



# De API a MCP

Integrando datos en el mundo real (caso UNICEF)



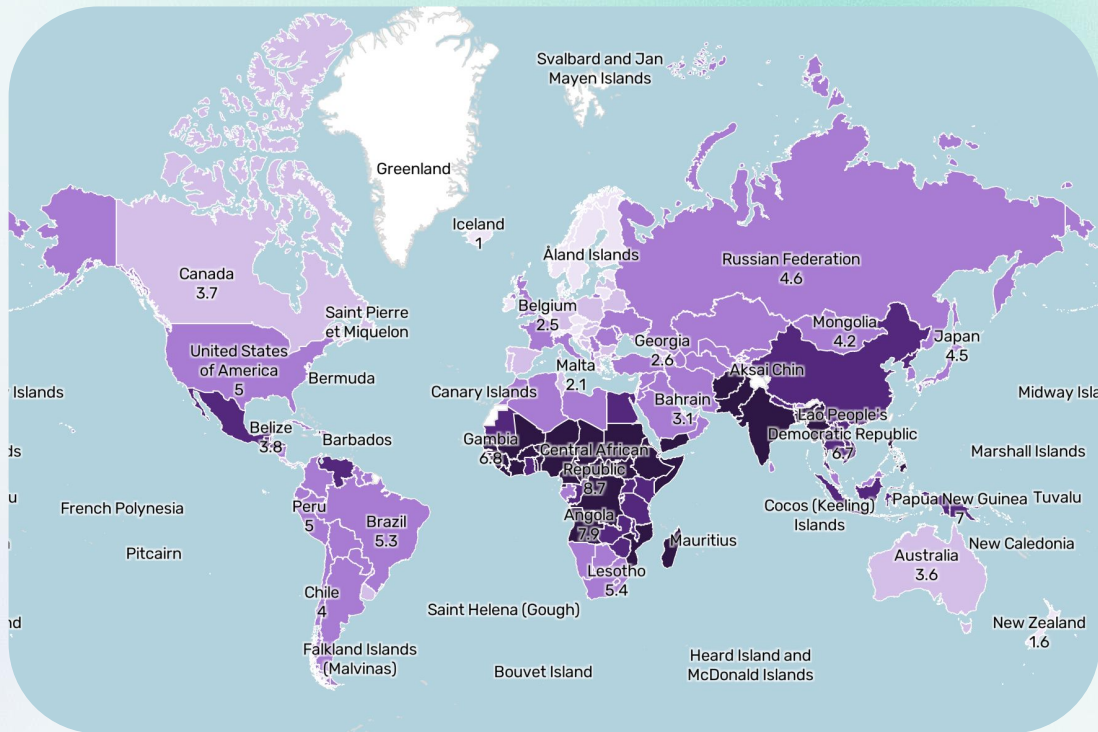
**Federico Bello**

Machine Learning Engineer | [fefo@tryolabs.com](mailto:fefo@tryolabs.com)



# UNICEF - CCRI

- **Múltiples fuentes heterogéneas:**  
Datos tabulares, imágenes y texto de distintos orígenes
- **Difícil integración:** Complejidad para cruzar información entre fuentes
- Referencia:
  - CCRI - UNICEF 2024

