

TALLER

CONSTRUYENDO AGENTES INTELIGENTES CON LLMS: DE LA TEORÍA A LA PRÁCTICA



Agenda



1 Presentación

5

Crea tu primer agente

2 LLms

6

Automatización de agentes

3 Asistentes y RAG

7

Agentes multiuso

4 Agentes y sus arquitecturas

8

Retos y conclusiones



Francisco Daniel López Huerta

- mata & GenAl Engineer en Data Bunker
- franciscodaniel-lh
- FranciscoDanielLh
- franciscodlh.online

¡Hola! Soy Fran, tengo experiencia en la creación de soluciones integrales como ingeniero de datos y desarrollador de software.

- Mi experiencia técnica incluye:
- Diseño e implementación de arquitecturas de datos escalables
- Automatización de flujos ETL para optimizar procesos empresariales
- Desarrollar soluciones fullstack adaptadas a múltiples plataformas
- Mi experiencia con agentes:
 - Agente virtual entrenado para ser un guía experto en sitios turísticos
 - Agente inteligente para financiera que clasifica clientes, consulta de históricos, da seguimiento a cuentas, predice tendencias y detecta fraudes.
 - Agente para soporte al cliente conectado a redes sociales
 - Agente de analítica geoespacial avanzada con interacción a mapas dinámicos
 - Agente especializado en la creación y análisis de encuestas implementado en plataforma

Cita del dia

La inteligencia artificial no es sólo sobre hacer máquinas que piensen como humanos, sino sobre expandir lo que los humanos pueden lograr con la ayuda de estas nuevas herramientas.

- Fei-Fei Li, destacada científica en IA y ex directora de investigación de IA en Google

Introducción

La inteligencia artificial está transformando nuestro mundo, convirtiendo la ciencia ficción en realidad cotidiana. Máquinas que comprenden, crean y resuelven problemas complejos ya no son fantasía.

Esta revolución impacta todas las industrias. El aumento de la IA permite que personas con grandes ideas pero recursos limitados desarrollen soluciones innovadoras que antes solo estaban al alcance de pocas organizaciones.

1 de cada 4 de los emprendedores en Y Combinator dijeron que al menos el 95% de su código era hecho por IA.

El sector en cifras

72%

De las organizaciones a nivel mundial se han integrado a la IA en al menos una función empresarial. 52%

En aumento de la inversión para startups de IA mientras que para startups tradicionales bajo 10%

1400M

De personas han interactuado con productos de inteligencia artificial 37.5%

De aumento en las vacantes para roles de inteligencia artificial.





LLMs

Un LLM (Large Language Model) es un modelo de inteligencia artificial basado en redes neuronales, entrenado con millones de textos (libros, artículos, sitios web), lo que le permite predecir, generar y comprender información en función del contexto. Estos modelos aprenden relaciones estadísticas entre palabras, frases y estructuras lingüísticas a partir de datos masivos.

Ejemplo: GPT-4o, desarrollado por OpenAl, es un LLM de última generación utilizado en aplicaciones como ChatGPT, puedes hacerle preguntas y te responde como si estuvieras hablando con una persona.

¿Qué modelo escoger?



Inferencia

La capacidad del modelo para realizar deducciones lógicas y generar conclusiones a partir de información dada.



Ventana de contexto

La cantidad de texto que el modelo puede "recordar" y procesar en una sola interacción. Medido en tokens (aprox 4 caracteres = 1 token).



Latencia

El tiempo que tarda el modelo en responder una solicitud. Menor latencia significa respuestas más rápidas, crucial para aplicaciones en tiempo real.



Permisos y limitaciones

Restricciones éticas y de seguridad implementadas en el modelo.



Razonamiento

Cadenas de pensamiento para obtener conclusiones lógicas a partir de cada una de las reflexiones para validar la respuesta final.



Lenguaje

Capacidad del modelo para entender diferentes lenguajes y poder contestar en el mismo idioma de manera nativa.

Parámetros de un LLm



Temperatura

Controla qué tan creativo o preciso es el modelo.

