

“El valor de la IA Generativa y de la IA Agéntica: Retos y oportunidades”

Mayo, 2026



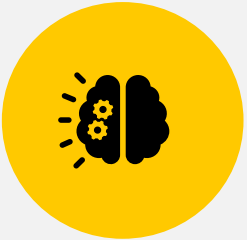
Contenido

03	Taxonomía básica
11	Visión: adopción, complementariedad y eficiencia
13	Del prompt engineering al context engineering
14	Human in the loop vs Human in the front
15	Stack tecnológico de IA
18	Riesgos de la IA
20	Negocios autónomos
21	Costos de la IA

Taxonomía básica

IA Tradicional

Optimizar decisiones a través del análisis de datos



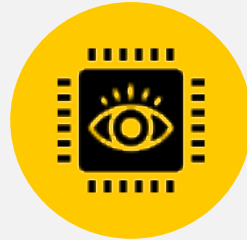
Machine learning

- Asociación, segmentación, predicción, pronósticos y clasificación
- Redes neuronales



Optimización

- Razonamiento basado en restricciones
- Programación lineal y no lineal



Visión computacional

- Reconocimiento facial
- Reconocimiento de gestos



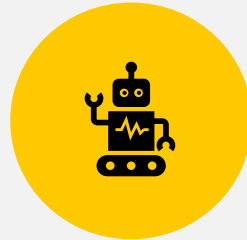
Procesamiento de lenguaje natural

- Entendimiento del lenguaje
- Chatbots y avatares



Lógica computacional

- Sistemas basados en reglas
- Inferencia lógica



Robótica

- Robots de almacenes
- Ensamblado inteligente

IA Generativa

Generar contenido original (datos, imágenes, videos, lenguaje, código, diseños)



Modelos fundacionales

- Asistentes virtuales
- Datos sintéticos



Modelos de dominio

- Asistente de programación
- Generación de contenido de marketing

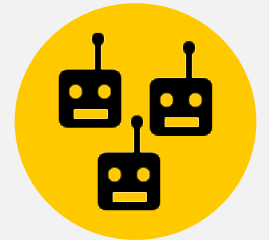
IA Agéntica

Tomar decisiones de forma autónoma



Agentes IA

- Planificadores
- Guardianes

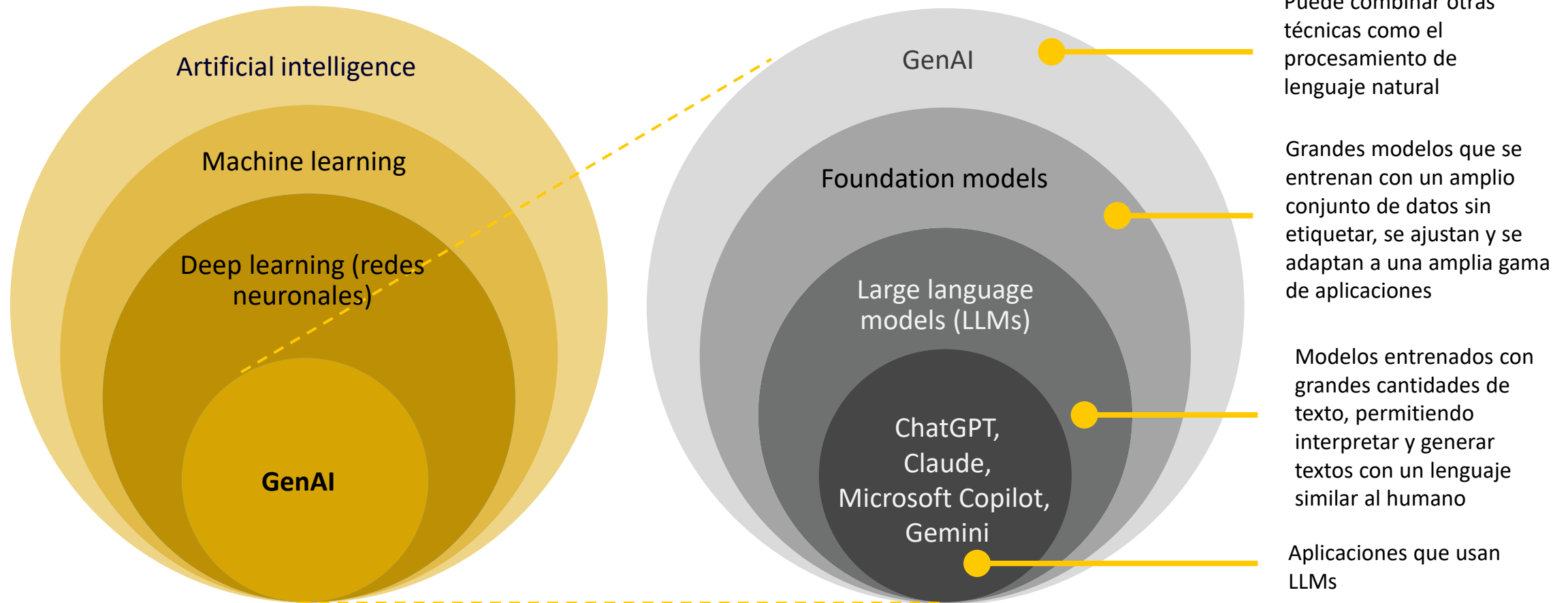


Sistemas multi-agente

Combinaciones de planificadores, con guardianes, expertos y orquestadores

Taxonomía básica

¿Dónde están ChatGPT, Claude, Microsoft Copilot y Gemini?



