

# VI Congreso ISACA Iberoamérica

*Del 26 al 28 de mayo de 2026. Formato virtual*

## IA Y RIESGOS DIGITALES

Gobernar lo inesperado, proteger lo esencial.



## **Implementación práctica de Gobernanza de IA en Sectores Industriales: Experiencias y Lecciones desde México en el Marco de Estándares Internacionales**

Jorge Pedroza Rivera

# Jorge Pedroza Rivera

- Director en Cognitactix, empresa especializada en Calidad de Datos y Gobernanza en IA
- Ex Director de Gestión de Riesgos y Cumplimiento en PwC México +20 años en auditoría, gestión de riesgos y transformación digital
- Contador Público Certificado, UNAM | Pasante en Licenciado en Derecho, UNAM
- Maestría en IA Aplicada, Tecnológico de Monterrey
- Maestría en Energy Management, Tecnológico de Monterrey
- Consultor líder en gobernanza de IA para corporaciones industriales
- Autor de artículos sobre riesgos de IA, regulación y cumplimiento normativo



# Objetivos de la sesión

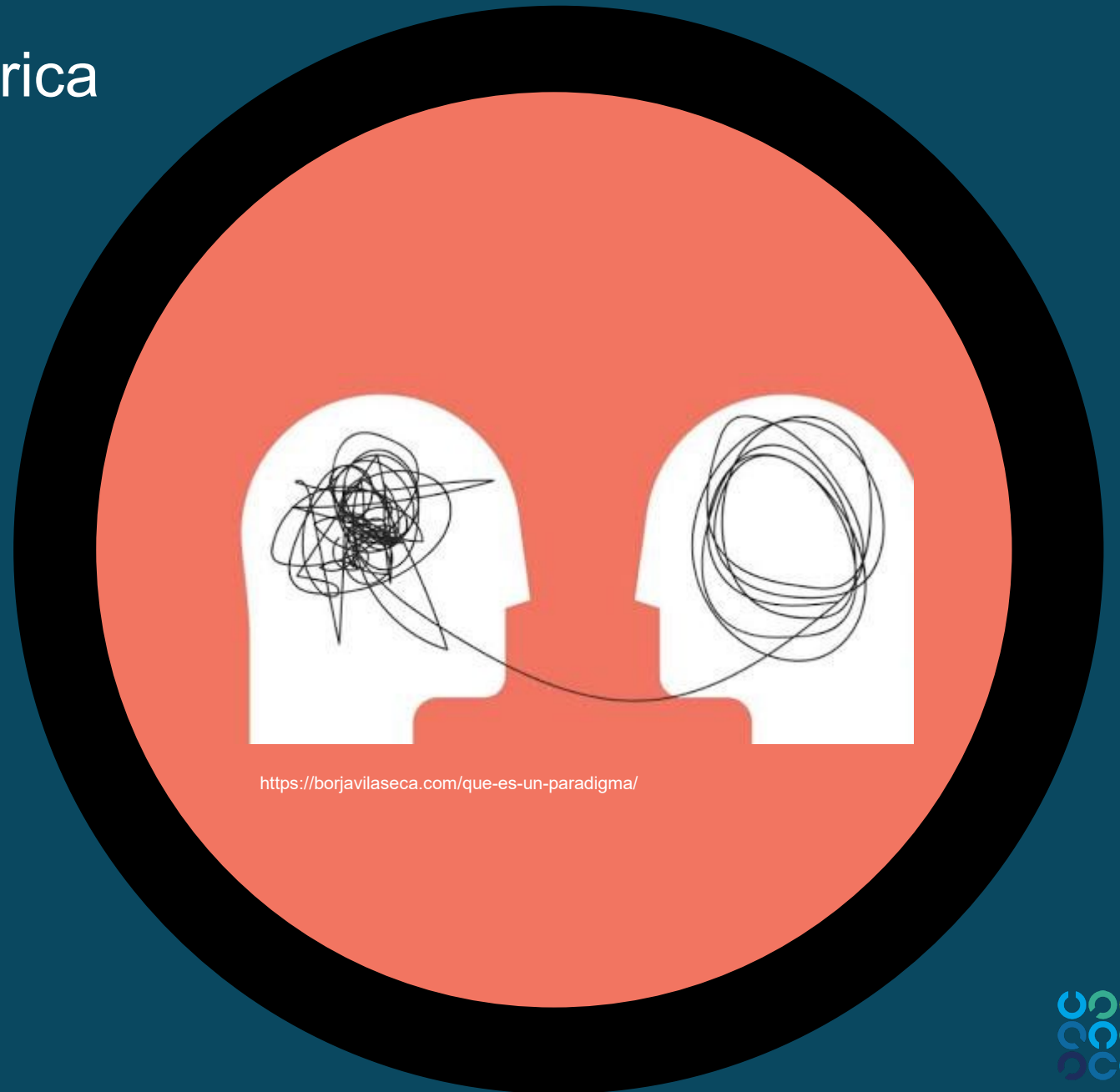
Compartir experiencias y casos de éxito de la implementación práctica de marcos de gobernanza de IA en corporaciones industriales mexicanas, integrando ISO/IEC 42001:2023, NIST AI RMF y EU AI Act (entre otros), con casos reales, abordando retos regulatorios y organizacionales específicos de LATAM.