Baja temperatura (ej. 0.2): respuestas más seguras, predecibles.

Alta temperatura (ej. 0.9): respuestas más creativas o aleatorias.

Longitud (Max tokens)

Límite de longitud en la respuesta para evitar respuestas largas y disminuir el consumo de tokens.

Top P y Top K

Top P: Limita las respuestas a las más probables, pero dentro de un porcentaje acumulado de confianza.

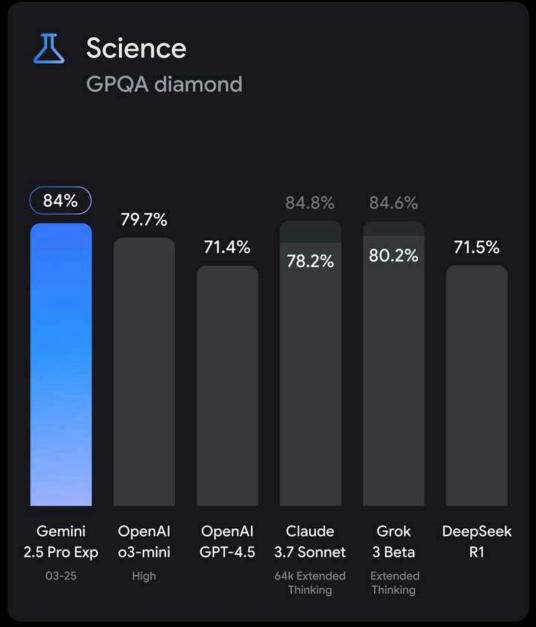
Top K: El modelo elige solo entre las k palabras más probables.

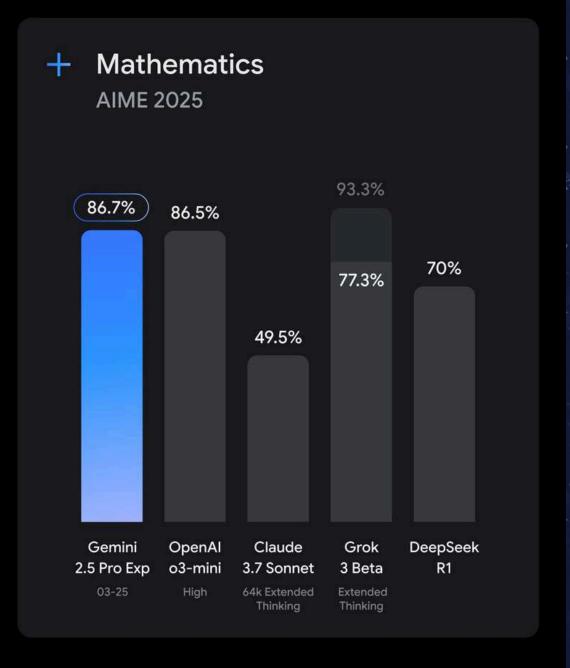
Secuencias de parada

Frases o caracteres que le dicen al modelo: "¡detente aquí!"