Taxonomía básica

¿Cuál es la diferencia entre IA Generativa e IA Agéntica?

IA Generativa



Preguntas y te responde

Genera una respuesta estática a una consulta basada en su entrenamiento y en el conocimiento disponible

Usuario: “¿Cómo actualizo mi dirección de facturación?”

IA: “Ve a Configuración > Cuenta > Facturación...”

IA Agéntica



Preguntas y **actúa**

Toma acciones autónomas a través de sistemas y canales para completar tareas en nombre del usuario

Usuario: “Actualiza mi dirección de facturación a 12, Main St.”

IA: “**Listo, acabo de enviarte un correo de confirmación**”

Taxonomía básica

Artefactos de negocio creados hoy por IA Generativa



Audio/Visual

- Rostros/cuerpos 2D/3D
- Arte a partir de *prompts* de texto (y viceversa)
- Fotografías, dibujos, videos, música, canciones
- Voz / personajes visuales



Programación y Activos de Datos

- Anotación y procesamiento de datos
- Datos de prueba y sintéticos
- Generación de código y actualización de código heredado
- Datos de contexto (por ejemplo, condiciones de mercado)



Lenguaje Natural

- Preguntas / respuestas
- Resúmenes
- Historias / narrativas
- Documentos
- Ofertas de empleo
- Descripciones de productos
- Atención / contacto con clientes



Diseños

- Diseños de producto
- Materiales
- Modelos 3D
- Optimización de manufactura
- Flujos de proceso
- Especificaciones / esquemas (ej. medicamentos, infraestructura y edificios, edición de películas)



Herramientas Estratégicas

- Pronósticos
- Estrategias de juego no programadas
- Escenarios estratégicos no anticipados
- Simulación enriquecida con IA Generativa
- Orquestación de tareas y equipos

