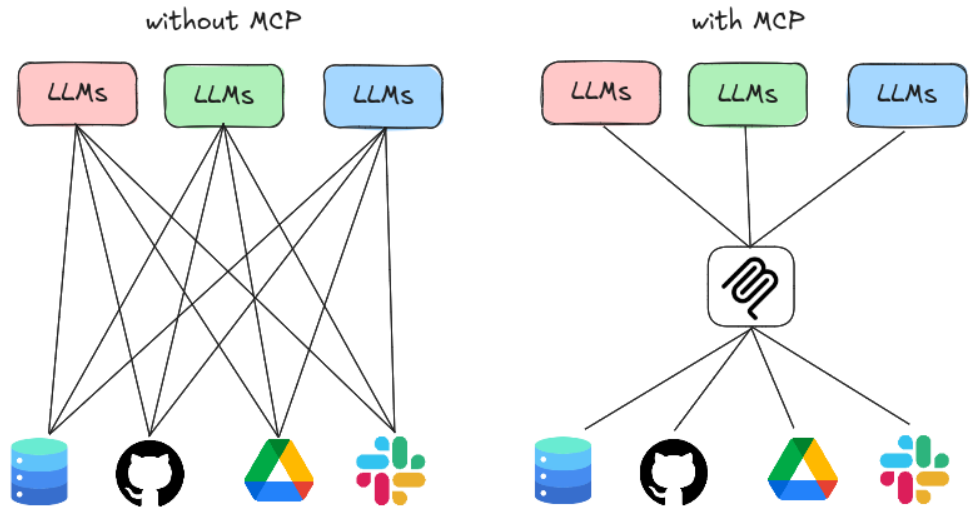
Model Context Protocol (MCP) como tecnología emergente para la integración segura de sistemas con IA

MCP es un estándar abierto que permite conectar aplicaciones de IA (por ejemplo, modelos de lenguaje) con fuentes de datos, herramientas, APIs o flujos de trabajo externos.
Funciona como un “USB-C para IA”: un conector universal que evita que cada integración requiera código ad hoc.
Este enfoque me parece emergente y estratégico ya que define una infraestructura común que puede acelerar la construcción de agentes de IA útiles, componibles y seguros esencial para llevar IA generativa o cognitiva de laboratorio a entornos de aplicaciones reales



Los siguientes principios teóricos garantizan que la integración sea escalable, mantenible y más segura que las integraciones ad-hoc tradicionales.

- Interoperabilidad y modularidad: MCP usa una arquitectura cliente-servidor. El cliente se comunica con uno o varios servidores MCP que exponen herramientas, datos o plantillas. Este diseño abstrae el acceso a sistemas externos detrás de una interfaz universal.
- Contextualización y persistencia de contexto: MCP no es solo para llamadas puntuales: permite que los agentes mantengan contexto, estado o “memoria” en el servidor, lo que posibilita flujos de trabajo multi-paso.

Cuando hablamos de métodos y herramientas para la implementación de MCP, MCP se implementa mediante SDKs disponibles en varios lenguajes (Python, TypeScript, Java, etc.) lo que facilita su adopción en distintos entornos de desarrollo [1].
Un servidor MCP expone capacidades (herramientas, datos, prompts) que pueden ser descubiertas dinámicamente por el cliente IA. Un ejemplo concreto es el MCP Server de Mercado Pago, que permite a agentes de IA interactuar con su documentación y servicios de pago directamente desde entornos de desarrollo. Esto facilita la búsqueda de información, la generación de código y la validación de integraciones de checkout, demostrando cómo MCP puede aplicarse en un caso real del ámbito financiero, mejorando la productividad y reduciendo errores de implementación.
MCP agiliza el desarrollo de aplicaciones de IA al simplificar la integración con APIs y sistemas externos, permitiendo crear agentes más útiles y contextuales que pueden acceder a datos actualizados y ejecutar acciones concretas. Además, su estándar favorece

la escalabilidad, la colaboración entre equipos y la transferencia tecnológica, al tiempo que impulsa arquitecturas de IA más modulares, distribuídas e innovadoras.

[1] Anthropic, *Model Context Protocol – Getting Started*, 2024. [En línea]. Disponible en: https://modelcontextprotocol.io/docs/getting-started/intro