WEBMCP EXPLICADO: QUÉ ES Y QUÉ NO ES



Posted on 23 de octubre de 2026 by Tomás

¿Cómo puede un asistente de IA **completar una tarea** en su web? Leer la información de un producto es una cosa. Elegir la variante correcta, preparar un carrito o dejar lista una reserva exige funciones adicionales. WebMCP está pensado para que las webs ofrezcan **una vía de acceso clara** para esas tareas, en lugar de obligar a los agentes a moverse solo por la interfaz visible.

Y ya no es teoría: Shopify ya ofrece herramientas WebMCP en todas sus tiendas Liquid. OpenAI admite estas funciones web en el navegador integrado de la aplicación de escritorio de ChatGPT, y Cloudflare ofrece una vista previa para desarrolladores que simplifica la integración. Eso sí, estas siglas no esconden otra herramienta para crear textos con IA ni un truco para posicionarse mejor en Google.

QUÉ ES WEBMCP

WebMCP son las siglas de Web Model Context Protocol. Se trata de una **propuesta de estándar web** con la que las webs pueden **ofrecer determinadas funciones como herramientas para agentes de IA**. Un agente es un asistente de IA que usa esas herramientas para ejecutar tareas, en lugar de limitarse a redactar una respuesta.

Una herramienta así podría, por ejemplo, buscar productos, consultar el estado de un pedido o rellenar una opción de un formulario. La web describe qué hace la función y qué datos necesita. Con esa descripción, el agente puede llamarla directamente. Técnicamente, estas herramientas se pueden registrar, entre otras vías, con JavaScript: cada una recibe un nombre, una descripción y un esquema fijo para sus datos de entrada.

Hay que tener en cuenta en qué punto está: WebMCP todavía no es un estándar aprobado del W3C. La especificación la publica el Web Machine Learning Community Group y figura **expresamente como borrador**. Que ya haya productos disponibles y que el proceso de estandarización siga abierto no es una contradicción.

CÓMO FUNCIONA WEBMCP EN UNA WEB

Pongamos una tienda online de muebles de oficina. **Un cliente le pide a su asistente de IA**: «Busca una silla de oficina negra por menos de 300 euros y añade al carrito un modelo disponible». Para un usuario, la tarea es sencilla: escribir la búsqueda, filtrar los resultados, elegir el producto y pulsar el botón del carrito.

Sin una interfaz adecuada, un agente en el navegador tiene que averiguar primero cómo funciona la página. Puede, por ejemplo, analizar la estructura de la página e imitar clics o la escritura de texto. Los controles poco habituales, los diálogos adicionales o los cambios de diseño pueden complicar el proceso. WebMCP añade otra vía más directa: funciones que la web ofrece y que el agente puede llamar sin rodeos.

En el ejemplo, el agente podría usar herramientas para buscar en el catálogo, consultar un producto y gestionar el carrito. Shopify ofrece para ello, entre otras, search_catalog, get_product y update_cart. El agente decide qué función necesita a partir del encargo y de las descripciones de las herramientas. Las acciones se realizan en la sesión abierta del cliente: los cambios afectan al carrito que el cliente ve en pantalla.

Paso	Quién actúa	Qué ocurre
1	Usuario	Da la instrucción a su asistente de IA.
2	Agente de IA	Elige la herramienta adecuada entre las que ofrece la web.
3	Web	Ejecuta la acción a través de la interfaz WebMCP del navegador (herramientas definidas y datos estructurados).
Resultado	Usuario y agente	La web mantiene su interfaz normal: el cliente ve y puede revisar lo que ha hecho el agente.

La interfaz normal se mantiene. El cliente puede seguir navegando por la tienda y revisar el resultado. WebMCP añade a la web un acceso para el agente, mientras usuario y asistente trabajan con la misma página abierta. Resulta especialmente útil cuando usuario y agente se reparten una tarea y conviene ir revisándola sobre la marcha.

¿Quiere preparar su web y su empresa para los agentes de IA?

