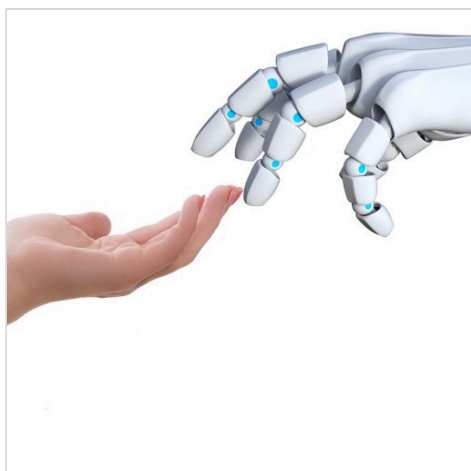


L U M B R E



Uso de herramientas y funciones

Grado: 8

Materia: Agentes de IA · Inteligencia Artificial

11/10/2026

Antes de empezar

Un modelo por sí solo no navega ni ejecuta código. Al darle un catálogo de herramientas y la capacidad de llamarlas con argumentos correctos, el agente extiende sus manos al mundo digital.

QUÉ APRENDERÁS

- Dotar a un agente de acceso a herramientas externas (APIs, calculadoras, buscadores) mediante llamadas a funciones bien estructuradas.

Uso de herramientas y funciones

Del texto a la acción

Dar herramientas a un agente es darle manos. El modelo sigue siendo un generador de texto, pero aprende a emitir órdenes estructuradas —«llama a esta función con estos argumentos»— que un ejecutor convierte en acción real.

VIDEO

Tool calling: conectar modelos a funciones

Vídeo en español que define herramientas con esquema y las invoca desde un modelo paso a paso.



Escanea para verlo en Lumbre

<https://www.youtube.com/watch?v=a1rfEQnHkm8>

Por qué un modelo necesita herramientas

- No accede a datos en tiempo real por sí mismo.
- No hace cálculos fiables ni ejecuta código.
- Las herramientas cubren sus puntos ciegos.

El catálogo de herramientas

Se define un conjunto de funciones con nombre, descripción y parámetros. El agente lee esas fichas y elige cuál invocar según la tarea.

Llamada a función

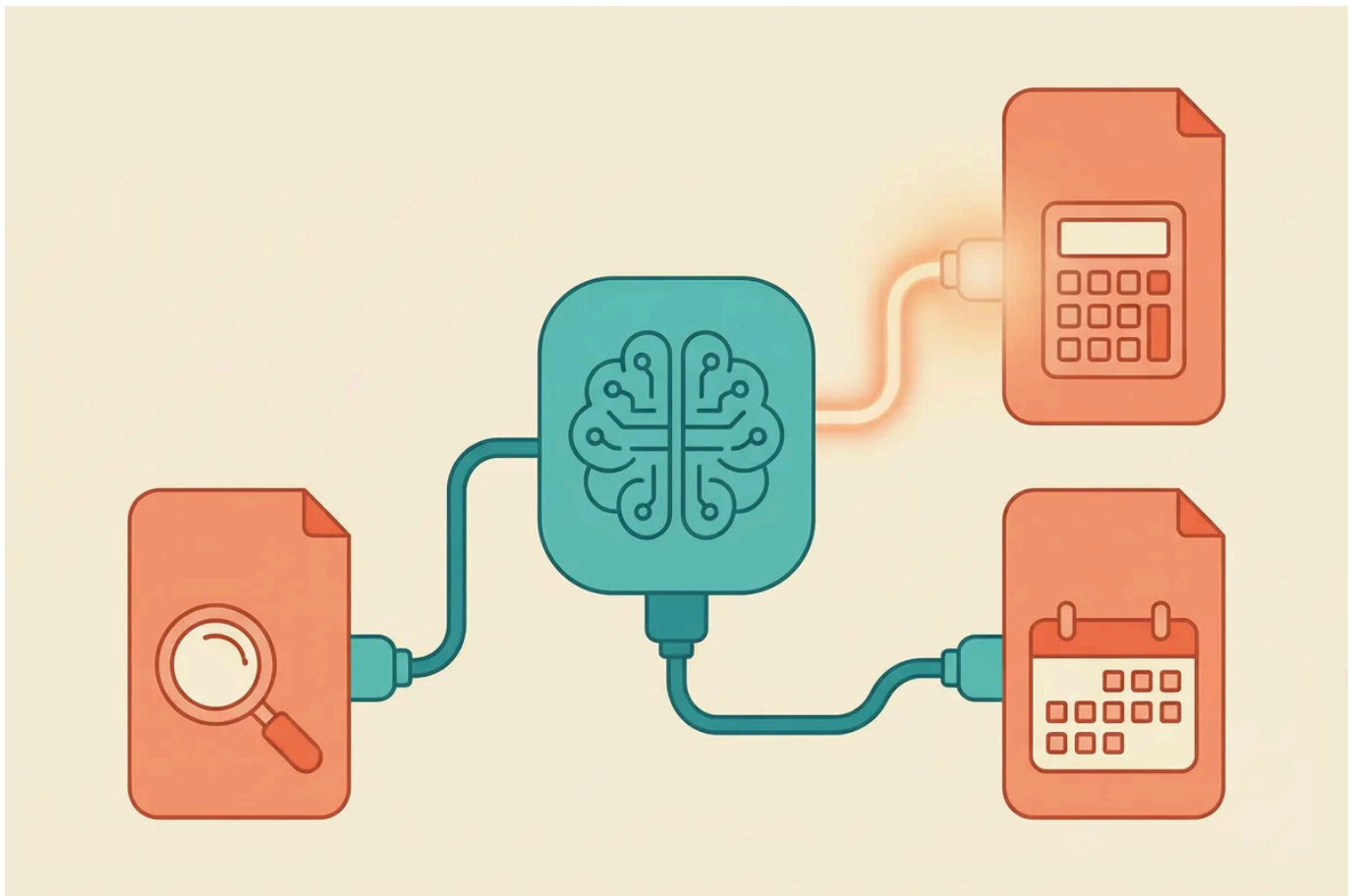
El modelo, en lugar de responder en prosa, emite una llamada estructurada: nombre de la herramienta y argumentos, normalmente en formato tipo JSON. Un ejecutor la lleva a cabo.