Competencia de LLMs



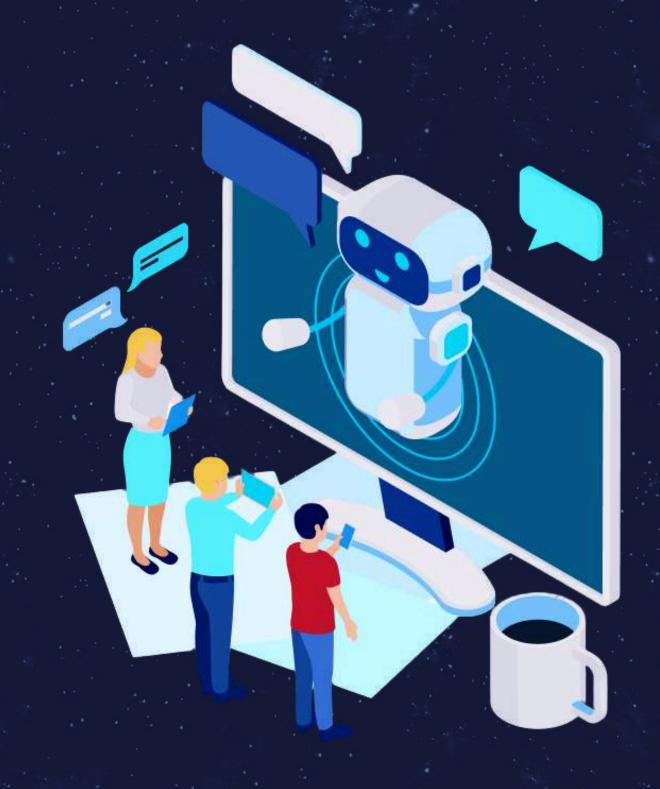




Asistente Inteligente

Un asistente inteligente es una aplicación de inteligencia artificial que utiliza un LLM para realizar tareas específicas basadas en su conocimiento, estos asistentes están diseñados para interpretar y responder a instrucciones, permitiendo interacciones fluidas.

Se puede añadir información a su ventana de contexto para que se comporte de manera especifica o que complemente su información con datos personalizados.



Ampliar el conocimiento

Few Shots

Das unos pocos ejemplos
dentro del prompt para guiar
el comportamiento del modelo
en cada consulta.
Ejemplo: Provees al agente de
ejemplos de preguntas
frecuentes de tu negocio.

Fine tuning

Entrenas al modelo con ejemplos personalizados para que aprenda un estilo o conocimiento específico. Ejemplo: Dataset con 1,000 preguntas y respuestas legales.

Base de conocimiento

Combina una base de datos con un modelo para buscar información en tiempo real.

Ejemplo: Cargas un PDF con manuales técnicos de tu empresa.

Ingeniería de prompts

Proporciona Contexto Adecuado

Un cliente joven, de 30 años, busca invertir en empresas ecológicas con un presupuesto de \$50,000.

Define el Objetivo Claramente

Proporciona una lista de cinco empresas recomendadas para inversión, incluyendo una descripción de cada una y el sector al que pertenecen.

Indica el Tono o Estilo Deseado

Utiliza un lenguaje claro y accesible para alguien sin conocimientos financieros profundos.

