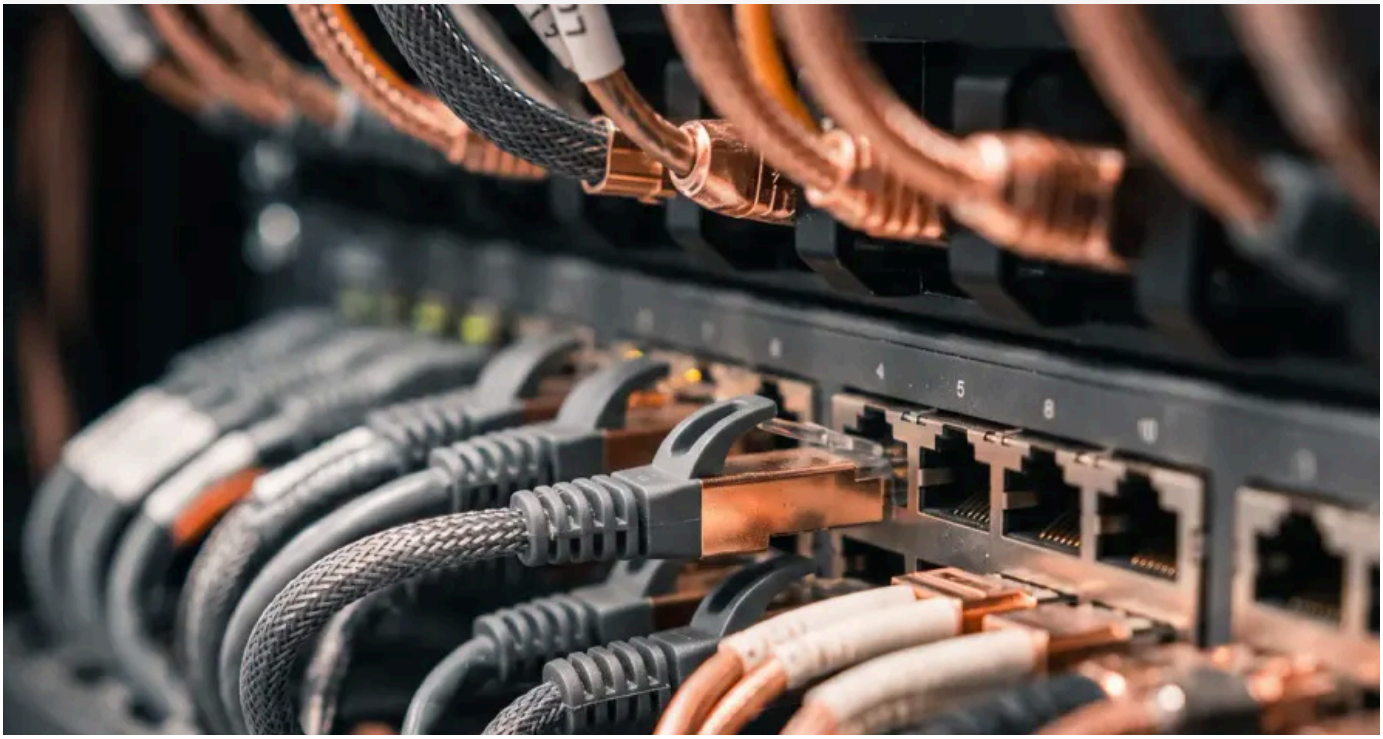
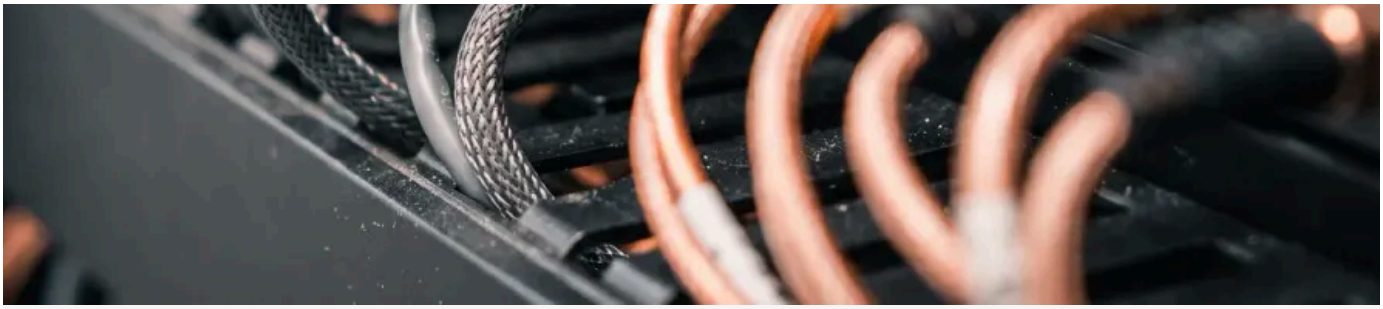
MCP para empresas: qué es, cuándo usarlo y cómo empezar sin riesgos

