

L U M B R E



Herramientas y MCP: cómo una IA toca tus sistemas

Materia: Desarrollo de Software con IA

07/10/2026

Antes de empezar

Tu IA no "está conectada a tu base de datos": eso es una ficción cómoda. Lo que existe es un convenio: la IA pide, una herramienta intermedia ejecuta, el sistema responde. MCP (Model Context Protocol) es el estándar que convierte ese convenio en enchufe universal —el USB de las herramientas de IA—. Entender la cadena IA → herramienta → aplicación → base de datos te deja ver dónde están los permisos, dónde la memoria y dónde exactamente puede filtrarse un dato que no debía.

QUÉ APRENDERÁS

- Explicar herramienta, API y MCP y el flujo IA → herramienta → aplicación → base de datos.

La IA no toca nada: pide que le toquen

Cuando un agente "lee tu calendario" o "consulta la base de datos", no hay un robot con tus credenciales: hay una **herramienta** —un programa pequeño expuesto a la IA con un nombre, una descripción y una firma de entrada/salida. La IA decide usarla, escribe la petición, la herramienta la ejecuta con sus propios permisos y devuelve el resultado. Todo el espectáculo ocurre en tres actos que ya conoces: pedir, hacer, responder.

ACTIVIDAD INTERACTIVA DISPONIBLE EN LUMBRE

1. La cadena completa



Y aquí llega MCP: el estándar del enchufe

Antes de **MCP** (Model Context Protocol), cada quien conectaba IAs a sistemas con adaptadores a medida: mil enchufes distintos para el mismo voltaje. MCP estandariza los tres actos: cómo la herramienta se describe («tengo query_sql, recibe una consulta, devuelve filas»), cómo recibe órdenes y cómo devuelve resultados. Un servidor MCP escrito una vez sirve a cualquier IA que hable el protocolo —como el USB: un conector, mil periféricos—.

Piénsalo como el portero de un edificio: la IA habla con el portero; el portero tiene las llaves, decide a qué pisos sube y copia en una nota lo que te encuentra. El problema no es la nota: es quién es el portero y qué llaves tiene.

Concepto	Qué es	Dónde está el peligro
Herramienta	la capacidad expuesta a la IA: un nombre, una descripción, unos parámetros	la descripción engaña: «busca clientes» puede estar haciendo un SELECT *
Servidor MCP	el programa que agrupa herramientas y ejecuta con sus credenciales	es el que tiene la llave buena: si se fuga, se fuga la llave
Permisos	lo que la herramienta del servidor puede hacer en el sistema	un «solo lectura» mal configurado que en realidad puede escribir
El contexto	lo que la IA ve de la respuesta: entra en su memoria de sesión	datos sensibles devueltos quedan expuestos en la conversación

Audita una conexión antes de encenderla

La ficha antes del código: auditar el enchufe antes de enchufarlo

Quiero conectar mi asistente con IA a la base de datos del proyecto via MCP.\nAntes de escribir cualquier código, responde la ficha de la conexión:\n\n1. HERRAMIENTAS: lista cada herramienta que el servidor expondra (nombre + descripción\n real de lo que ejecuta). Si una descripción dice "busca" y el código hace "lista todo",\n corrígela.\n2. PERMISOS: con que usuario de base de datos corre cada herramienta. Debe ser un usuario\n de SOLO LECTURA para consultas (crealo si no existe). Nada de administrador.\n3. MINIMIZACION: que campos devuelve cada herramienta? Si estoy buscando un cliente,\n por que regresa correo, telefono y direccion? Define la proyección mínima.\n4. LIMITES: máximo de filas por consulta y tiempo máximo. Sin límite, una consulta\n tonta puede tumbar la base o costar una fortuna.\n5. REGISTRO: cada llamada debe quedar en un log: quien, cuando, que pidió, cuantas filas\n salieron.\n\nEntregame la ficha completa y el código del servidor MCP cuando yo apruebe la ficha.

Para reforzar

Prueba

2. Tu agente «tiene acceso a la base de datos vía MCP». Al auditar, ¿qué configuración es la correcta?

- ☐ La IA conecta directo al motor de base de datos con el usuario administrador para que sea más rápido.
- ☐ El servidor MCP usa un usuario de solo lectura, devuelve columnas mínimas y registra cada llamada.
- ☐ El servidor MCP usa el usuario administrador pero limita las filas por consulta.
- ☐ La IA recibe un CSV con toda la base descargada al inicio de la sesión.

3. MCP es un protocolo de la empresa dueña de la IA, así que solo funciona con esa IA.

- ☐ Verdadero
- ☐ Falso

Detecta la descripción mentirosa

ACTIVIDAD
INTERACTIVA
DISPONIBLE EN
LUMBRE

4. Revisa la ficha de un servidor MCP que encontré en internet. Señala el problema que lo hace inaceptable:



5. Enumera las herramientas que tu proyecto expondría a un agente (buscar, listar, crear, consultar métricas...). Para cada una escribe su promesa en una línea: qué recibe, qué devuelve y qué NO devuelve. Si una de ellas escribes «los datos del cliente», acabas de encontrar tu primera corrección de minimización.

Conectar es fácil; conectar con manos ajenas y llaves propias es lo que merece una ficha de auditoría.

Referencia curricular

Materia:	Desarrollo de Software con IA
-----------------	-------------------------------

Versión interactiva completa (con actividades, videos y autoevaluación):



<https://empresa.lumbre.lat/object/fsi-m19-oa03>

Material educativo generado desde Lumbre · lumbre.lat