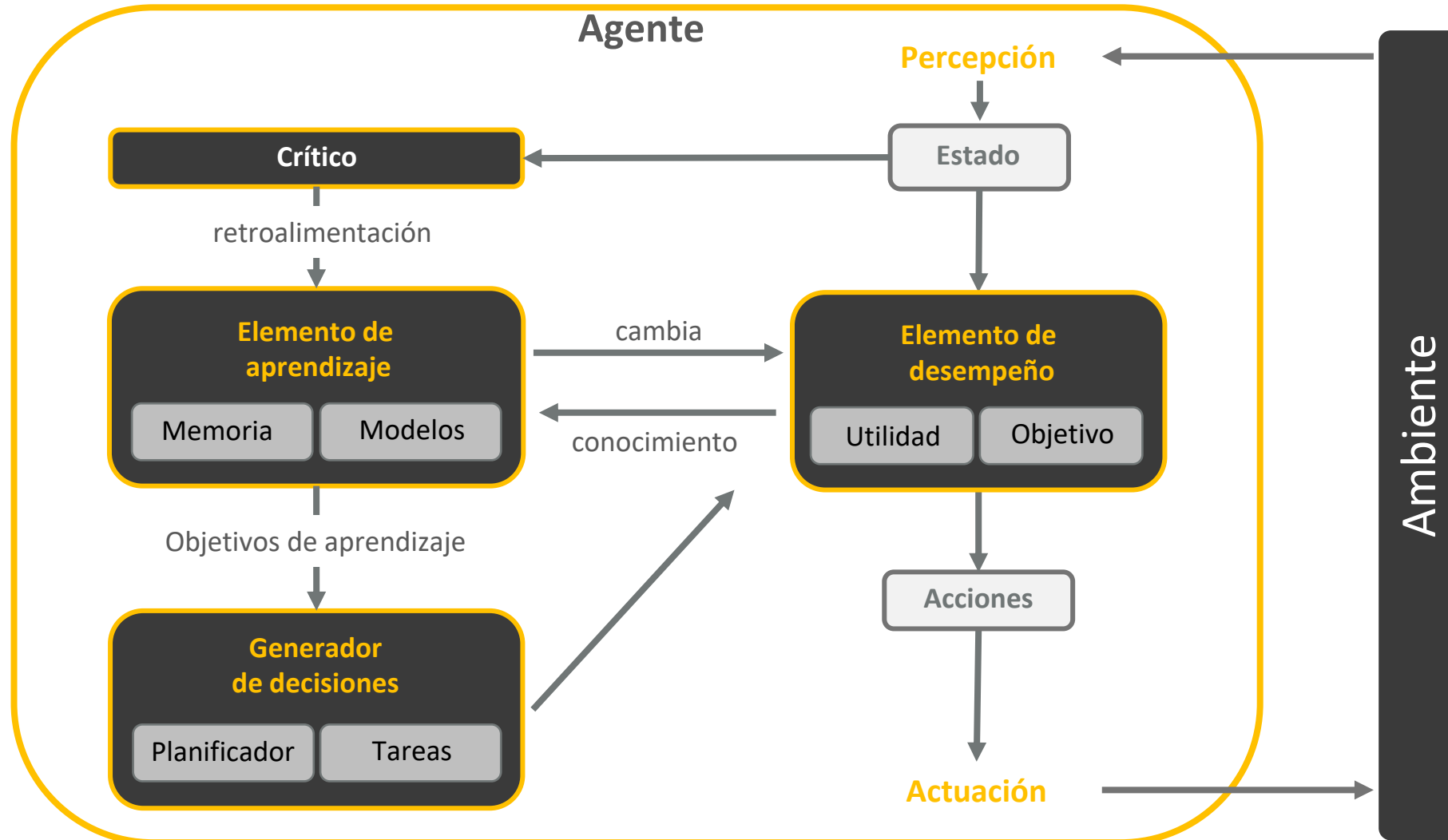


Aprendizaje y Tácticas de Entrenamiento

- Reglas / inferencias
- Entrenamiento / *onboarding* personalizado
- Modelos de aprendizaje por refuerzo
- Mecanismos alternativos de aprendizaje
- Asistentes para personas con discapacidades (ej. apoyo para sordera y ceguera)