Descubra cómo, con nuestro servicio AI-Connect, los asistentes de IA compatibles pueden acceder al conocimiento y a las funciones que su empresa autorice.
AI-Connect

QUÉ OFRECEN YA SHOPIFY, OPENAI Y CLOUDFLARE

Cada uno de estos tres proveedores cumple un papel distinto. Shopify ofrece funciones en las webs de sus tiendas, OpenAI ofrece un entorno en el que un asistente puede usarlas y Cloudflare simplifica la implementación técnica. Conviene tener clara esta diferencia para valorar qué es posible ya hoy en su propia web.

SHOPIFY: HERRAMIENTAS EN TODAS LAS TIENDAS LIQUID

En agosto de 2026, Shopify activó herramientas WebMCP en todas las tiendas Liquid (y en la vista previa para desarrolladores de Hydrogen), es decir, en todas las tiendas creadas con las plantillas Liquid de Shopify. Los comerciantes no tienen que instalar ni configurar nada. Las herramientas cubren la búsqueda en el catálogo, la elección de variantes, los cambios en el carrito y el paso a la caja. Por ahora solo funcionan con agentes compatibles en navegadores basados en Chromium, a través de una prueba de origen (origin trial).

Hay un matiz clave: el límite entre el carrito y el pedido. La herramienta de la tienda solo lleva hasta la caja. Para los procesos de pago compatibles, Shopify documenta herramientas propias que leen y actualizan el pago y cierran el pedido una vez que el comprador lo confirma. Una selección de productos preparada por el agente no es, por tanto, un pedido que se lance solo.

OPENAI: CHATGPT PUEDE USAR HERRAMIENTAS DE LA WEB

OpenAI llama a su implementación de WebMCP «site tools» (herramientas del sitio). En el navegador integrado de la aplicación de escritorio de ChatGPT, el asistente detecta y usa las herramientas adecuadas de la web que tiene abierta. Lo que está disponible depende, entre otras cosas, de la cuenta, del modelo y de la página. Por eso, que «ChatGPT admita WebMCP» no significa que cualquier usuario pueda manejar así cualquier web.

Además, conviene probar cada integración. Según la documentación de OpenAI, el navegador integrado puede detectar herramientas también en páginas incrustadas (iframes), del mismo dominio o de otros, siempre que cada marco use un contexto seguro y tenga los permisos necesarios. Aun así, un formulario de reserva integrado desde un servicio externo no tiene por qué funcionar de entrada: la implementación tiene que encajar con el navegador y el agente previstos.

CLOUDFLARE: INTEGRACIÓN SIN TOCAR EL SERVIDOR WEB

La vista previa para desarrolladores de Cloudflare añade a las páginas que se sirven un pequeño script que registra paquetes de herramientas seleccionados. El código de la web en el servidor no cambia. Entre los primeros paquetes están la conexión con servidores MCP existentes y la lectura de la información de origen de las imágenes.

La integración resulta así más sencilla, pero no prepara cualquier proceso de negocio para los agentes: si su web no tiene una reserva de citas que funcione, el script tampoco la crea. Lo que puede hacer un agente sigue dependiendo de las herramientas disponibles.

QUÉ NO ES WEBMCP

Hay muchos términos parecidos en torno a la búsqueda con IA, las interfaces y la automatización, y eso complica las cosas sin necesidad. Para su web conviene separar tres preguntas: ¿cómo la encuentran?, ¿cómo se accede a su información? y ¿cómo se usan sus funciones? **WebMCP** se ocupa sobre todo de la interacción en una web que el agente ya está visitando.

NO SUSTITUYE AL SEO NI AL GEO

WebMCP no decide por qué una empresa aparece en una respuesta de búsqueda. Las herramientas quedan disponibles para un agente compatible cuando visita la web en cuestión. Una web más fácil de manejar para los agentes **no obtiene por ello ninguna ventaja automática en el ranking ni en las recomendaciones de la IA**. Una web puede ofrecer funciones muy fáciles de usar y, aun así, apenas recibir visitas.

Para los resultados de búsqueda con IA de Google, según la propia Google, siguen valiendo las recomendaciones básicas de SEO. Para aparecer en las vistas creadas con IA o en el modo IA no hacen falta optimizaciones especiales; siguen contando los fundamentos de siempre, como el E-E-A-T. WebMCP no sustituye ni los contenidos útiles ni una web que los buscadores puedan rastrear e

indexar sin problemas.