Especifica la Estructura del Resultado

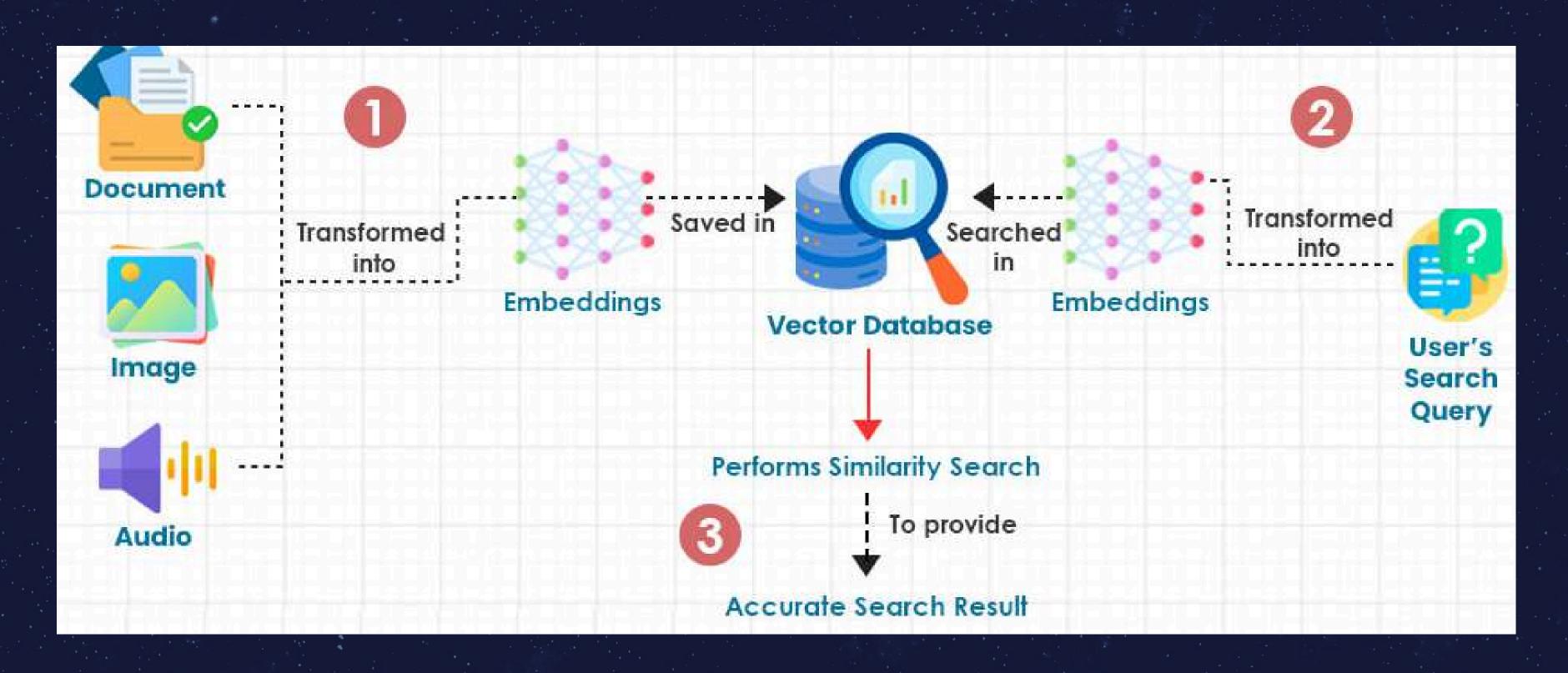
Presenta la información en formato de tabla, incluyendo el nombre de la empresa, su descripción y su sector además de las ventajas de invertir ahí.

Indica Restricciones o Límites

Enfócate en empresas sostenibles y con un presupuesto de \$50,000.



Arquitectura RAG





Agente inteligente

Un agente es una aplicación impulsada por inteligencia artificial que no solo comprende lenguaje natural, sino que también puede razonar, tomar decisiones, y ejecutar acciones de manera autónoma para alcanzar un objetivo definido.

A diferencia de un asistente que responde a comandos específicos, un agente inteligente tiene la capacidad de:

- Entender una meta general.
- Dividir esa meta en sub-tareas.
- Planificar y ejecutar cada paso, ya sea consultando
 herramientas externas (como APIs, bases de datos o
 buscadores), accediendo a otros sistemas (correo, calendario,
 apps) o tomando decisiones sin supervisión constante.
- Adaptarse dinámicamente a cambios en el entorno o a nuevas instrucciones.

Orquestación

Guardrail

Establece políticas y filtros para asegurar que las interacciones con el modelo sean seguras, éticas y alineadas a los objetivos.

Preprocesamiento

Transforma y limpia la entrada del usuario antes de enviarla al sistema para que sea procesada correctamente.

Selección de herramientas

Determina si se debe usar una herramienta externa (API, base de datos, buscador, calculadora, etc.) para resolver la consulta.

Procesamiento

Es el corazón del sistema: ejecución del razonamiento del modelo, invocación de herramientas, recuperación de contexto, etc.