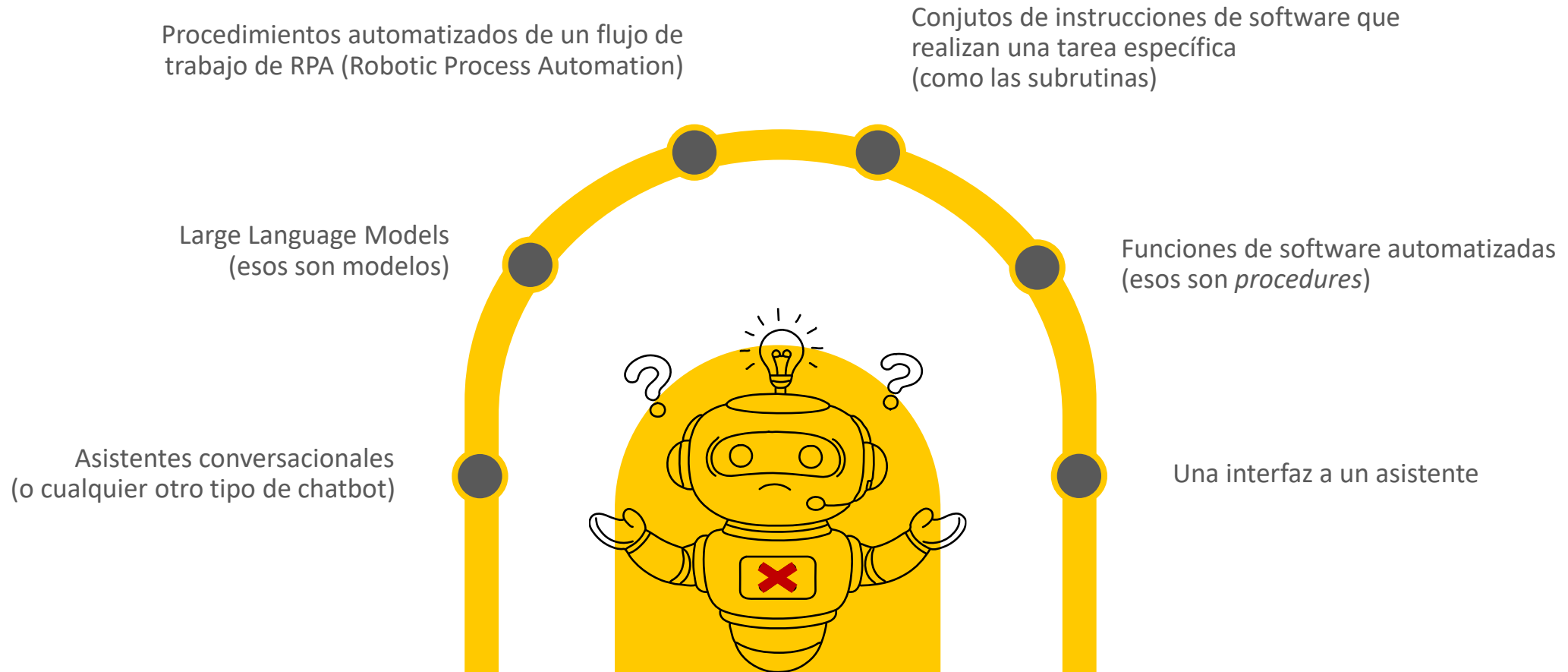
Taxonomía básica

Anatomía de un agente de IA



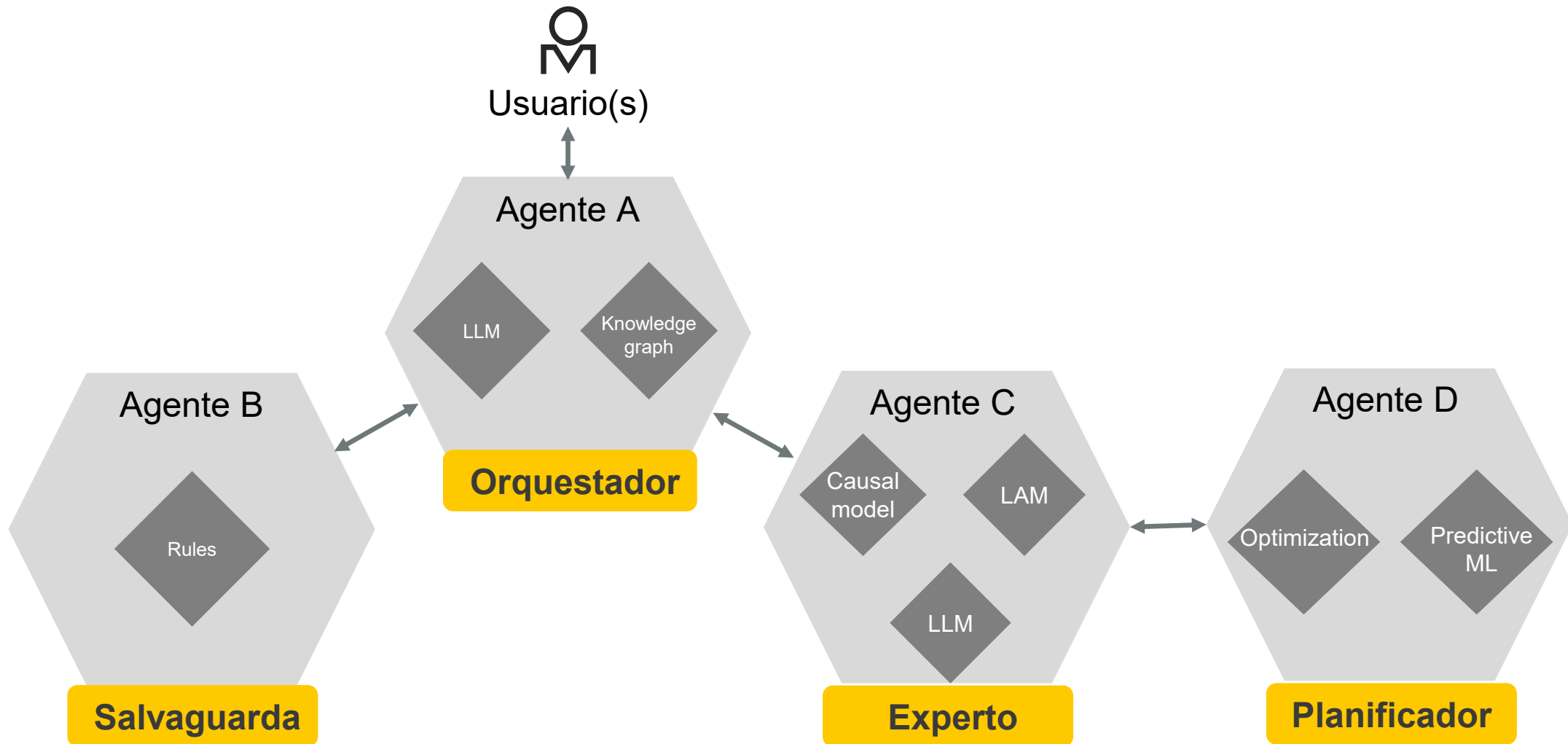
Taxonomía básica

¿Qué **NO** es un agente?



