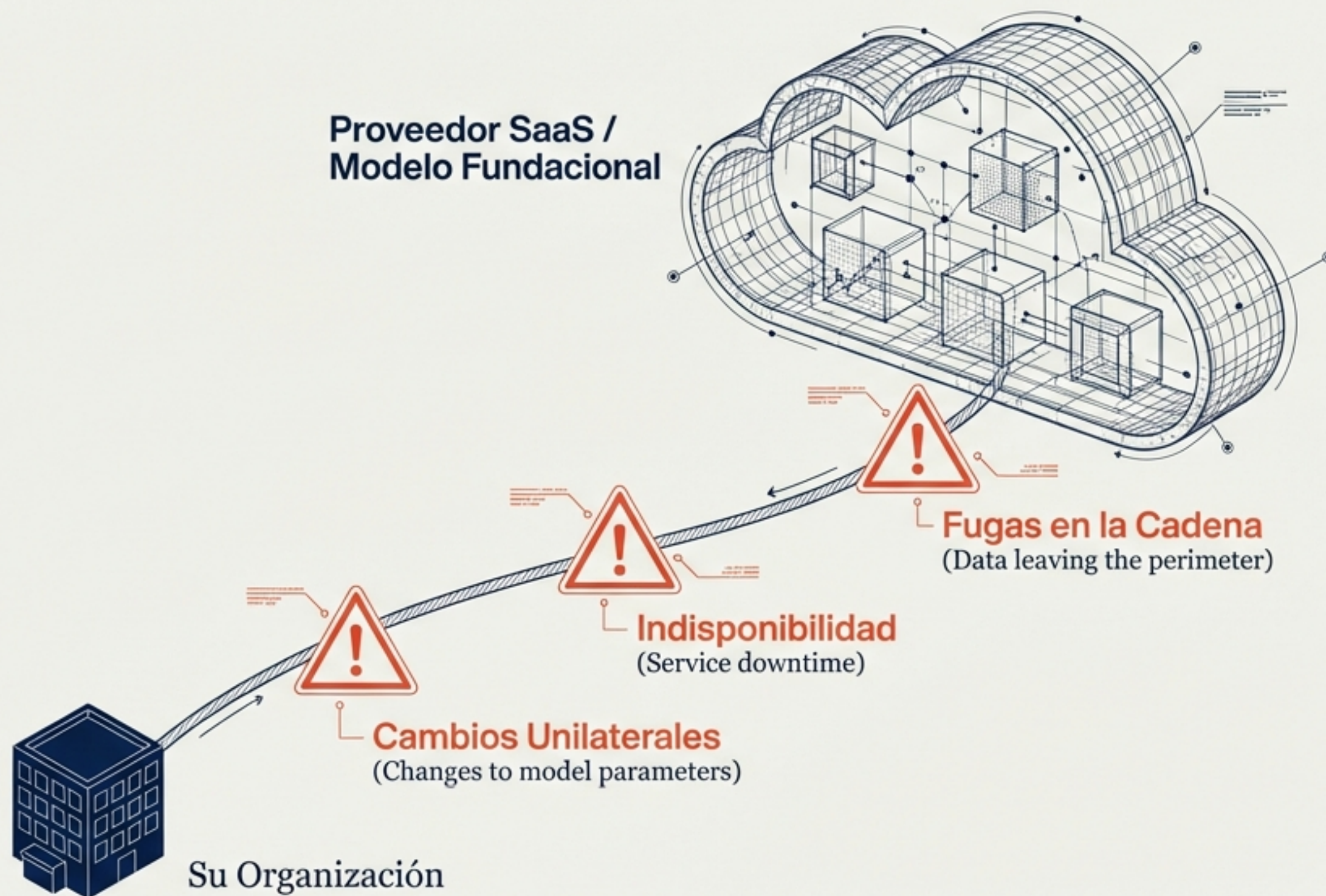
¿Cómo se corrige un error?

(Capacidad técnica de ajuste).

Sin explicabilidad, la IA se convierte en un riesgo legal y reputacional activo.