Postprocesamiento

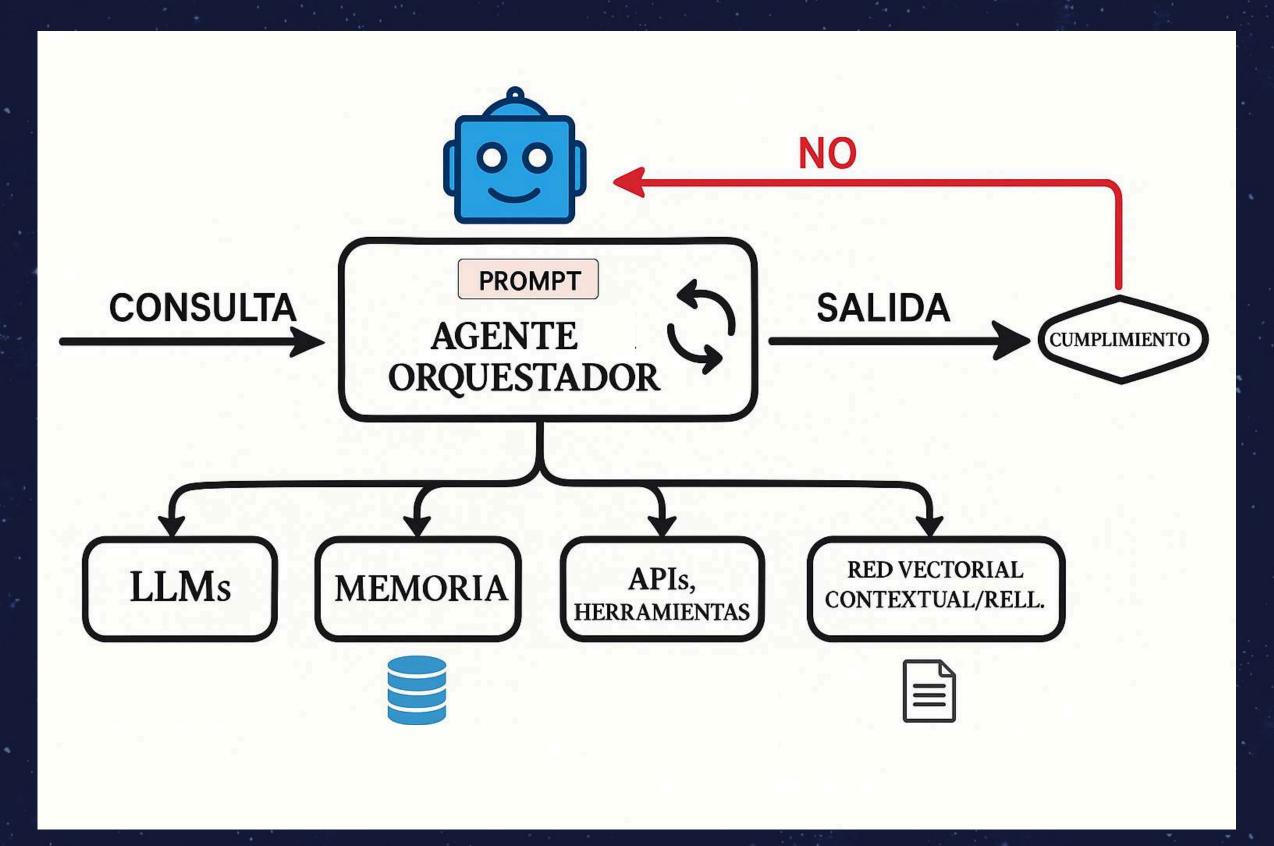
Ajusta o refina la salida del modelo antes de mostrarla al usuario.



Herramientas nativas



Diagrama de agente



Herramientas para crear agentes

Frameworks

Ofrecen flexibilidad y personalización para desarrolladores con conocimientos técnicos.
CrewAl, LangChain,
LlamaIndex

No Code

Permiten a usuarios sin
experiencia en
programación desarrollar
agentes de IA mediante
interfaces gráficas intuitivas.
BotPress, N8N,