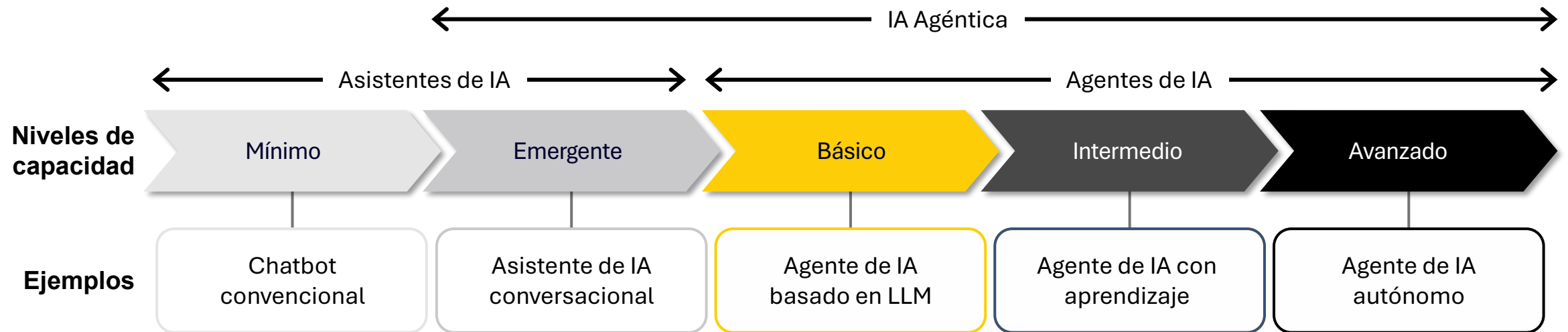
Taxonomía básica

Los agentes pueden trabajar solos o en conjunto (sistemas multi-agente)