# VI Congreso ISACA Iberoamérica

*Del 26 al 28 de mayo de 2026. Formato virtual*

## 10 Paradigmas en la Gobernanza de la IA



# Diez paradigmas en la Gobernanza de IA

01

“Vámos tarde en la adopción de IA...”

02

La IA es “ChatGPT”

03

El área responsable: TI

04

Las organizaciones no tienen gobernanza de IA

05

La adopción de Gobernanza es costoso...

06

“No hay ley... no hago nada...”

07

“Vámos tarde en la adopción de IA...”

08

La IA es “ChatGPT”

09

El área responsable: TI

10

“No choqué... me chocaron”

# Sentido de urgencia...

## Paradigma 1

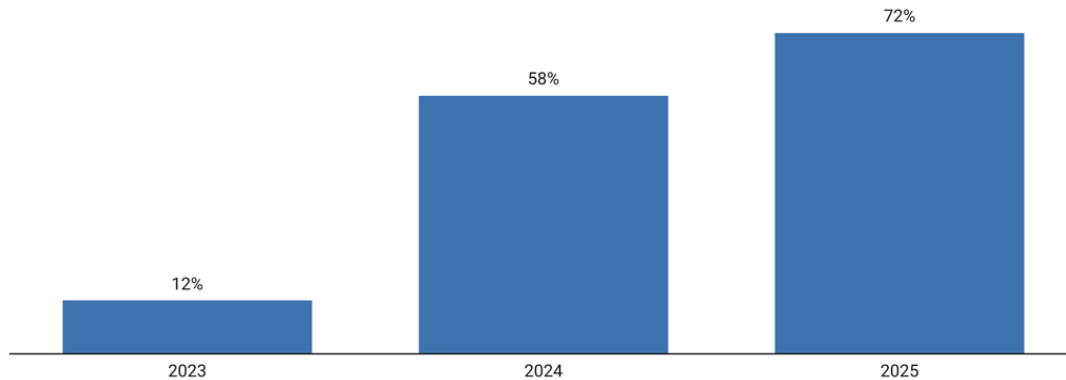
“Vámos tarde en la adopción de IA y en la implementación de gobernanza...”

# Paradigma 1: “Vámos tarde”

THE CONFERENCE BOARD



El 72% de las empresas del S&P 500 divulgan riesgos materiales relacionados con IA en informes 10-K (Oct 2025)



<https://www.conference-board.org/publications/AI-risk-disclosures-in-the-S-and-P-500-reputation-cybersecurity-and-regulation>



<https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai/>

- 88% de los encuestados confirman que ya tienen implementadas soluciones de IA...
- Una tercera parte afirma que las soluciones de IA han escalado a toda la organización. El resto sólo han hecho pequeños experimentos.



# Paradigma 1: “Vámos tarde”

Encuesta KPMG para México y Centroamérica: Las soluciones y sistemas de IA más utilizadas, son las relacionadas a la IA Generativa

Tecnología/Infraestructura	México
<b>Herramientas/aplicaciones de IA, incluida la IA generativa (IAGen)</b>	<b>38%</b>
Nube	25%
Sistemas/herramientas de gestión de datos estandarizados e integrados	17%
<b>Algoritmos de aprendizaje automático/aprendizaje profundo</b>	<b>8%</b>
Sistemas avanzados de ciberseguridad	8%
Métodos de analíticos avanzados	5%

- La mayoría de las organizaciones (41%) en ambas regiones tiene conocimiento de IA pero no ha desarrollado un caso de negocio.
- 1 de cada 4 organizaciones tiene una estrategia de IA completamente definida y alineada.

<https://kpmg.com/mx/es/sala-de-prensa/comunicados-de-prensa/2025/10/cp-empresas-en-mexico-y-centroamerica-apuestan-por-la-ia.html>



# Paradigma 1: “Vámos tarde”

## El 5% Exitoso:

- Pilotos de IA integrados
- Generando **millones en valor**
- Impacto medible en P&L