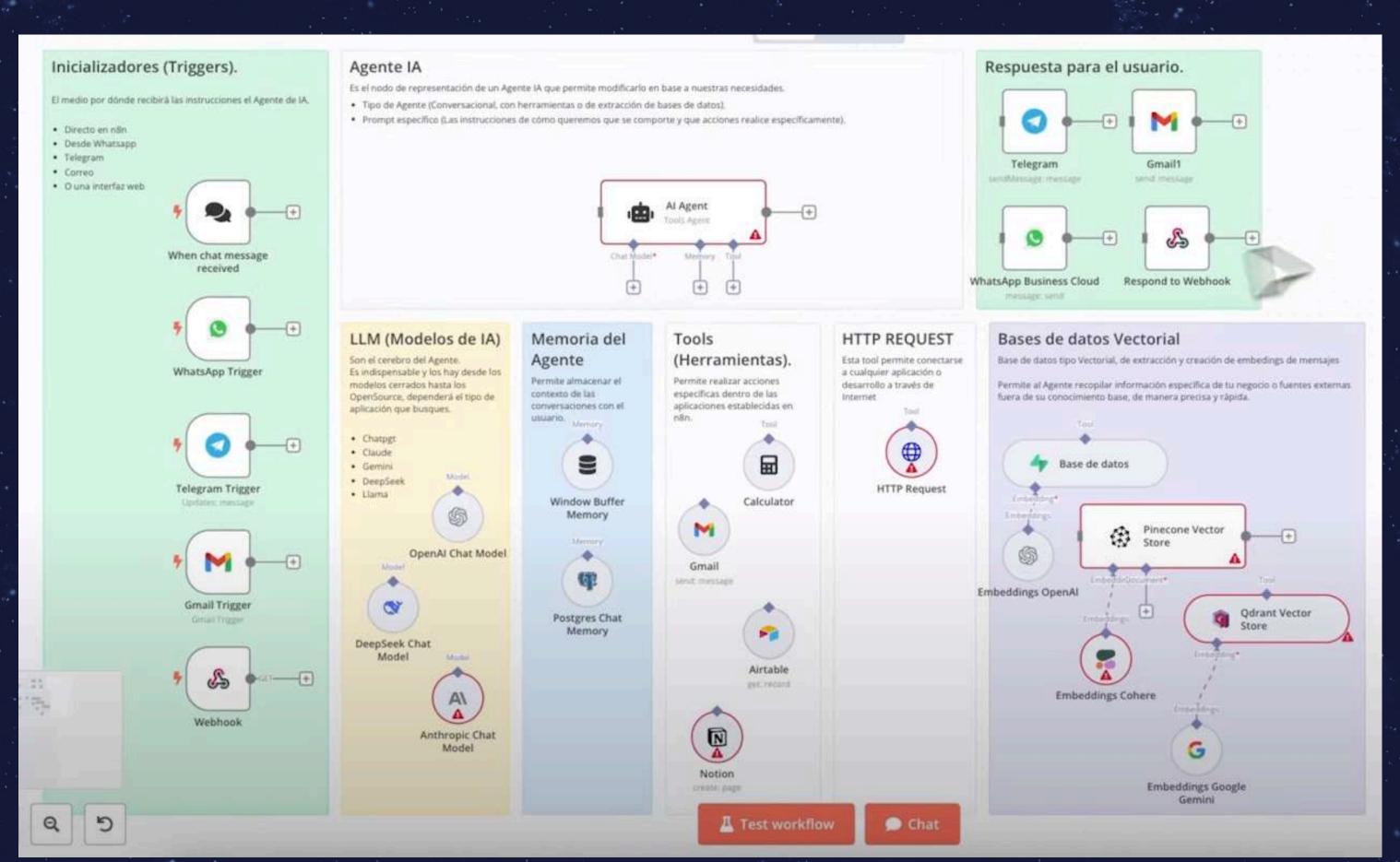
Nube

Proporcionan herramientas escalables y gestionadas para desarrollar agentes de IA.

