

MCP EXPLICADO SIMPLE

LAS LLAVES DE CLAUDE



QUÉ ES MCP

Claude puede escribir, razonar y explicar, pero por sí solo no ve tu calendario, tu base de datos ni tus archivos de trabajo. Para usar herramientas de verdad necesita una forma de conectarse con ellas. Esa forma se llama MCP.

MCP significa Model Context Protocol. Es un estándar abierto creado por Anthropic y presentado en noviembre de 2024, para que una aplicación de IA se conecte con herramientas y datos de una forma común.

Piensa en un asistente que sabe mucho pero está encerrado en una oficina sin llaves, así que no puede abrir ningún cajón. **MCP son las llaves**: cada servidor conectado le abre una puerta concreta, y tú decides cuáles le entregas.

LAS PIEZAS

LA APLICACIÓN

CLIENTE

Donde conversas: Claude Desktop, Claude Code y otras apps compatibles.

EL PROGRAMA

SERVIDOR MCP

Un programa que habla con una herramienta concreta: tu calendario, tus archivos, una base de datos.

LO QUE EXPONE

HERRAMIENTAS Y RECURSOS

Las herramientas son acciones que Claude puede pedir. Los recursos son datos para leer.

LO QUE EXPONE

PROMPTS

Instrucciones preparadas de antemano para tareas frecuentes.

CÓMO FUNCIONA

1

EL SERVIDOR DECLARA SUS HERRAMIENTAS

Al conectarse, cada herramienta llega con un nombre, una descripción y los datos que necesita para ejecutarse.

2

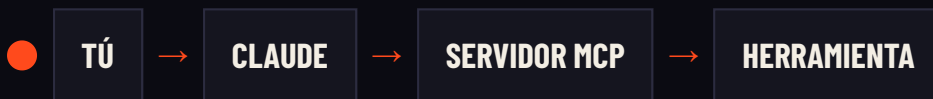
CLAUDE DECIDE CUÁNDO USAR UNA

Lee esas descripciones mientras conversas, y cuando una sirve para tu pedido, la solicita con los datos que corresponden.

3

EL SERVIDOR LA EJECUTA Y DEVUELVE EL RESULTADO

Claude no ejecuta nada por su cuenta, solo pide, y quien hace el trabajo es el servidor. Con el resultado, Claude sigue con tu pedido.



MCP Y LAS APIS

Una API es la puerta de cada servicio, y cada servicio tiene la suya, con sus propias reglas. MCP es una forma común de abrir esas puertas, así que una aplicación de IA no necesita aprender una conexión distinta para cada herramienta.

Muchos servidores MCP usan por dentro la API del servicio: traducen lo que Claude pide a lo que esa API entiende.

CONECTAR TU PRIMER SERVIDOR EN CLAUDE CODE

Para un servidor local, que corre como un programa en tu computador (transporte stdio):

```
claude mcp add <nombre> -- <comando>
```

Lo que va después de `--` es el comando que arranca el servidor. Si necesita variables de entorno, se agregan con `-e`:

```
claude mcp add mi-servidor -e API_KEY=xxx -- npx mi-servidor-mcp
```

Para un servidor remoto, que vive en una dirección web, se indica el transporte y la URL:

```
claude mcp add --transport http <nombre> <url>
```

REVISAR LO CONECTADO

☐ `claude mcp list` en la terminal muestra los servidores configurados.

☐ `/mcp` dentro de Claude Code muestra el estado de cada uno.

QUÉ REVISAR ANTES DE DARLE PERMISOS

Un servidor MCP corre con tus accesos. Si prefieres que Claude te guíe, copia este prompt:

```
Ayúdame a conectar un servidor MCP para [herramienta]. Antes de instalar nada, dime qué permisos pide, si es de una fuente oficial y cómo lo desconecto.
```

CHECKLIST

- ☐ Conecto solo lo que voy a usar.
- ☐ Distingo leer de editar y de borrar, y empiezo con solo lectura cuando se puede.
- ☐ Lo instalo desde una fuente de confianza, preferentemente la oficial.
- ☐ Revisé qué herramientas expone y no ofrece más de las que necesito.
- ☐ Leo qué va a hacer cada herramienta antes de aprobarla: Claude Code pide confirmación.
- ☐ Tengo pocos servidores: cada uno ocupa contexto, y con muchos Claude se confunde y gasta más.

RESUMEN

MCP es el estándar abierto que le da a Claude acceso a tus herramientas y datos. Cada servidor declara lo que ofrece, Claude decide cuándo pedirlo y el servidor lo ejecuta. Por eso conviene conectar pocos servidores, de fuentes confiables y con los permisos mínimos, y leer cada acción antes de aprobarla.

Sígueme en [Elkis Dev](#) para más IA y desarrollo, explicados simple.