## El 95% Estancado:

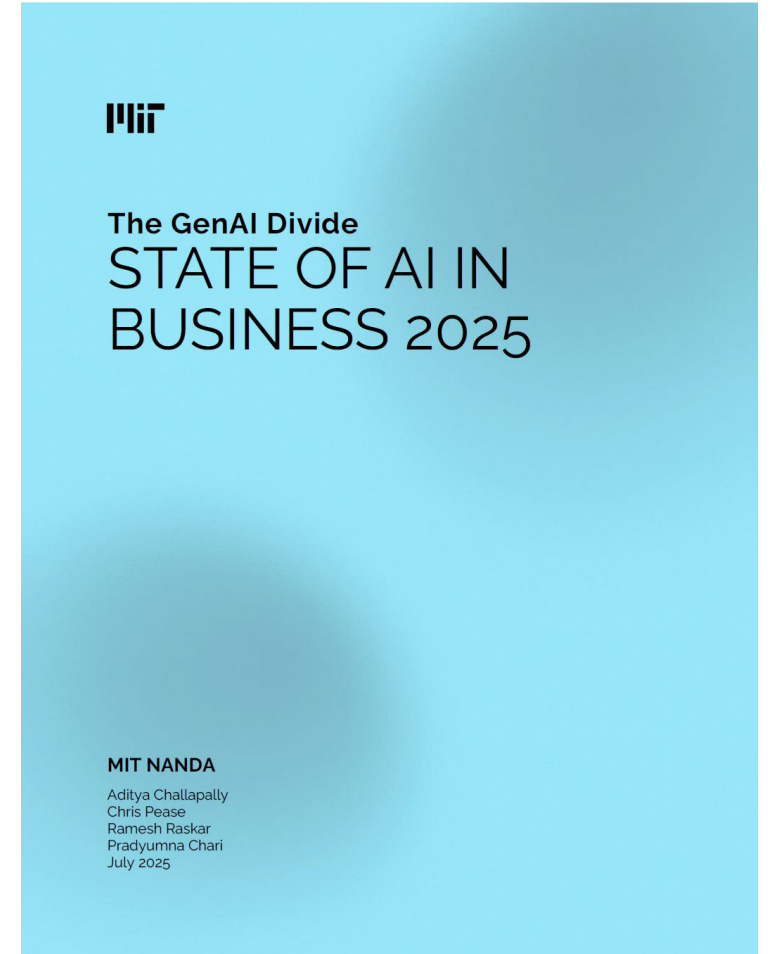
- Sin impacto medible en P&L
- Inversión sin retorno
- Proyectos que no escalan

## La causa raíz

**No es tecnología, es enfoque**

La brecha NO parece estar determinada por:

- Calidad de los modelos
- Regulación



Fuente: MIT, The GenAI State of AI in Business 2025



# Paradigma 1: Vámos tarde

De una muestra de 20 empresas en 7 bolsas a nivel mundial, se identifican algunos estándares en revelaciones de IA en información pública...

1

Las organizaciones usan la IA pero no lo revelan

2

Casi ninguna empresa tiene un responsable formal de IA

3

Ninguna empresa en la muestra, ha declarado adoptar los estándares globales de IA

4

Sector financiero muestra varios modelos a seguir en gobernanza de IA

5

Hay empresas que convierten la IA en producto y negocio

6

Hay empresas más abiertas sobre los riesgos de la IA

7

Hay empresas que no hacen ninguna mención de IA

8

No se revela cuánto dinero se invierte específicamente en IA

9

El sector bancario lleva ventaja en revelaciones de IA

**La IA es algo muy reciente... la organización no estaba preparada para ella... sólo lleva 75 años de existir...**

**Paradigma 2**

**La IA es “ChatGPT”**

# Paradigma 2: La IA es “ChatGPT”



# Paradigma 2: La IA es “ChatGPT”

La IA se puede dividir en tradicional y generativa: la primera encuentra un amplio número de aplicaciones actuales y sigue ofreciendo soluciones robustas de negocio.

IA TRADICIONAL	
<b>Machine Learning</b> Años 70's	Se pueden identificar conjuntos para clasificar datos (ej. identificar fraudes) y hacer proyecciones (ej. forecastings).
<b>Natural Language Process (NLP)</b> Años 90's	Se crean bibliotecas del lenguaje a partir de diferentes mecanismos de análisis de las palabras.
<b>Deep Learning</b> Años 2010	Se aprovecha el algoritmo de redes neuronales para procesar billones de datos e identificar patrones.
<b>Large Language Models (LLM's)</b> 2015	Es el mecanismo para predecir palabras y construir textos o hacer traducciones.

IA GEN	
<b>Transformer</b> 2017	Potencializa una la comunicación “casual” con las máquinas.
<b>Retrieval Aumented Generation RAG</b> 2020	Los modelos de IA utilizan información real seleccionada.
<b>Modelos de razonamiento (Omni)</b> 2024	Respuestas bajo un mejor escrutinio.
<b>Model Context Protocol (MCPs)</b> 2024	Conectividad de la IA Generativa a aplicaciones como email.
<b>Agentes IA</b> 2024	Tareas rutinarias ejecutadas autónomamente de principio a fin.
<b>IA Agentic</b> 2024	Coordinación de tareas de varios agentes.
<b>Small Language Models (SLM's)</b> 2025	Personalización de los modelos con info. real de las empresas.
<b>Open World</b> 2025	Obtención de información de entrenamiento a partir de IoT.