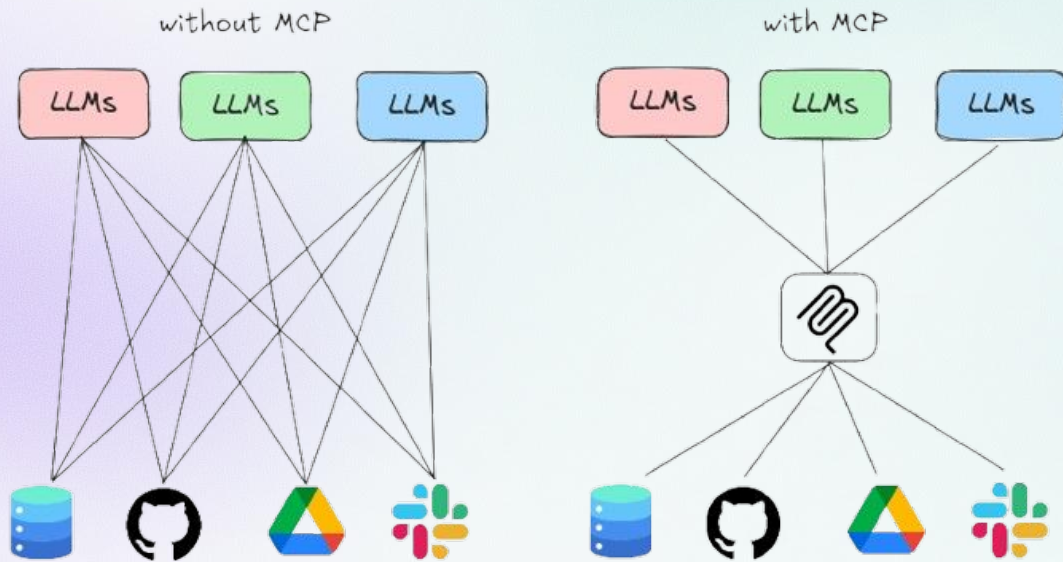


# ¿Qué es MCP?

# ¿Qué es MCP?

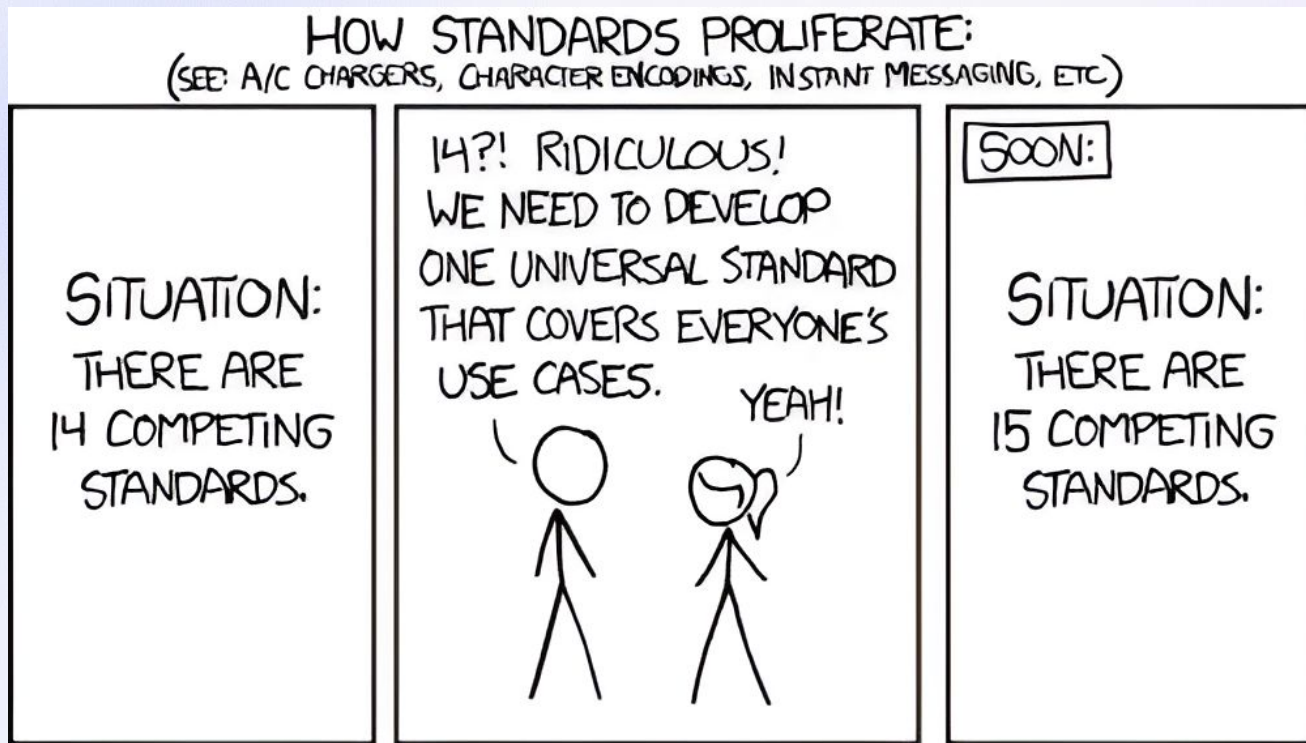
## Model Context Protocol (MCP):