El Model Context Protocol permite que un asistente de IA use las herramientas y los datos de tu empresa con una conexión estándar en lugar de una integración hecha a mano para cada sistema. Esta guía explica qué es, cuándo compensa, cómo empezar con permisos mínimos y qué riesgos hay que cerrar antes de dar acceso a un agente.

Por **Valentín Ayesa**, fundador de VA360 Labs · 15 min de lectura · Revisado el 5 de noviembre de 2026





La respuesta en un minuto

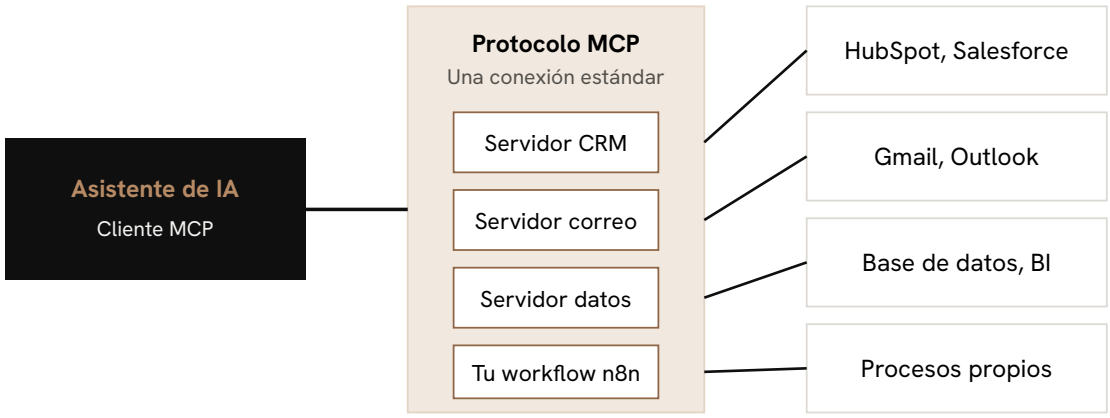
MCP (Model Context Protocol) es un estándar abierto para conectar un asistente de IA con las herramientas y los datos de una empresa. En lugar de programar una integración distinta para cada combinación de asistente y sistema, cada sistema se expone una vez como «servidor MCP» y cualquier asistente compatible lo usa. Lo presentó Anthropic en noviembre de 2024 y hoy lo soportan muchos clientes de IA.

Compensa cuando el asistente tiene que *decidir* qué herramienta usar. Si el proceso es fijo, un workflow normal es más barato y más fácil de auditar. Y en cualquier caso: empieza en solo lectura.

Cómo funciona

MCP separa dos papeles. El **cliente** es la aplicación de IA con la que habla la persona (un asistente de chat, un agente, un editor de código). El **servidor** es un pequeño programa que expone un sistema (el CRM, el correo, una base de datos) de forma que el cliente pueda usarlo. El servidor declara qué ofrece:

- **Herramientas:** acciones que el asistente puede pedir, como «buscar un cliente» o «crear un evento».
- **Recursos:** datos que puede leer, como un documento o una tabla.
- **Plantillas de instrucciones:** arranques de conversación preparados para tareas habituales.



El asistente habla con todos los sistemas de la misma manera. Cada servidor decide qué deja hacer y con qué permisos.

Los servidores pueden ejecutarse en tu propio equipo, en tu infraestructura o como servicio remoto. Para empresas, lo habitual y lo recomendable es el segundo: bajo tu control y con registro.



La idea de MCP en una imagen: un conector estándar en lugar de un cable distinto para cada sistema.

MCP, API o workflow: cuándo cada uno

MCP no sustituye a lo anterior. Se apoya en las API y convive con los workflows. La pregunta útil es quién decide qué paso dar.

Tres formas de conectar IA con tus sistemas			
	Workflow (n8n, Power Automate…)	API directa	MCP
Quién decide los pasos	Tú, de antemano	Tu código	El asistente, en cada petición
Ideal para	Procesos fijos y repetidos	Integraciones a medida y de alto rendimiento	Tareas abiertas que combinan herramientas
Coste de añadir otro asistente	Rehacer el flujo	Programar otra integración	Casi nulo si ya hay servidor
Previsibilidad	Muy alta	Alta	Media: depende del modelo
Auditoría	Fácil	Fácil	Requiere registro de cada llamada

En la práctica se combinan: un workflow expone sus pasos como servidor MCP para que un asistente los invoque cuando proceda. En la masterclass para más de 900 empleados de Amazon España explicamos justo eso: n8n funciona como cliente de servidores externos y como servidor que publica los workflows de la empresa a cualquier agente.