Nivel	Pregunta clave	Ejemplos	Enfoque
1. Visibilidad	¿Cómo se hace visible una empresa en los buscadores y en las respuestas de la IA?	Contenidos útiles, buena base técnica, entidades, notoriedad de marca y fuentes fiables	SEO / GEO
2. Conexión de datos	¿Cómo pueden los sistemas de IA autorizados consultar y procesar los datos de una empresa de forma estructurada?	Información de productos, servicios, disponibilidad y conocimiento de la empresa	API / MCP
3. Uso de funciones	¿Cómo puede un agente de IA usar funciones en una web que ya tiene abierta?	Filtrar productos, actualizar carritos, rellenar formularios y preparar citas	WebMCP

Los niveles pueden solaparse: una interfaz de datos también puede permitir acciones, y WebMCP puede consultar información sin cambiar nada. Aun así, la distinción ayuda a planificar, porque ser más fácil de encontrar y ser más fácil de usar son objetivos distintos.

NO ES LO MISMO QUE UN SERVIDOR MCP

El Model Context Protocol, MCP para abreviar, **conecta aplicaciones de IA con sistemas externos**. A través de él se puede, por ejemplo, consultar información de bases de datos o ejecutar tareas en otras aplicaciones. **Es decir, MCP no se limita a leer datos**. WebMCP, en cambio, se centra en las funciones que una web ofrece en el navegador.

Pregunta	MCP	WebMCP
¿Dónde se ofrecen las funciones?	En un servidor MCP local o remoto.	En la página web abierta en el navegador.
¿Hace falta tener una web abierta?	No necesariamente.	Sí. Las herramientas dependen del contexto de cada página.
¿Qué se puede hacer?	Consultar información y ejecutar acciones en los sistemas conectados.	Consultar información y ejecutar acciones en la web, dentro de la sesión abierta del usuario.
¿Para qué sirve este enfoque?	Para conectar servicios y sistemas de la empresa.	Para que usuario y agente trabajen juntos en una web.

Ambos enfoques pueden complementarse. Una empresa no tiene por qué elegir uno de los dos: la

clave está en dónde se necesita la función. Google deja claro que WebMCP no es ni un sustituto ni una simple extensión de MCP.

¿Quiere que los asistentes de IA puedan usar el conocimiento de su empresa sin visitar su web? Con AI-Connect ponemos información autorizada y funciones definidas a disposición de los asistentes de IA compatibles, a través de una interfaz gestionada para su empresa.

NO ES UN CHATBOT QUE SE INSTALA EN LA WEB

WebMCP no hace que aparezca una ventana de chat en su web. Lo que permite es que un asistente compatible acceda a las funciones que la web pone a su disposición. Del mismo modo, una web creada con IA no incluye herramientas WebMCP por defecto: cómo se ha creado una web y si un agente puede usarla después son dos cuestiones distintas.

PARA QUÉ EMPRESAS PUEDE SER INTERESANTE WEBMCP

En nuestra opinión, merece la pena estudiarlo con calma sobre todo cuando los visitantes tienen que dar varios pasos seguidos en una web. Algunos casos de uso posibles son **catálogos de productos amplios, configuradores, reservas de citas y áreas de cliente**. La utilidad está en facilitar una tarea concreta, no en poner la etiqueta «IA» al mayor número posible de funciones.

En un distribuidor técnico, por ejemplo, un agente podría comparar componentes según unas características dadas y preparar una solicitud de presupuesto. Una empresa de servicios podría permitir consultar las citas libres para un servicio concreto. En un área de cliente, el agente podría abrir un pedido anterior y preparar a partir de él una nueva solicitud. Son aplicaciones posibles, y todas requieren las funciones adecuadas y los permisos de acceso necesarios.

En una web corporativa pequeña, cuya función principal es presentar los servicios y los datos de contacto, nuestras prioridades son otras. Si los clientes potenciales todavía no entienden la oferta o no ven claro cómo contactar, hay que empezar por ahí.

LÍMITES Y RIESGOS DE WEBMCP

TODAVÍA NO FUNCIONA EN TODAS PARTES

El directorio oficial de implementaciones recoge, entre otros, ChatGPT para escritorio, versiones de prueba para Chrome y Edge y compatibilidad experimental en Brave. Por tanto, no está disponible de forma general en todos los navegadores habituales. En un proyecto web no basta con registrar las herramientas: hay que probarlas con los agentes y navegadores que se vayan a usar de verdad.

