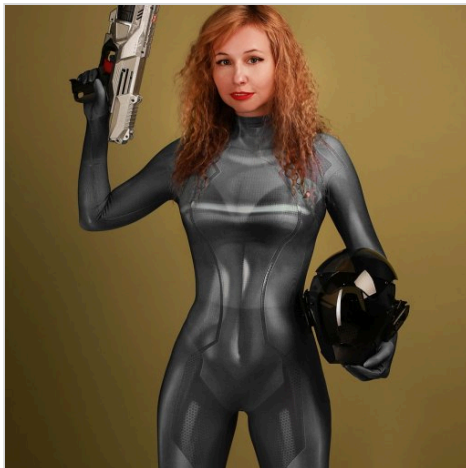


L U M B R E



Herramientas, memoria y contexto: lo que le das al agente

Materia: IA Aplicada, Vibe Coding y Negocios Digitales

07/10/2026

Antes de empezar

Un agente solo puede hacer lo que sus herramientas, memoria y contexto le permiten. Aquí aprendes a dotarlo de los adecuados y a ponerle límites.

QUÉ APRENDERÁS

- Entender qué son las herramientas, la memoria y el contexto de un agente, y cómo estas definen lo que puede y no puede hacer de forma segura.

El agente es tan capaz como lo que le das



Imagen libre de Wikimedia Commons (CC0, autor: Keinmy)

VIDEO

¿Qué son los Agentes de IA? Explicación sencilla

Un agente percibe, razona, actúa y evalúa. Este video lo resume en simples palabras; el curso lo lleva a tu caso empresarial.



Escanea para verlo en Lumbre

<https://www.youtube.com/watch?v=Xh1Jv33RIKw>

Un modelo de lenguaje, solo, predice texto. Lo que convierte a un agente en algo útil son tres ingredientes que tú le proporcionas: **herramientas** (acciones sobre el mundo: buscar, leer un archivo, llamar una API, escribir en tu CRM), **memoria** (lo que recuerda entre pasos y entre sesiones) y **contexto** (la información que tiene a la mano en este momento).

Si a un agente le das pocas herramientas, hace poco. Si le das demasiadas sin control, hace daño. El diseño está en el medio.

Herramientas = manos; memoria = cuaderno; contexto = la mesa de trabajo de hoy.

Ingrediente	Qué es	Ejemplo en un negocio
Herramienta	Una acción que el agente puede ejecutar	Enviar correo, consultar inventario
Memoria	Lo que el agente conserva	Recordar que el cliente pidió no lo llamen
Contexto	La información disponible ahora	El historial de este cliente en la conversación

La regla del mínimo necesario

Dale al agente solo las herramientas que la tarea requiere. Un agente de cotizaciones no necesita poder reembolsar dinero. Menos permisos, menos superficie para equivocarse.

1. Clasifica cada decisión de diseño para un agente de atención a clientes.

Elementos:

- Darle acceso a la API para crear tickets
- Guardar que este cliente ya fue escalado dos veces
- Pasarle el último pedido del cliente en la conversación actual
- Poder emitir reembolso sin aprobación
- Recordar las preferencias de idioma del cliente entre sesiones

Herramienta	. . .
Memoria	. . .
Contexto	. . .

Contexto no es lo mismo que memoria

El **contexto** es lo que el agente 've' ahora mismo; tiene un límite de tamaño y se llena con lo relevante del momento. La **memoria** es cómo decide qué guardar para después, más allá de esta conversación. Confundirlas genera agentes que o pierden el hilo, o guardan datos que no debían guardar.

Por eso la seguridad también vive aquí: si el contexto o la memoria incluyen datos personales o secretos, hay que acotar qué se guarda, dónde y por cuánto tiempo.

2. Quieres que un agente de ventas "recuerde" que un cliente es alérgico a ciertos productos, aunque pasen semanas entre conversaciones. ¿Qué necesitas?

- ☐ Solo más contexto en esta conversación.
- ☐ Memoria persistente que guarde esa preferencia entre sesiones.
- ☐ Una herramienta que envíe correos.
- ☐ Un modelo de lenguaje más grande.

ACTIVIDAD
INTERACTIVA
DISPONIBLE EN
LUMBRE

3. Un agente de soporte recibió una "configuración". Una decisión es un riesgo de seguridad. Márcala.



4. Para el agente que imaginaste en el objeto anterior, lista: dos herramientas que sí necesita, qué guardaría en memoria y qué datos NO debería ver nunca. Termina con un límite que le pondrías.

Piensa el límite como "no puede gastar más de X sin pedir permiso" o "máximo N acciones por tarea".

ACTIVIDAD INTERACTIVA DISPONIBLE EN LUMBRE

5. Antes del proyecto



Siguiente paso: *Proyecto* — diseñas de arriba abajo un agente para una tarea empresarial completa.

Referencia curricular

Materia:	IA Aplicada, Vibe Coding y Negocios Digitales
----------	---

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



<https://empresa.lumbre.lat/object/iav-c03-r01-0a03>

Material educativo generado desde Lumbre · lumbre.lat