Ejemplos: Bedrock,

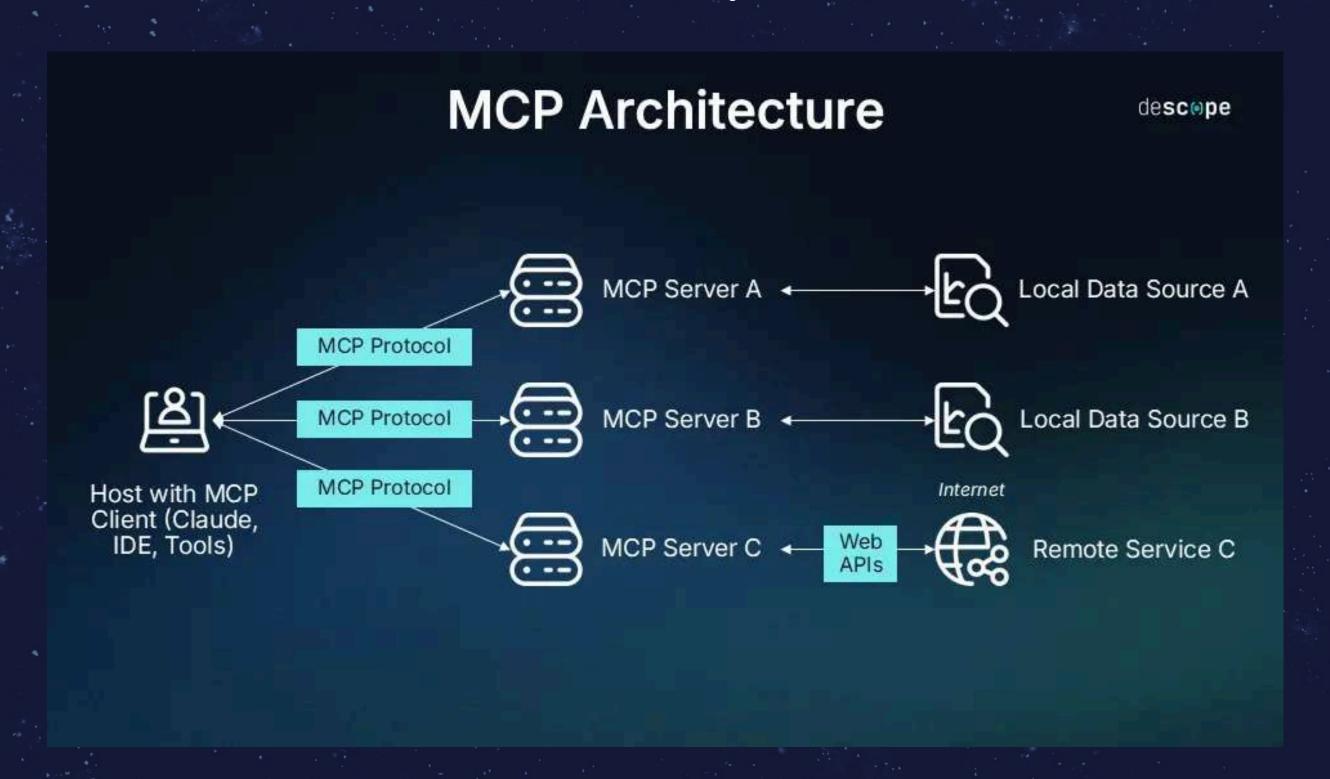
Vertex Al, Azure OpenAl

Arquitectura n8n



Protocolo MCP

Busca estandarizar la forma en que las aplicaciones de inteligencia artificial, interactúan con fuentes de datos y herramientas externas.





Retos actualmente

- 1. Ética y sesgos en la IA
- 2. Seguridad y vulnerabilidades
- 3. Transparencia y explicabilidad
- 4. Impacto en el empleo y transformación laboral
- 5. Consumo de recursos y sostenibilidad
- 6. Regulación y gobernanz

Conclusiones

- Definición y características de los agentes inteligentes:
 Sistemas autónomos que perciben su entorno y actúan de manera proactiva para alcanzar objetivos específicos.
- Aplicaciones prácticas: Utilización en asistentes virtuales, automatización industrial, análisis de datos y más, mejorando eficiencia y precisión en diversas tareas.
- Beneficios en la automatización: Optimización de recursos, reducción de costos operativos y mejora en la toma de decisiones basada en datos en tiempo real.
- **Desafíos éticos y técnicos:** Consideraciones sobre ética, privacidad y seguridad en el desarrollo y uso de agentes inteligentes, asegurando transparencia y confiabilidad.





Coctacto

Número de teléfono 5516576015

Correo electrónico franciscodaniel.lh@gmail.com

Sitio web franciscodlh.online

Redes sociales
franciscodaniel-lh