UNA BUENA DESCRIPCIÓN DE LA HERRAMIENTA NO BASTA COMO PROTECCIÓN

Una herramienta debe dejar claro si solo consulta información, si prepara un proceso o si ejecuta una acción vinculante. «Ver cita» y «reservar cita» no deben poder confundirse. Google recomienda descripciones claras de las funciones, validaciones fiables de los datos introducidos y mensajes de error fáciles de entender. Una descripción bien redactada no sustituye a las comprobaciones en el código.

Además, existe **el riesgo de contenidos manipulados**. En la llamada inyección de instrucciones (prompt injection), las órdenes ocultas en el contenido de una web o en las respuestas de una herramienta pueden intentar desviar al agente de su encargo real. Google advierte expresamente de este problema. Para las acciones con consecuencias, los desarrolladores deberían prever mecanismos de protección y confirmaciones adicionales, en lugar de fiarse solo del comportamiento del modelo.

OpenAI revisa además las llamadas a las herramientas del sitio y describe controles contra la cesión de datos no autorizada y contra acciones que vayan más allá del encargo del usuario. Estos controles reducen riesgos, pero no hacen fiable cualquier web ni cualquier respuesta de una herramienta. En compras, cambios en datos de clientes u otros procesos delicados, el proceso tiene que seguir bajo control.

QUÉ SIGNIFICA WEBMCP PARA SU WEB

WebMCP ya ha llegado a productos reales, pero todavía no se puede usar en todas partes, y cada función necesita límites claros. Si compensa el esfuerzo depende menos de la tecnología que de una pregunta: **¿en qué puntos los asistentes de IA no pueden ayudar hoy de forma fiable a sus clientes?** Estas son algunas señales habituales:

- Los clientes se atascan una y otra vez en un proceso de su web, por ejemplo al buscar un producto, al configurarlo o al pedir cita.
- Las mismas preguntas que requieren asesoramiento llegan constantemente a su equipo, por ejemplo sobre usos, compatibilidades o la variante adecuada.
- Parte del conocimiento técnico importante no está en la web, sino en fichas técnicas, listas de precios o la experiencia de sus empleados.
- La información cambia a menudo (disponibilidad, plazos de entrega o citas libres) y, sin una fuente actualizada, un asistente de IA solo puede hacer estimaciones.
- Después del asesoramiento hay un siguiente paso claro, como una solicitud o un presupuesto, que un asistente podría preparar.

Solo el primer punto tiene que ver directamente con el manejo de su web. Para los demás también puede tener sentido un acceso a través del cual los asistentes de IA conectados consulten información autorizada y preparen solicitudes sin necesidad de abrir su web. Es el segundo nivel de la tabla anterior. Si no se reconoce en ninguno de estos puntos, lo normal es que le aporten más unos contenidos mejores o una navegación más clara.

CONCLUSIÓN: WEBMCP AFECTA AL USO DE SU WEB, NO AUTOMÁTICAMENTE A SU VISIBILIDAD

WebMCP da a los agentes de IA un acceso definido a las funciones de una web. Las implementaciones actuales demuestran que el enfoque ya se puede usar en la práctica, mientras el estándar y la compatibilidad siguen avanzando. Para las empresas con procesos digitales complejos puede merecer la pena hacer una prueba. Lo que no existe es una obligación general de implantarlo.

Para planificarlo, todo empieza por la tarea de su cliente: ¿qué debería funcionar mejor en su web y dónde surgen hoy las dificultades? Con eso claro, se puede valorar si la opción adecuada son mejores contenidos, una navegación revisada, una interfaz de datos o WebMCP. En la siguiente parte de esta serie de artículos verá qué conviene revisar en su web ahora que los agentes de IA también la visitan.

En **Wisea** le ayudamos a desarrollar su web y a decidir qué papel deben tener en ella los agentes de IA. Analizamos juntos su web y los procesos que hay detrás, y vemos **qué mejoras ayudan de**

verdad a sus clientes y qué complementos técnicos tienen sentido para ello. ¿Quiere saber si WebMCP encaja en su proyecto? No dude en ponerse en contacto con nuestra agencia.