- Estándar abierto para conectar LLMs con datos y herramientas externas
  - “El puerto USB-C para IA”





# ¿Qué es MCP?

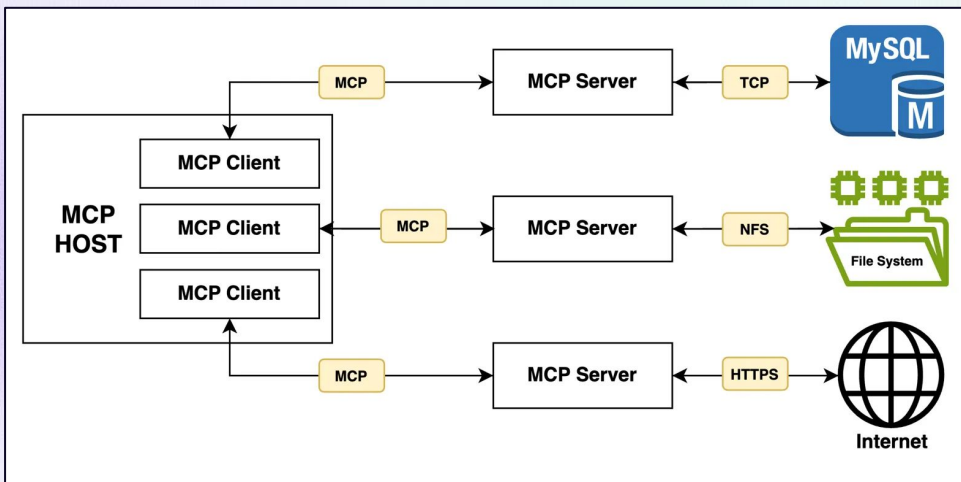


# Arquitectura

# Arquitectura

## 3 Participantes:

- **MCP Host:** la aplicación de IA (Claude Desktop, VSCode)
- **MCP Client:** componente que maneja la conexión con el MCP Server
- **MCP Server:** expone herramientas y contexto de sistemas externos





# Arquitectura

- **Capa de Datos:** protocolo de intercambio basado en JSON-RPC 2.0
  - **Servidor:** exponer herramientas, recursos y prompts
  - **Cliente:** solicita consultas LLM, input del usuario y logging
- **Capa de Transporte:** maneja canales de comunicación y autenticación
  - **Stdio:** comunicación local, usa la salida estandar
  - **HTTP:** comunicación remota

# Componentes

# Componentes

## Las 3 piezas fundamentales

### Tools

→ Funciones que el LLM puede invocar para tomar acciones

### Resources

→ Datos que la aplicación puede buscar y usar como contexto

### Prompts

→ Templates reutilizables de instrucciones llamadas por el usuario

# Componentes - Tools

- **Utilidad:** Funciones que el LLM puede invocar para tomar acciones
- **Control:** El modelo decide cuándo usarlas
- **Operaciones:**
  - `tools/list` para el descubrimiento
  - `tools/call` para la ejecución