Taxonomía básica

Chatbots ≠ Asistentes de IA ≠ Agentes de IA



Visión: adopción, complementariedad y eficiencia

Roadmap de IA

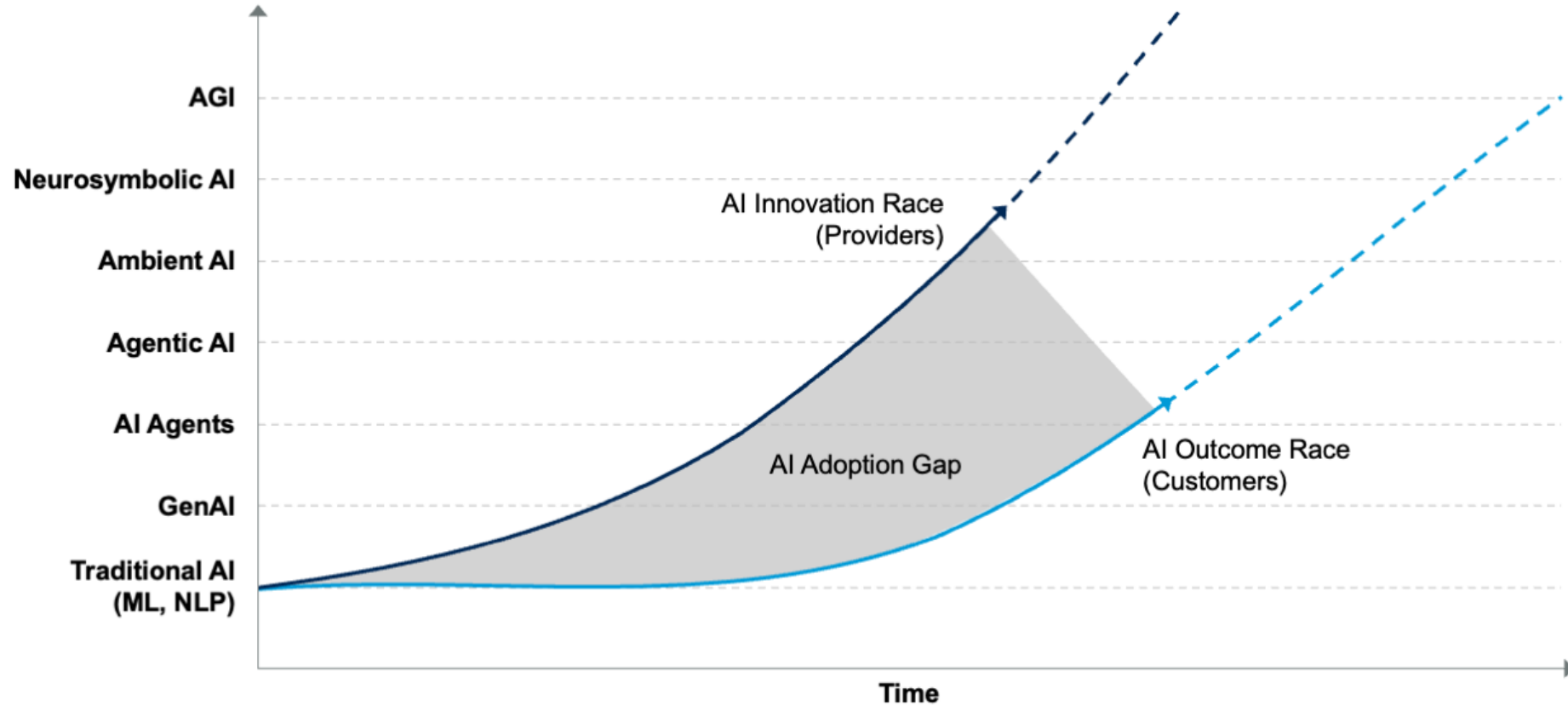
Initial activities

Advanced activities

	AI strategy	Define the AI vision	Analyze external trends	Communicate the AI strategy	Identify priorities for AI portfolio	Establish process to refine AI strategy
		Measure AI maturity	Initiate the AI strategy	Set adoption goals for AI roadmap	Measure AI strategy success	
	AI value	Prioritize initial AI use cases	Run initial AI pilots	Establish process to prioritize AI portfolio	Implement AI FinOps practices	Setup AI value monitoring system
		Define value for initial AI use cases	Track value of initial AI use cases	Introduce product management practices	Launch an initial AI product	Establish an AI product portfolio
	AI organization	Create an AI resourcing plan	Appoint an AI leader	Establish AI target operating model	Set up process to manage AI partnerships	
		Set up an AI community of practice	Set up an initial AI team/center of excellence	Form initial external AI partnerships		
	AI people & culture	Create an initial AI workforce plan	Create an AI change management plan	Set up process to evaluate AI workforce impact	Define business champions to drive AI literacy	Funding of strategic projects for the development of champions
		Set up process for review of roles and job redesign	Create initial AI awareness campaigns	Launch an AI literacy program	Set up monitoring of employee readiness for AI	
	AI management	Identify top AI risks and mitigation	Establish AI ethical principles	Set enforcement processes	Set up cross-functional AI governance board	Use AI literacy programs for AI Management
		Define initial AI policies	Define decision rights for AI	Define target management AI Operation model	Pilot AI Management tooling	
	AI engineering	Establish build vs. buy framework	Set up a sandbox environment	Define AI reference architecture	Establish MLOps/ModelOps practice	Design and embed AI UI/UX best practices
		Select vendors for initial AI use cases	Develop a library of design patterns	Create an AI vendor and application strategy	Set up an AI observability system	Stand up AI platform engineering
	AI data	Assess data readiness for initial AI use cases	Build data analytics for AI	Extend data governance to support AI	Establish an AI data quality framework	Implement data observability for AI
		Implement data readiness plan	Gain buy-in to evolve data capabilities for AI	Evolve data capabilities for AI	Adapt metadata practices for AI	

Visión: adopción, complementariedad y eficiencia

The AI Adoption Gap



AGI = Artificial General Intelligence

Del prompt engineering al context engineering

Prompt: instrucción, pregunta o entrada de texto en lenguaje natural que se proporciona a un sistema de inteligencia artificial (IA) para guiar su respuesta y activar su capacidad generativa

Prompt Engineering

Establece las mejores prácticas para especificar y limitar el conjunto de respuestas que un modelo de IA puede producir.



Context Engineering

Proporcionar el contexto adecuado a los modelos de IA para que provean las mejores respuestas en función de instrucciones, ejemplos, datos, reglas, etc.

Tipos de prompting:

- **Zero-shot:** Haces una pregunta sin ejemplos
- **Few-shot:** Haces una pregunta proveyendo algunos ejemplos
- **Chain-of-Thought:** Fuezas al modelo a explicar su razonamiento paso a paso

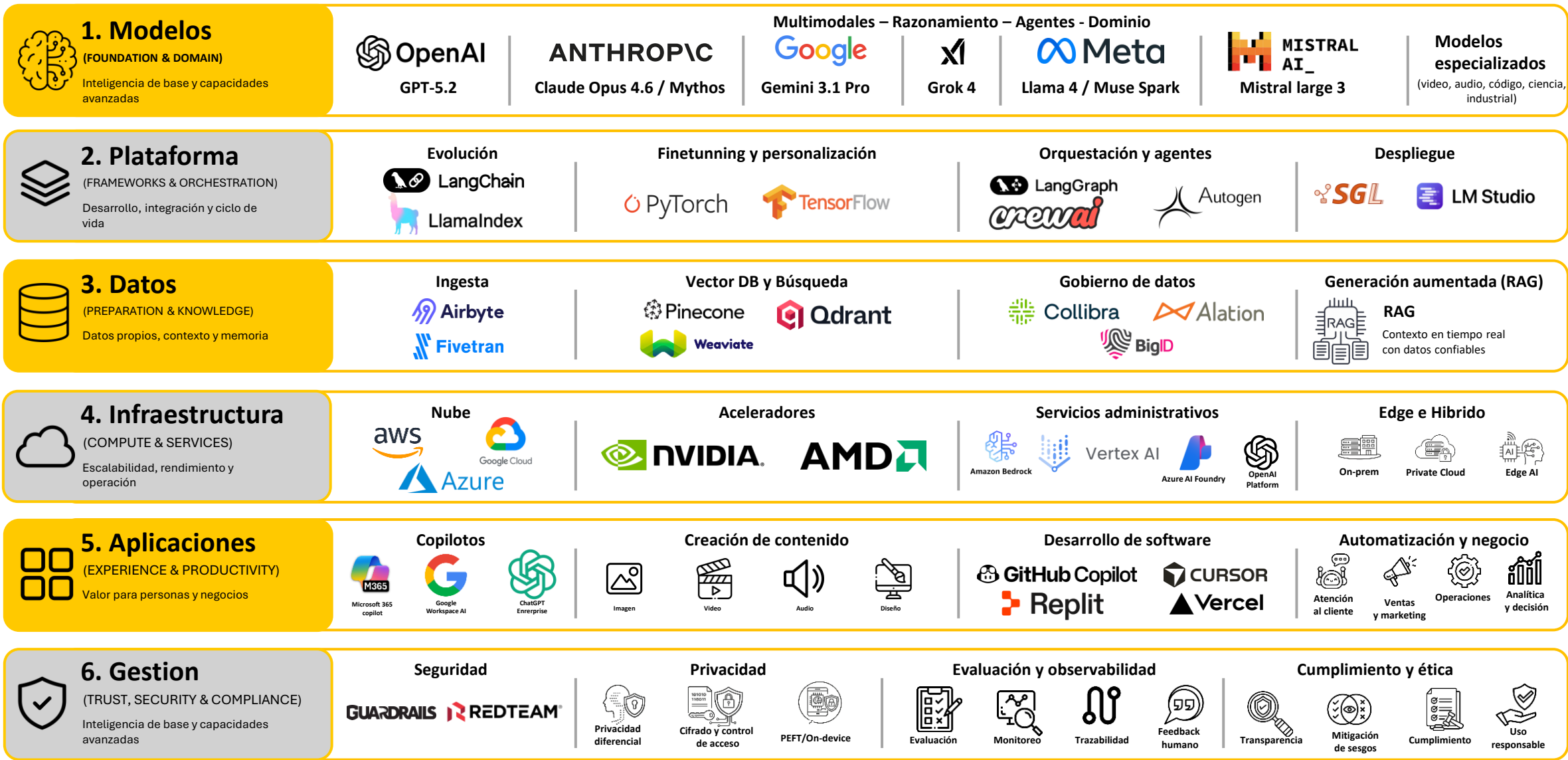
—
+
Consumo de Tokens,
precisión,
complejidad de tareas