Argumentos correctos

La calidad del agente depende de que rellene bien los parámetros: tipos, formatos y valores plausibles. Un argumento torcido rompe la llamada o da resultados falsos.

Devolver la observación

El resultado de la herramienta regresa al agente, que lo integra en su razonamiento. Es el cierre del bucle herramienta-observación.



El modelo no toca el mundo: emite llamadas estructuradas que un ejecutor convierte en acciones reales sobre cada herramienta.

Encadenar herramientas

Para una tarea compleja, el agente puede necesitar varias llamadas en secuencia: buscar, extraer, calcular. Encadenarlas correctamente es parte del reto.

Elegir la herramienta adecuada

- Debe decidir si la tarea requiere buscar, calcular o escribir.
- Equivocarse aquí desperdicia pasos o falla el objetivo.
- Un buen catálogo describe cuándo usar cada herramienta.

Manejo de errores

Las herramientas fallan: tiempos de espera, datos vacíos, formatos raros. El agente debe reconocer el fallo y reintentar o cambiar de estrategia en vez de inventar el resultado.

No alucinar la salida

Un riesgo sutil es que el modelo «simule» la respuesta de la herramienta sin llamarla. Hay que forzar que use el resultado real devuelto.

Diseño de la interfaz

Buenas herramientas tienen contratos claros y poco ambiguos. La claridad de la firma reduce errores del agente al invocarla.

Seguridad de la acción

- Toda herramienta que escribe o envía debe estar vigilada.
- Limitar permisos y confirmar acciones irreversibles.
- Un agente con manos necesita rienda.

Errores frecuentes

- Firmas ambiguas: parámetros con nombres crípticos o descripciones vagas producen argumentos inventados.
- Dejar que el modelo simule el resultado de la herramienta en prosa en lugar de obligarlo a esperar la observación real.
- Otorgar permisos de escritura sin confirmación: un agente con manos necesita rienda en las acciones irreversibles.

Ejemplo resuelto: cotizar un envío con tres herramientas

«¿Cuánto cuesta enviar 3 kg de Madrid a Lisboa mañana?» exige datos que el modelo no puede saber de memoria.

1. El agente elige la herramienta de código postal y confirma las coordenadas de ambas ciudades.
2. Invoca la calculadora de tarifas con peso, origen, destino y fecha como argumentos tipados.
3. La API del transportista devuelve dos opciones: estándar y exprés, con sus plazos.
4. El agente integra las observaciones y redacta la comparación citando los números reales recibidos.
5. Si la tarifa devolviera error, reintentaría o cambiaría de transportista en vez de inventar el precio.

¿Para qué sirve en la realidad?

Copilotos que ejecutan código, asistentes que reservan vuelos y sistemas de atención que consultan el estado de un pedido son tool calling en producción: el puente entre el lenguaje y los sistemas de empresa.

1. ¿Qué añade la «llamada a funciones» a un agente basado en un modelo de lenguaje?

- ☐ memoria ilimitada dentro del modelo
- ☐ la capacidad de ejecutar acciones externas con argumentos estructurados
- ☐ eliminación de la necesidad de razonar
- ☐ acceso directo al peso del modelo

2. Un agente que alucina la respuesta de una herramienta sin llegar a llamarla está cometiendo un fallo de uso de herramientas.

- ☐ Verdadero
- ☐ Falso

ACTIVIDAD INTERACTIVA DISPONIBLE EN LUMBRE

3. Herramientas



4. Ordena el ciclo de una llamada a herramienta:

Elementos:

- seleccionar la herramienta adecuada a la tarea
- emitir la llamada con argumentos
- el ejecutor realiza la acción externa
- incorporar el resultado al razonamiento

Elegir	. . .
Invocar	. . .
Ejecutar	. . .
Integrar	. . .

API <https://en.wikipedia.org/wiki/API> Interfaz que permite a un programa invocar servicios de otro.

5. Une cada término del tool calling con su papel.

5.	ficha con nombre, descripción y parámetros de una acción	-----
5.	orden estructurada que emite el modelo para usarla	-----
5.	valores tipados que el agente pasa como entrada	-----
5.	resultado externo que regresa al razonamiento	-----

Opciones: herramienta · llamada a función · argumentos · observación

Del texto a la acción

Uso de herramientas

Catálogo

fichas claras

cuándo usar cada una

Llamada

argumentos tipados

ejecutor externo

Bucle

observación real

encadenar pasos

Control

reintentos ante fallo

permisos y confirmación

El mapa mental interactivo es interactivo en la versión online.



Función [https://en.wikipedia.org/wiki/Function_\(computing\)](https://en.wikipedia.org/wiki/Function_(computing)) El concepto computacional de caja negra con entrada y salida que el agente aprende a operar.

6. Tu agente a veces inventa el precio de un producto en vez de consultarlo. ¿Es un problema de diseño de la herramienta, del prompt o de la verificación? Razona.

Referencia curricular

Grado:	8
Materia:	Agentes de IA · Inteligencia Artificial

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



<https://univ.lumbre.lat/object/cdia-agent-002-uso-de-herramientas-y-funciones>

Material educativo generado desde Lumbre · lumbre.lat