¿A quién le toca en las organizaciones dar el primer paso en una Gobernanza Formal de IA...?

Paradigma 3

El área responsable: TI

# Paradigma 3: El área responsable TI

## Nuevos riesgos específicos generados por la IA

Riesgo de ética y sesgo

Seguridad y confiabilidad

Seguridad y privacidad

Riesgo de gobernanza

Riesgo existenciales  
(con impacto a la sociedad)

### Evaluación de riesgos

- Evaluación de riesgos tradicionales + IA
- Monitoreo continuo
- Planificación de escenarios

## Riesgos transformados por la IA

Riesgo operacional

Ciberseguridad avanzado

Riesgo estratégico IA

Riesgo financiero amplificado por la IA

Riesgo de cumplimiento IA

### Mitigación de riesgos

- Controles híbridos
- Detección asistida por IA
- Supervisión humana

Amplificación de riesgos

Transformación de riesgos

### Marco de gobernanza

- Comités de ética de IA
- Equipos multifuncionales
- Auditorías regulares

## Riesgos tradicionales

Riesgo operacional

Riesgo financiero

Riesgo de ciberseguridad

Riesgo de cumplimiento

Riesgo estratégico

### Cumplimiento y monitoreo

- Tableros en tiempo real
- Reportes automatizados
- Seguimiento regulatorio

# Las organizaciones usan la IA... hay un nivel de gobernanza, pero: ¿cómo medirlo?

## Paradigma 4

“Las organizaciones no tienen gobernanza de IA”

VS

“Los colaboradores no usan la IA si la organización no la ha adoptado formalmente”

# Paradigma 4, “Las organizaciones no tienen gobernanza de IA”



## Identificación de hallazgos consistente...

- Ejecución de IA en procesos críticos de producción
- Carecen de política formal de uso responsable
- El Shadow AI es un riesgo constante...
- La falta de gobernanza incrementa la exposición a riesgos de ciberseguridad y protección de datos
- Las preocupaciones principales de los privacidad y seguridad de datos

La mayoría de organizaciones cuenta con:

1. Política de Ciberseguridad
2. Política de Protección de Datos
3. Sistemas Enterprise (Gobernanza a través de los sistemas del proveedor)

Una licencia de GenAI cuesta USD20 al mes... una prueba piloto en Python con open source todavía menos... pero un proyecto de gobernanza... cuesta una fortuna...

Paradigma 5

“Es costoso...”

# Paradigma 5: Es costoso

Llevar a cabo sesiones de sensibilización en la C-Suite, talleres de capacitación y desarrollo de casos de uso, acerca a la organización a un mejor entendimiento de:

1. Casos de uso
2. Riesgos asociados

Se debe de involucrar a toda la organización... para ello, la designación de champions hace más fácil su coordinación

## Actividades sugeridas:

1. Encuestas iniciales de percepción del uso de herramientas de IA

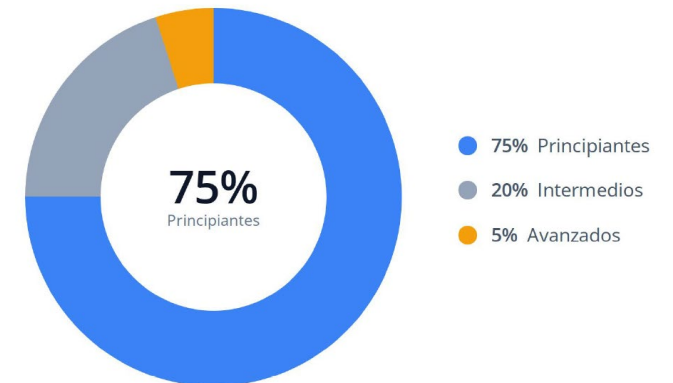
2. Obtención de retroalimentación en talleres

3. Evaluación de conocimientos

Es más caro no hacer nada, que dar pasos alineados a:

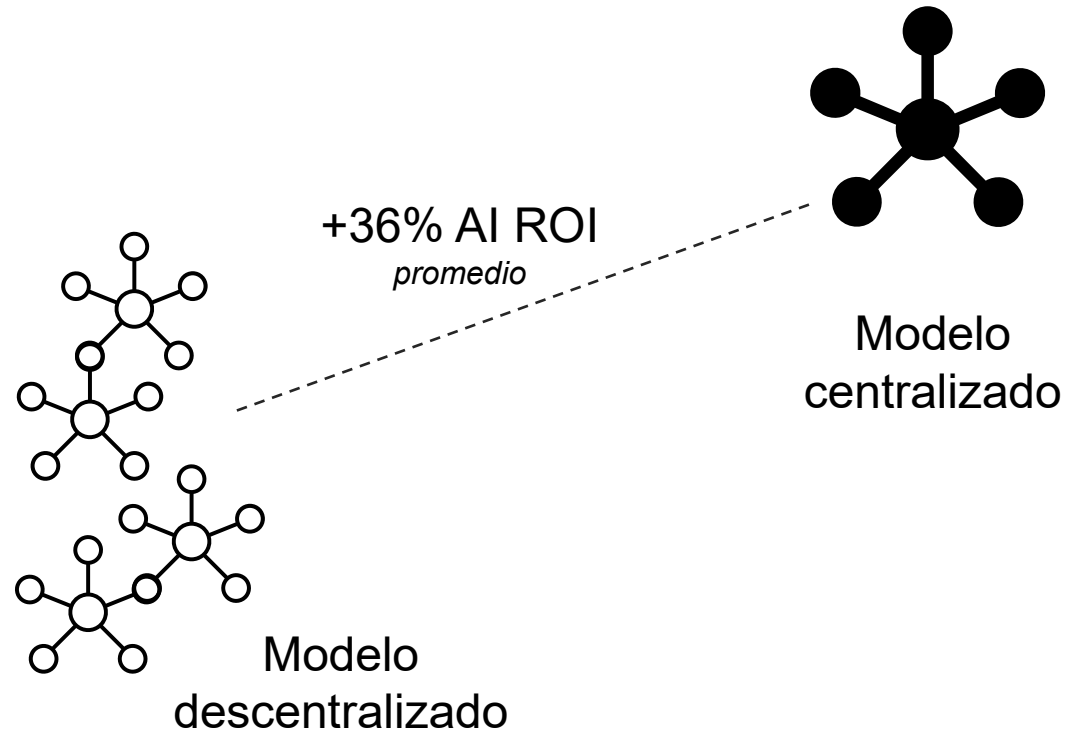
1. Cumplir los objetivos estratégicos
2. Lograr una mejor gestión del riesgo

## Percepción de entendimiento



# Paradigma 5: Es costoso

La estrategia de IA debe centrarse en: gobernanza (que incluye seguridad), ROI positivo y entrenamiento