REV	DATE	PROJECT
		AI RISK VECTORS

Vector 3: Dependencia de Terceros y Modelos Externos



La mayoría de las soluciones se consumen “como servicio”, utilizando modelos que la organización no controla.

REV

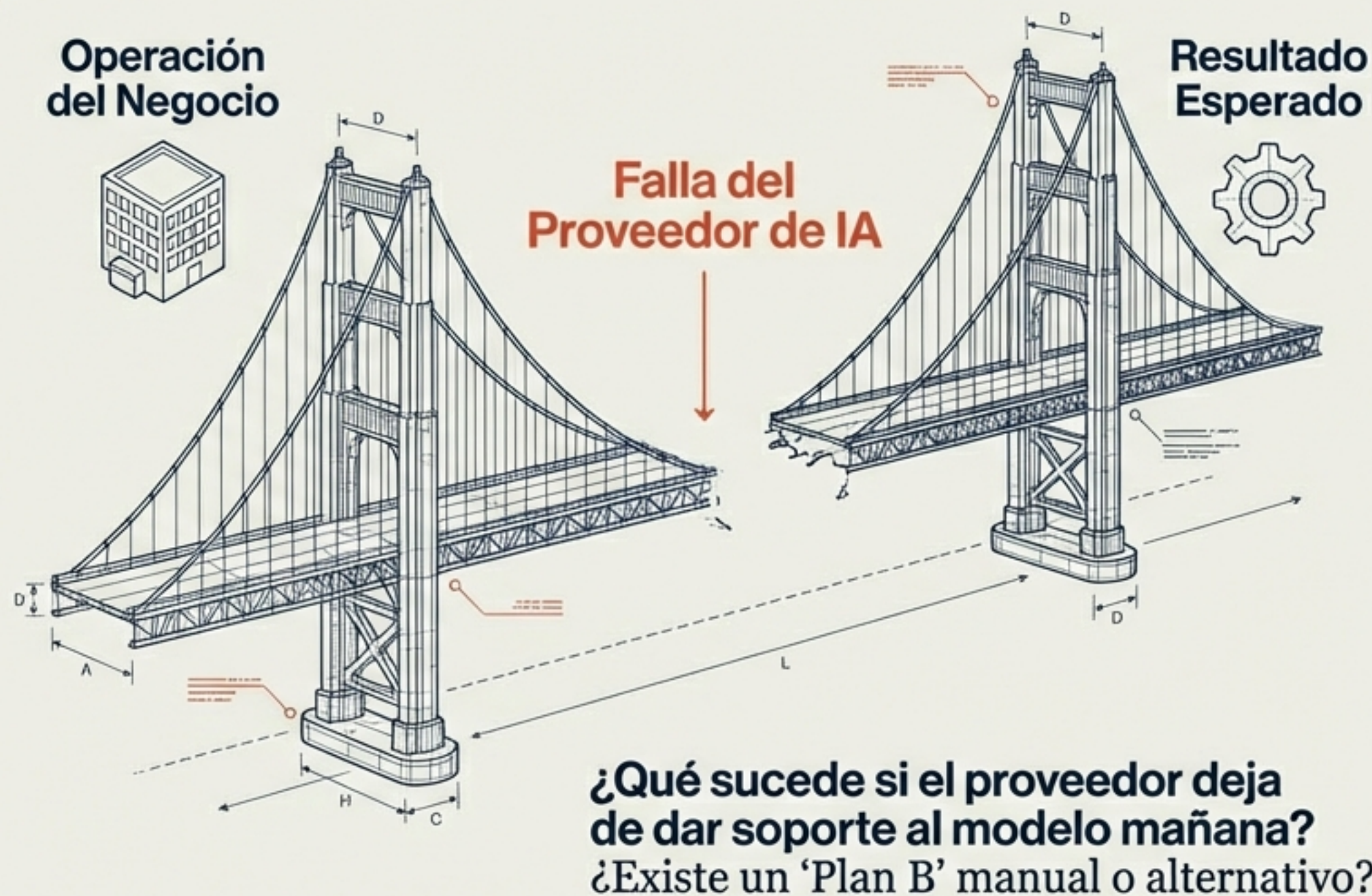
DATE

PROJECT

AI RISK VECTORS

Riesgos de Continuidad Operativa

La dependencia crítica de un proveedor externo sin un plan de contingencia es una falla de gobierno.