# Componentes - Tools

```
@mcp.tool()
```

```
def sumar(a: int, b: int) -> int:
```

```
    """
```

```
    Suma dos números enteros.
```

```
    Args:
```

```
        a (int): Primer número.
```

```
        b (int): Segundo número.
```

```
    """
```

```
    return a + b
```



```
{
    "name": "sumar",
    "description": "Suma dos números enteros.",
    "inputSchema": {
        "type": "object",
        "properties": {
            "a": {
                "type": "integer",
                "description": "Primer número"
            },
            "b": {
                "type": "integer",
                "description": "Segundo número"
            }
        },
        "required": ["a", "b"]
    }
}
```



# Componentes - Resources

- **Utilidad:** Datos que la aplicación puede buscar y usar como contexto
- **Control:** La aplicación accede de forma directa y decide su uso
- **Operaciones:**
  - `resources/list` para el descubrimiento
  - `resources/templates/list` para la ejecución
  - `resources/read` para obtener los datos
  - `resources/subscribe` para monitorear cambios

# Componentes - Prompts

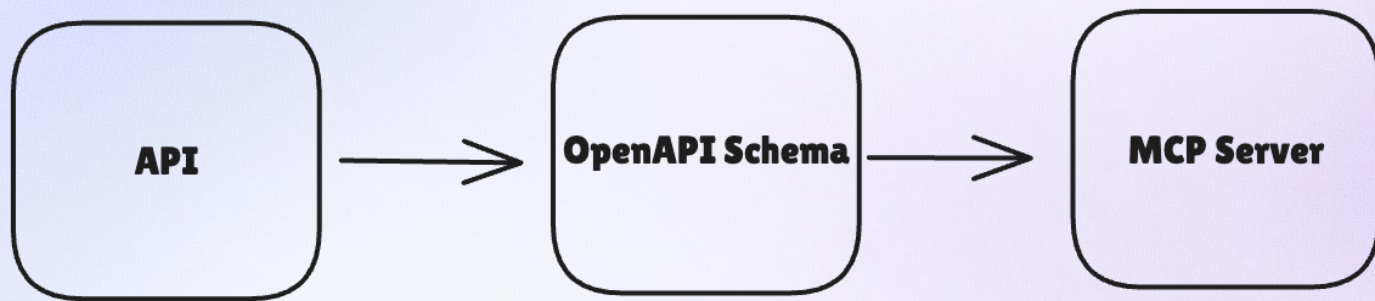
- **Utilidad:** Templates reutilizables. Definen entradas e interacciones esperadas
- **Control:** Requieren invocación del usuario
- **Operaciones:**
  - `prompts/list` para el descubrimiento
  - `prompts/get` para obtener los detalles

# Demo

API → MCP

# API → MCP

## Auto Generación





# API → MCP

## Auto Generación

### Limitaciones de LLMs

- Más Contexto → Peor Rendimiento
- Más Responsabilidades → Peor Rendimiento

### Usuarios

- **API** se documenta para **humanos**
- **MCP** se documenta para **modelos**

### Riesgos

- ⚠ Endpoints sensibles (delete, admin, etc.)

# API → MCP

## Diseño

### Curación

- Remover endpoints innecesarios
- Agrupar operaciones
- Explicitar descripciones, agregar ejemplos

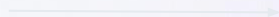
### Seguridad & Control

- Filtrar/excluir endpoints críticos
- Permisos para cada par agente/servidor
- Validar inputs en el servidor

# Referencias

# Referencias

- Model Context Protocol: <https://modelcontextprotocol.io/docs/getting-started/intro>
- Conectar a Server Locales: <https://modelcontextprotocol.io/docs/develop/connect-local-servers>
- FastMCP: <https://gofastmcp.com/getting-started/welcome>
- OpenAPI a MCP: <https://gofastmcp.com/integrations/openapi>
- Stop Converting your REST APIs to MCP  
<https://www.jlowin.dev/blog/stop-converting-rest-apis-to-mcp>
- Proyecto UNICEF  
<https://knowledge.unicef.org/CEED/resource/childrens-climate-and-environment-risk-index-ccri>



**Gracias!**