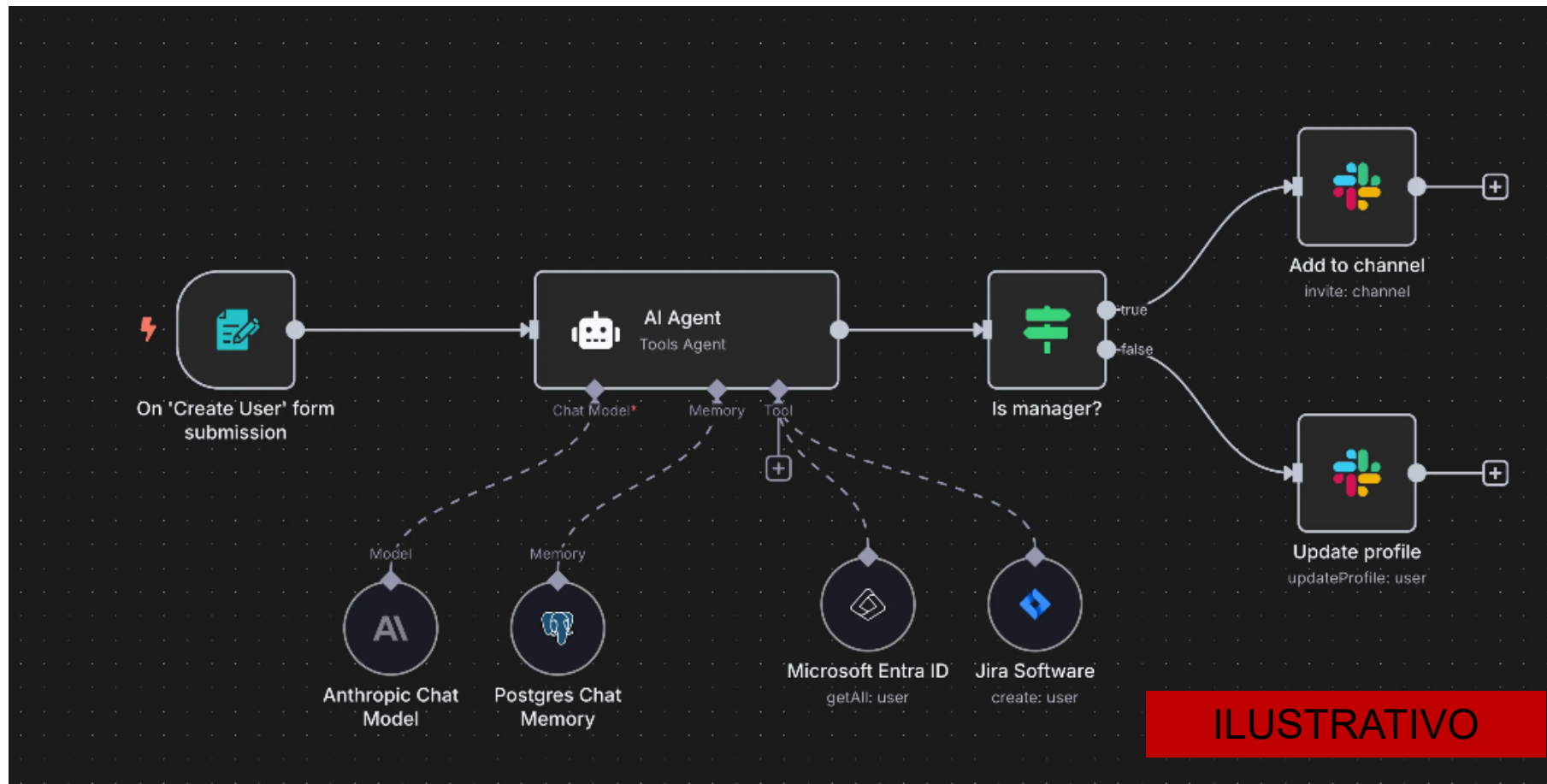


- Cuando la industria está siendo impactada por IA, es necesario contar con alguien que asegure las decisiones correctas.
- Las inversiones que se lleven a cabo en IA deben estar supervisadas de manera centralizada.

# Paradigma 5: Es costoso

CASO:

Ataque a través de un agente de IA para distribución de Ransomware



# ¿¿¿Cómo reaccionar a tiempo???

## Paradigma 6

“No hay ley... no hago nada...”

# Paradigma 6: No hay ley... no hago nada...

<b>87</b> Iniciativas de ley en 2025 (Mx)	<b>3</b> Modelos de regulación global	<b>0</b> Leyes y regulaciones obligatorias en México	<b>AI Act UE</b> Marco normativo de mayor influencia	<b>0</b> Árbitro técnico independiente INAI/IFETEL
--	--	---	---	---

## Auto regulación - Marcos de referencia

**Marco normativo vigente aplicable al uso de herramientas y sistemas de IA**

- Ley Federal de Protección de Datos Personales en Posesión de Particulares
- Ley Federal de Protección a la Propiedad Industrial
- Ley Federal del Derecho de Autor
- Código Penal de Procedimientos Penales (incluyendo la responsabilidad de las Personas Morales - Art. 421)
- Ley Federal del Trabajo
- Código de Comercio
- Código Fiscal de la Federación
- Entre otros

**Actualidad: Riesgo de Cumplimiento**

<b>Propiedad Industrial</b> Autoría y outputs generados por IA	<b>Derecho de Autor</b> Cont. generado · SCJN Amparo 6/2025
<b>Código Penal Federal</b> 18 iniciativas de reforma activas	<b>Ley Federal del Trabajo</b> Automatización · Derechos laborales
<b>Código Fiscal</b> Decisiones autom. con impacto fiscal	<b>Código de Comercio</b> Validez de actos comerciales con IA

 <b>ISO 42001:2023</b> Gestión de Riesgos y Gobernanza de IA	 <b>ISO 23894:2023</b> Gestión de Riesgos de IA	  
---	--	---

La estrategia óptima es implementar gobernanza interna (ISO 42001 + COSO GenAI) que anticipe la regulación y convierta el cumplimiento en ventaja competitiva, no en carga reactiva.



En un programa de socialización de Gobernanza en IA, podemos encontrar “resistencias naturales”...

## Paradigma 7

“Lo que no esta prohibido,  
esta permitido...”

# Paradigma 7: Lo que no esta prohibido, esta permitido...



Microsoft Stock Images

## Shadow AI

Shadow IA es el uso de herramientas y aplicaciones de IA por parte de los empleados sin la aprobación formal o la supervisión del departamento de TI.

**Aunque la política de la empresa frente la IA es “no usarla...” las personas la usan... y esto genera riesgos.**

# Paradigma 7: Lo que no esta prohibido, esta permitido...



Adobe Stock

## **Zero click attack**

Es un tipo de ciberataque en el que se explota una vulnerabilidad sin ninguna interacción del usuario, lo que significa que el objetivo no necesita hacer clic en un enlace o abrir un archivo.

**Es más fácil usar este ataque desde redes públicas no confiables o sin seguridad VPN**

**Tradicionalmente, se piensa en Gobernanza (políticas, lineamientos, etc.), como barreras burocráticas...**

## Paradigma 8

La Gobernanza es una barrera para la innovación

# Paradigma 8: La Gobernanza es una barrera para la innovación



- La Política de IA para habilitar y empoderar
- Hacer exigible a terceros los requisitos de seguridad
- Papel del Auditor Interno como consultor: Generación de valor
- Aplicación de metodologías y marcos de referencia para dar orden, estructurar y validar
- Alineación con los objetivos de negocio: ROI, Seguridad y escalabilidad

Se da el primer paso, pero ¿cómo saber hasta dónde llegar?