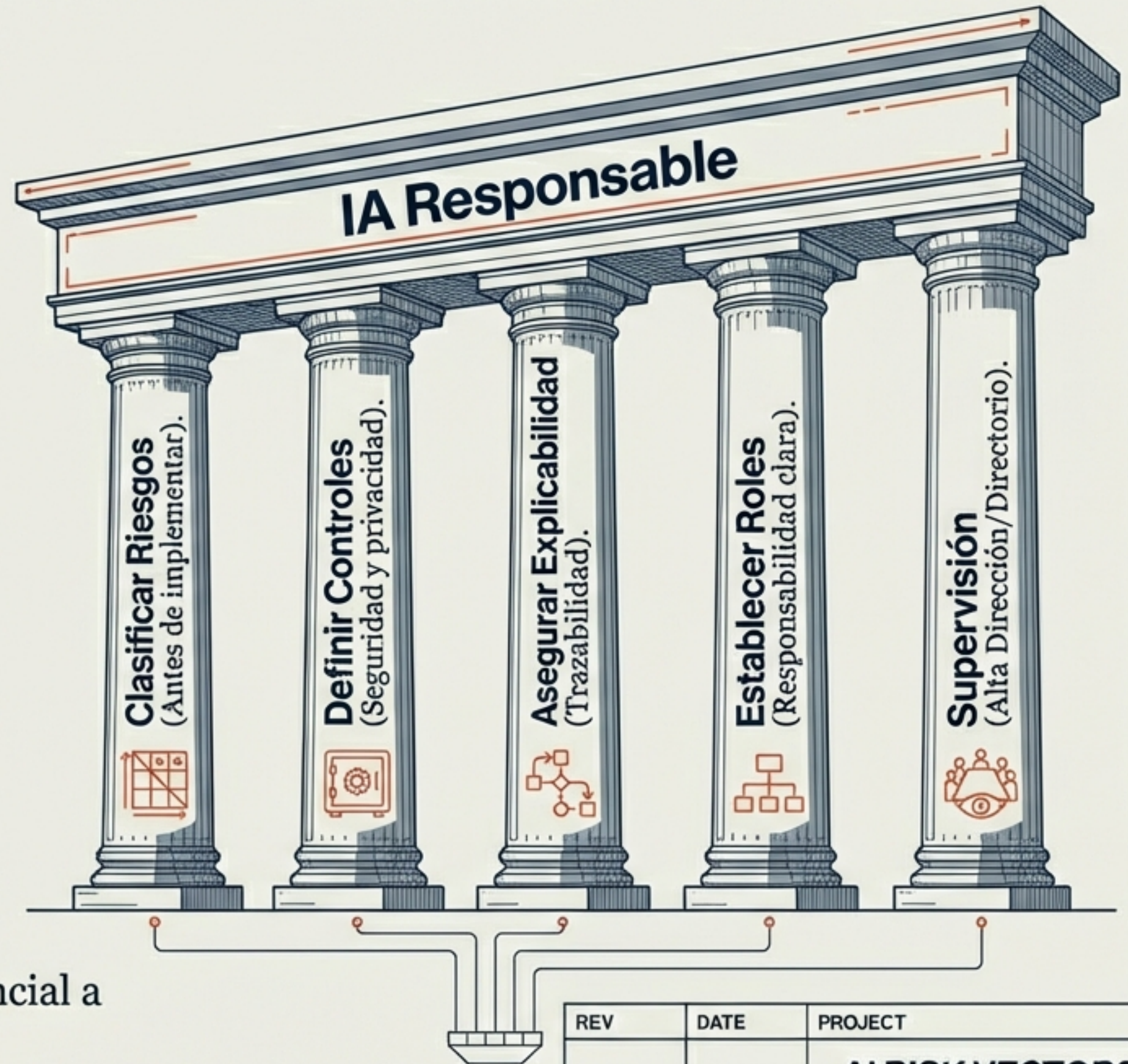


Aquí el riesgo no es tecnológico, es de continuidad y cadena de suministro.