Human in the loop vs Human in the front

	Human in the Loop (HITL)	Human in the Front (Human-Driven)
Objetivo	Reducir errores y gestionar casos excepcionales que la IA no puede / no debe, resolver por si sola	Potenciar las capacidades analíticas y ejecutivas del ser humano a través de la IA
Principal factor determinante	Sistema de IA	Humano
Enfoque en el proceso	Impulsado por la IA con supervisión humana	Impulsado por humanos con asistencia de la IA
Rol humano	Aprobador/Supervisor (punto de control)	Operador/Usuario (participante activo)
Modelo de confianza	Confianza en la fiabilidad del sistema	Confianza en el criterio humano
Caso de uso principal	Mitigación de riesgos, decisiones de alto impacto	Productividad, creatividad, eficiencia

Stack tecnológico de IA

Stack tecnológico de IA Generativa (2026)



Stack tecnológico de IA

Stack tecnológico de IA Agéntica (2026)

Agent Frameworks

LangChain

LangGraph

CrewAI

AutoGen

OpenAI Agents SDK

Google ADK

Anthropic Agent SDK

Semantic Kernel

LlamaIndex

Haystack

Agno

Mastra

PydanticAI

Smolagents

Letta

CAMEL-AI

MetaGPT

BabyAGI

AutoGPT

DSPy

No-Code / Low-Code Builders

n8n

Dify

Flowise

Langflow

Rivet

Voiceflow

Botpress

Relevance AI

MindStudio

Wordware

Lindy AI

Gumloop

Coze

BuildShip

Zapier

Make

Activepieces

Stack AI

Airia

Observability & Evaluation

LangSmith

Langfuse

Braintrust

Arize Phoenix

Portkey

Helicone

AgentOps

W&B Weave

Patronus AI

Galileo

Opik

Promptfoo

DeepEval

Memory & Vector Databases

Zep

Pinecone

Weaviate

Chroma

Qdrant

Milvus

LanceDB

pgvector

Turbopuffer

Cognee

Browser Use & Web Scraping

Browser Use

Crawl4AI

Skyvern

Stagehand

Browserbase

Playwright MCP

Firecrawl

Steel

Agent Tool Integrations

StackOne

Arcade AI

Nango

Composio

Paragon

Merge

Pipedream

Agent Protocols

MCP (Anthropic)

A2A (Google)