## Paradigma 9

Nos debemos de certificar en todo... o en nada...

# Paradigma 9: Nos debemos de certificar en todo... o en nada...

Un marco de gobernanza efectivo debe alinearse con estándares internacionales reconocidos y adaptarse al contexto regulatorio específico de cada organización

## **ISO/IEC 42001:2023** - Sistema de Gestión de IA

Marco integral para establecer, implementar, mantener y mejorar un sistema de gestión de IA.

## **ISO/IEC 23894:2023** - Gestión de Riesgos de IA

Guía específica para identificar, evaluar y tratar riesgos asociados a sistemas de IA.

## **COSO ERM 2017** - Gestión de Riesgos Empresariales

Integración de riesgos de IA en el marco general de gestión de riesgos corporativos.

## **COBIT 2019** - Gobernanza de TI

Objetivos de gobernanza y gestión aplicados a iniciativas de IA.

## **Marco ISACA de Auditoría de IA** - Aseguramiento

Metodología para auditar sistemas y controles de IA.

## **Ley de IA de la Unión Europea** - Cumplimiento Regulatorio

Requisitos legales con alcance extraterritorial y multas hasta 7% de facturación global.

# Paradigma 9: Nos debemos de certificar en todo... o en nada...

Existen diferentes niveles de madurez en el uso de sistemas y herramientas de IA



# Responsabilidad irrenunciable

## Paradigma 10

“No choqué... me chocaron”

# Paradigma 10: No choqué... me chocaron

Entender el algoritmo y que la responsabilidad siempre corresponde a una persona...

## Monitoreo oportuno

Identificar fallas incluso antes de la implementación

## Dar confianza en las salidas/ resultados

Resultados seguros, justos, legales y que funcionen como fueron diseñados

## Mantener los datos y la Propiedad Intelectual protegida

Sin fugas de información y sin entrenamiento en datos no conocidos

## Validaciones mínimas en los lugares correctos

Revisiones sencillas antes de pasar a productivo

## Habilitación de la intervención humana

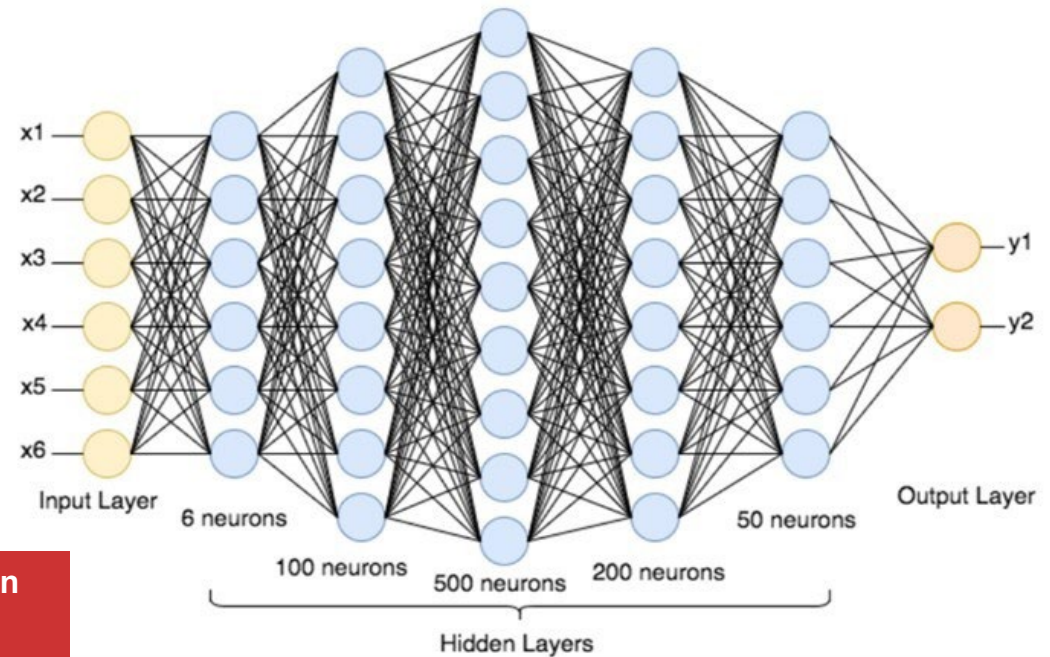
Las personas pueden revisar, corregir o detener los sistemas y herramientas

## Ayudar a los equipos a determinar qué está bien y qué no

Dar guía clara y evitar suposiciones

## Ser claro en quién es el dueño y cuáles son los resultados

Designar a una persona como responsable a cada sistema o herramienta



# Diez paradigmas en la Gobernanza de IA

01

“Vámos tarde en la adopción de IA...”

02

La IA es “ChatGPT”

03

El área responsable: TI

04

Las organizaciones no tienen gobernanza de IA

05

La adopción de Gobernanza es costoso...