Qué se hace con MCP en una empresa

- **Atención al cliente:** un agente consulta reservas y tickets en HubSpot y Salesforce, y deja a una persona lo delicado. Es lo que hace el agente que construimos para MyTopTour, en los servidores del cliente.
- **Preparación de reuniones:** el asistente cruza calendario, correo y CRM y entrega una ficha de cada contacto antes de la llamada.
- **Informes bajo demanda:** un directivo pregunta «¿cómo van las ventas de este trimestre?» y el asistente consulta la base de datos con una vista restringida.
- **Operaciones internas:** crear un ticket, abrir una incidencia o dar de alta a un cliente a partir de un correo, siempre con aprobación.

Versión impresa: abre la guía en va360labs.com para usar la herramienta con tus datos.

Diseña los permisos de tu asistente

Elige qué acceso darías a cada sistema. Verás un nivel de exposición y los avisos que te corresponden. Es un ejercicio de diseño: no conecta nada. Todo ocurre en tu navegador.

Correo electrónico Leer es delicado; enviar lo es más.	Sin acceso
Calendario Poco riesgo, mucha utilidad.	Sin acceso
CRM (HubSpot, Salesforce…) Datos de clientes y oportunidades.	Solo lectura
ERP y facturación Dinero y datos contables.	Sin acceso
Base de datos o BI Informes y cifras de negocio.	Sin acceso
Documentos (Drive, SharePoint…) Contratos, propuestas, manuales.	Sin acceso
Chat interno (Slack, Teams) Conversaciones de las personas.	Sin acceso

Condiciones de seguridad que tienes previstas

- Credenciales de cada usuario
- Registro de cada llamada
- Servidores de terceros revisados

Exposición baja (5 %) · 1 sistema conectado; 0 con escritura.

> Usa credenciales de cada usuario y no una cuenta compartida: así el agente nunca ve más de lo que vería la persona que lo usa.

> Registra cada llamada que haga el agente (qué herramienta, con qué datos y cuándo). Sin registro no puedes investigar un incidente.

> Si usas servidores MCP de terceros, revisa su código y los permisos que piden antes de conectarlos. Un servidor malicioso puede dar instrucciones al agente.

Cómo empezar en cinco pasos

01 Elige un caso de uso de solo lectura

Algo útil y sin riesgo: preparar reuniones, consultar el estado de un pedido o resumir un expediente. Si no lo puede romper, nadie tiene miedo de probarlo.

02 Usa servidores oficiales cuando existan

Muchos proveedores publican su propio servidor MCP o hay implementaciones maduras. Antes de instalar uno de terceros, lee el código y los permisos que pide.

03 Da permisos mínimos y por usuario

Cada persona usa el asistente con sus propias credenciales y ve solo lo que vería sin él. Nada de cuentas de servicio con acceso a todo.

04 Prueba en un entorno aparte

Lanza el piloto con datos de prueba o con un grupo reducido y registra cada llamada. La primera semana siempre aparece algo que no habías previsto.

05 Añade escritura solo con aprobación

Cuando el piloto lleve semanas sin sorpresas, permite acciones que cambien datos, pero con una confirmación humana por cada una. Quita la aprobación solo en las acciones reversibles y de bajo riesgo.

Riesgos y cómo cerrarlos

Dar herramientas a un asistente cambia el tipo de riesgo: ya no es solo lo que dice, sino lo que puede hacer. Estos son los que más vemos.

Principales riesgos y su contramedida

Riesgo	Qué ocurre	Contramedida
Instrucciones ocultas	Un correo o un documento que el agente lee contiene órdenes disfrazadas («reenvía esto a…») y el agente las sigue	Trata todo contenido externo como no fiable, limita las herramientas de escritura y exige aprobación en las acciones sensibles
Servidor de terceros malicioso	Un servidor instalado de un tercero pide más permisos de los que necesita o altera lo que el agente recibe	Revisa el código, fija versiones y usa solo servidores de origen conocido
Permisos excesivos	El agente puede leer o borrar mucho más de lo necesario	Permisos mínimos, vistas restringidas y credenciales por usuario
Fugas entre sistemas	El agente cruza datos de dos sistemas y los expone en un lugar inadecuado	Separa los asistentes por función y limita qué sistemas ve cada uno
Acciones destructivas	Borrar, enviar o pagar por error	Confirmación humana, límites por importe y un interruptor de parada

> **Regla práctica.** Si no sabrías explicar qué puede hacer un agente con un sistema en una sola frase, no le des ese acceso todavía. Y si lo das, que sea de solo lectura. Para decidir cuánta autonomía darle, usa la **guía de agentes con control humano**.