ANP

AG-UI

Coding Agents & AI IDEs

Cursor

Windsurf

Claude Code

GitHub Copilot

Devin

Replit Agent

Bolt.new

v0

Lovable

Aider

Continue

Cline / Roo Code

OpenHands

Codex

Amazon Q

Enterprise Agent Platforms

Salesforce Agentforce

Microsoft Copilot Studio

ServiceNow AI Agents

Workday AI Agents

IBM watsonx

Palantir AIP

Zendesk AI

Intercom Fin

SAP Joule

Oracle AI

Gemini Enterprise

AI Clouds

Modal

Groq

CoreWeave

Crusoe

Baseten

Replicate

Together AI

Fireworks AI

Foundation Models

OpenAI

Anthropic

Google

Meta

Mistral

xAI

Cohere

DeepSeek

Alibaba

Amazon

Moonshot

Stack tecnológico de IA

Stack tecnológico de aplicaciones populares de IA



Riesgos de la IA



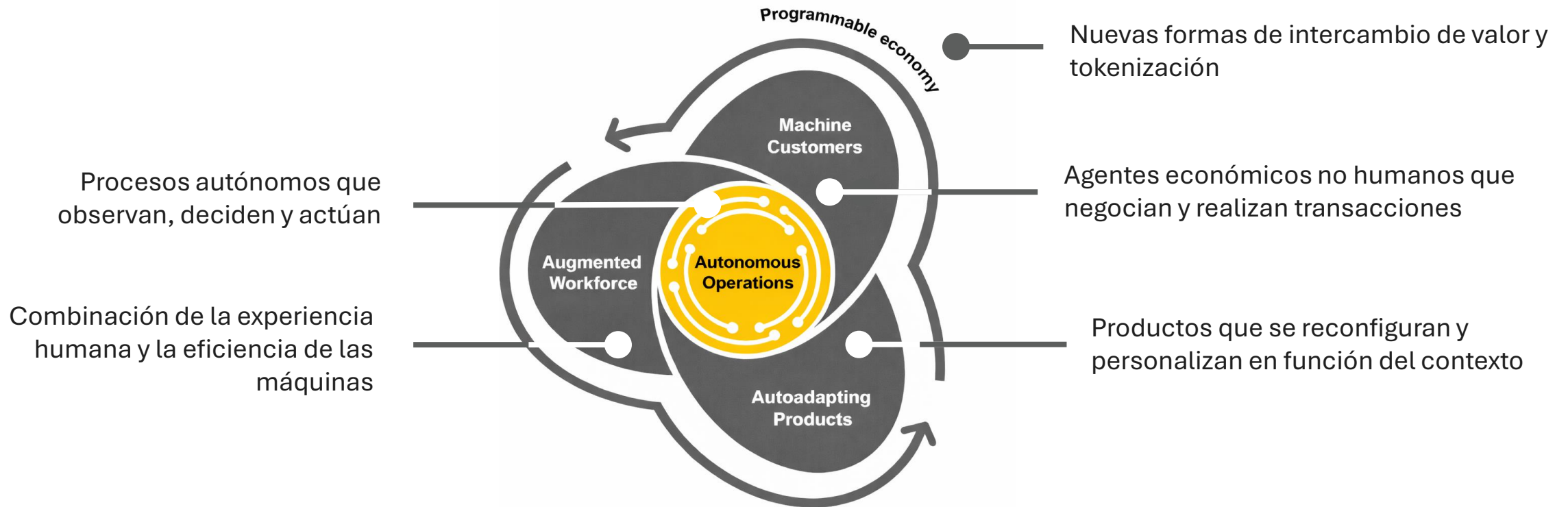
Riesgos de la IA: Ciberriesgos

Categoría de amenaza	Descripción	Impacto
Manipulación de datos de entrada y envenenamiento de datos	Dependencia de fuentes de datos manipulables o malinterpretadas.	Decisiones mal informadas, acciones perjudiciales
Secuestro y abuso de credenciales	Robo, uso indebido o sobreexposición accidental de credenciales	Control no autorizado, robo de datos
Fuentes maliciosas	Interacción con fuentes fraudulentas o falsas, como sitios web delictivos o bots de difusión de noticias falsas.	Acciones y resultados comprometidos
Desviación del agente y comportamiento no intencionado	Agente que actúa fuera de su propósito previsto debido a fallas internas o desencadenantes externos.	Daños a la reputación, interrupción de las operaciones
Ingeniería social y mal uso	Explotación o mal uso accidental de la confianza/contexto.	Erosión de la confianza, daño social
<i>Exploits</i> contra infraestructuras de alojamiento vulnerables	Vulnerabilidades en tiempo de ejecución o configuraciones incorrectas en las plataformas de alojamiento	Acceso no autorizado, compromiso del sistema
Fallos de comunicación e interfaz	Fallos o problemas de comunicación en la conectividad externa.	Pérdida de control, fugas de datos y <i>malware</i>
<i>Exploits</i> de modelos y algoritmos	Modelos/algoritmos centrales vulnerables o defectuosos	Pérdida de IP, rendimiento degradado, objetivos no alcanzados
Manipulación de memoria y ataques a la carga de trabajo	Errores en la ejecución de la memoria/carga de trabajo en tiempo de ejecución.	Robo de datos, secuestro de ejecución

Negocios autónomos

Estrategia que utiliza tecnología adaptable y con capacidad de autoaprendizaje para tomar decisiones, actuar y crear nuevos tipos de valor, aumentando las capacidades de autoservicio y autonomía de los clientes, empleados y de la infraestructura de TI.

Componentes de un negocio autónomo



Costos de la IA