06

“No hay ley... no hago nada...”

07

“Vámos tarde en la adopción de IA...”

08

La IA es “ChatGPT”

09

El área responsable: TI

10

“No choqué... me chocaron”

# Diez paradigmas en la Gobernanza de IA

01

“Vámos tarde en la adopción de IA...”

07

“Vámos tarde en la adopción de IA...”

02

03

04

**Paradigmas:  
Eliminados!!!**

05

La adopción de Gobernanza es costoso...

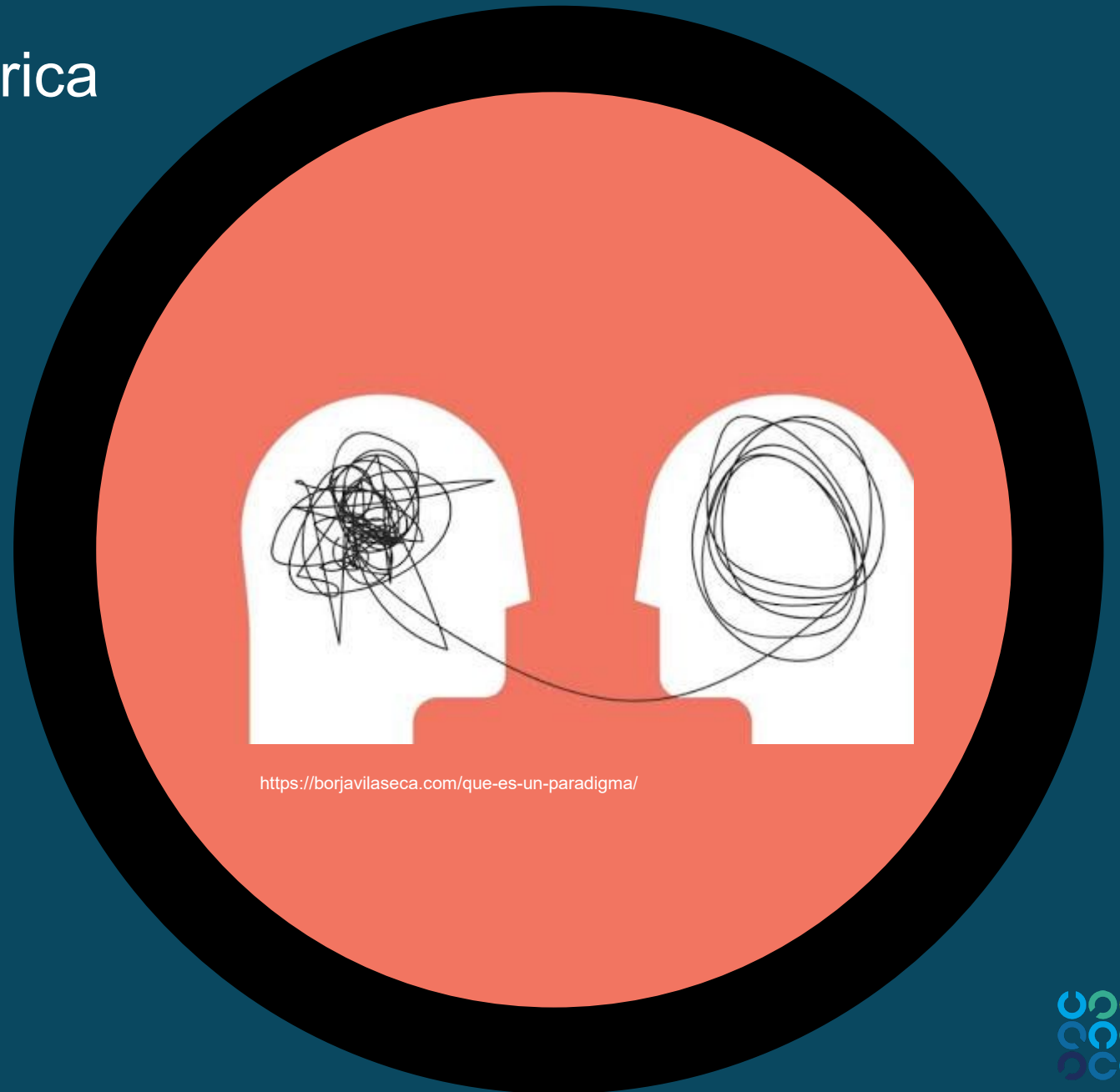
06

“No hay ley... no hago nada...”

# VI Congreso ISACA Iberoamérica

*Del 26 al 28 de mayo de 2026. Formato virtual*

## Q&A



Si quieres poder para hacer el bien... entonces  
más personas necesitan tener poder.

*Jeffrey Pfeffer*

**¡Sigamos en  
contacto!**



**Jorge Pedroza**  
27 de mayo, 2026

<https://www.linkedin.com/in/jorgepedrozarivera/>