REV	DATE	PROJECT
		AI RISK VECTORS

El Mandato: Seguridad y Gobierno de la IA

Implementar IA de forma responsable exige cinco pilares fundamentales:

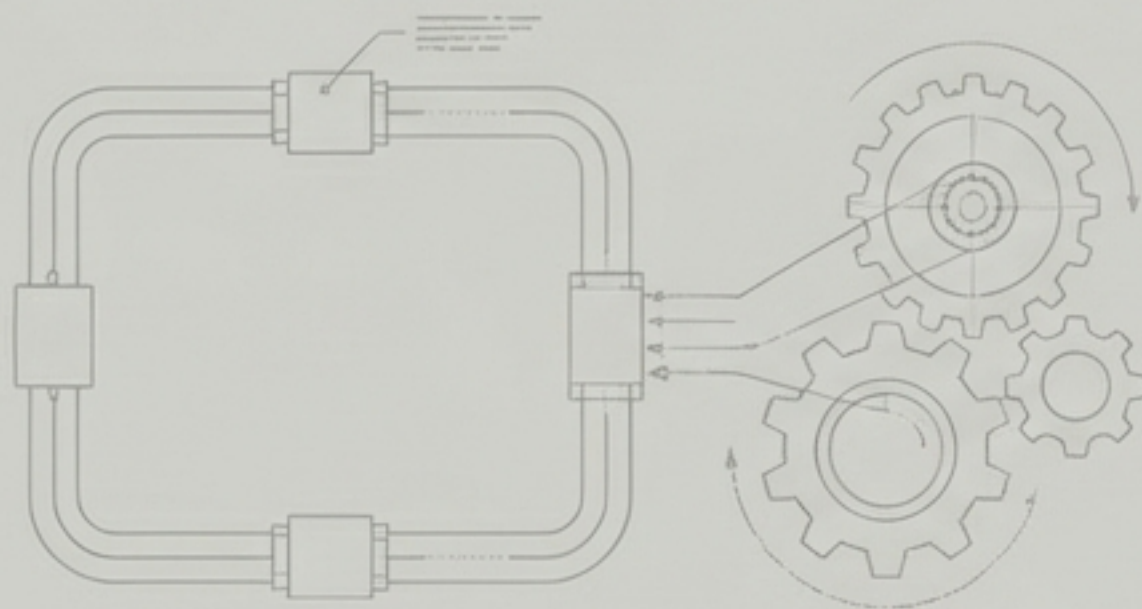


Estos pilares transforman la IA de un riesgo potencial a una ventaja competitiva sostenible.

La Nueva Pregunta Estratégica

La Pregunta Antigua:
¿La IA funciona?

(Enfoque puramente funcional)



La Nueva Pregunta:
¿Estamos dispuestos a asumir los riesgos que introduce esta IA?

(Enfoque de Gobierno)



La adopción de IA debe basarse en el apetito de riesgo de la organización, no solo en la disponibilidad tecnológica.

REV	DATE	PROJECT
		AI RISK VECTORS

Roles y Responsabilidades

La IA falla cuando se implementa sin gobierno.



REV	DATE	PROJECT
		AI RISK VECTORS

Conclusiones Clave

IA Bien Gobernada

Crea valor sostenible y ventaja competitiva.



IA Mal Gestionada

Crea riesgos y pasivos que el negocio no está preparado para enfrentar.

La innovación sin control no es estrategia, es azar.

REV	DATE	PROJECT
		AI RISK VECTORS

Generando Cultura de Riesgos

ALGERisk Corporation

www.algerisk.com
contacto@algerisk.com

REV	DATE	PROJECT
		AI RISK VECTORS