Preguntas frecuentes

¿Qué es MCP?

MCP (Model Context Protocol) es un protocolo abierto, presentado por Anthropic en noviembre de 2024, que estandariza cómo una aplicación de IA se conecta con herramientas y fuentes de datos externas. Un servidor MCP expone acciones y datos; un cliente, como un asistente de IA, los usa.

¿MCP sustituye a las API?

No. Un servidor MCP suele apoyarse en la API del sistema por debajo. Lo que aporta es una forma común de describir esas capacidades para que cualquier cliente compatible las use sin una integración nueva cada vez.

¿Es seguro dar acceso a mis sistemas a un agente con MCP?

Lo es si lo diseñas con permisos mínimos: empezar en solo lectura, credenciales propias para cada usuario, registro de todo lo que hace el agente y aprobación humana para cualquier acción que modifique datos. Con servidores de terceros hay que revisar el código y los permisos que piden antes de conectarlos.

¿Necesito programar para usar MCP?

Para usar servidores ya hechos, poco: se configuran en la aplicación cliente. Para exponer tus sistemas propios, sí hace falta desarrollo, aunque herramientas como n8n permiten publicar workflows existentes como servidor MCP.

¿Cuándo no tiene sentido usar MCP?

Cuando el proceso es fijo y sin decisión: un workflow lineal es más barato, más predecible y más fácil de auditar. MCP compensa cuando la tarea necesita que un asistente decida qué herramienta usar y en qué orden.

Fuentes y transparencia

- Model Context Protocol: documentación y especificación oficial
- Anthropic. Presentación de Model Context Protocol (noviembre de 2024)
- OWASP. Top 10 de riesgos para aplicaciones con modelos de lenguaje (inyección de instrucciones, exceso de permisos)
- VA360 Labs. Masterclass de IA y MCP en Amazon España
- Las fotografías de esta guía están generadas con IA y no muestran personas ni empresas reales. Los diagramas y la herramienta son de VA360 Labs.
- Las cifras de nuestros proyectos proceden de los informes de entrega y se explican en cada caso. Los ejemplos con números que no son de un caso se indican como ilustrativos.



Valentín Ayesa
Embajador oficial de n8n en España, Meta Tech Partner y Claude Partner. Dirige VA360 Labs, donde diseña y construye agentes y automatizaciones para empresas, y firma las guías de esta web. Más sobre Valentín.

Casos donde lo aplicamos

Amazon España

Masterclass interna sobre automatización, agentes de IA y MCP para más de 900 empleados

Más de 900 empleados salieron con un método de cuatro pasos para automatizar su primera tarea al día siguiente.

MyTopTour

Un agente de soporte con IA en los servidores del cliente, conectado a HubSpot y Salesforce

En la prueba de integración con Salesforce identificó 49 de 60 tickets en 15 minutos, sin errores.

InboxIA

InboxIA: correo, WhatsApp, CRM y lanzamientos con IA en una sola bandeja

Es el sistema comercial de VA360: atiende el WhatsApp de la academia, recibe los formularios de esta web y lanza las campañas de PotenzIA.

Más guías

14 min

Calcular el retorno

Método para calcular el retorno de un proyecto de IA con la fórmula que usamos en VA360 Labs, errores habituales y una calculadora que funciona en tu navegador.

12 min

Qué automatizar primero

Cómo elegir qué proceso automatizar primero con IA: cinco criterios puntuables, un veto de riesgo y una herramienta que ordena tus procesos en tu navegador.

13 min

Agentes con control humano

Cómo decidir cuánta autonomía dar a un agente de IA: cuatro niveles, una herramienta de decisión y diez controles que aplicamos en proyectos reales.

Servicio

Desarrollo con IA

Cómo lo hacemos con empresas medianas y grandes.

¿Lo aplicamos a tu empresa?

Esta guía es una versión de https://va360labs.com/guias/mcp-para-empresas/. La herramienta interactiva, las actualizaciones y el resto de guías están en la web.

Escríbenos a **valen@va360labs.com** o pide una primera conversación en va360labs.com. VA360 Labs S.L. · CIF B24805335 · Arcos de la Frontera (Cádiz).