# El cliente agéntico

*¿Qué pasa cuando su cliente le manda un agente?*

> *«Su cliente ya delega en agentes de IA, y un agente pide siempre. Bloquear pierde negocio, tolerar cuesta concesiones que nadie mide: la postura se decide por recorrido, con datos.»*

QUÉ ES

## Un cliente con agente propio

Un agente personal de IA investiga, compra, reclama o contrata por el cliente. Llega por cuatro caminos: le investiga con un asistente, compra con un agente, pide servicio y su agente habla con el de la compañía. Su tráfico se parece al de un ataque, pero actúa de forma legítima.

**Implicación:** ¿Sabe su compañía cuántos de sus contactos con clientes los hace ya un agente?

**Riesgo:** Sin decisión, cada equipo bloquea o tolera por su cuenta y nadie suma el coste.

QUÉ PROPONE

## Una postura por recorrido

En venta, servicio, concesiones y bajas, el consejo fija si bloquea, tolera o atiende al agente por un canal identificado: identidad del agente y de quien responde de él, permisos revocables, límites, registro y reglas de concesión fuera del modelo. Se exige con exposición directa a clientes.

**Implicación:** ¿Quién es el dueño de negocio de la postura ante agentes en cada recorrido?

**Riesgo:** Sin canal identificado, nadie puede probar qué autorizó el cliente a su agente.

CÓMO SE COMPRUEBA

## Exposición medida y canal probado

La exposición económica se calcula como escenario aparte, con datos propios, y nunca suma al neto. El tráfico de agentes se detecta y se etiqueta, y las concesiones que resuelve se miden. El canal se prueba antes y siempre con clientes sintéticos, simulación de usuarios y red teaming.

**Implicación:** ¿Ha probado su compañía su canal de atención contra agentes que intentan abusar de él?

**Riesgo:** Un canal sin probar se prueba, de hecho, con los clientes.

### CUATRO PREGUNTAS PARA EL CONSEJO

1. **¿Qué recorridos atienden ya agentes de clientes?**
   Tráfico de agentes detectado y etiquetado por recorrido, con su volumen, su coste y las concesiones que resuelve, separado del tráfico humano.
2. **¿Qué postura hemos fijado en cada recorrido?**
   Postura escrita por recorrido (bloquear, tolerar o atender), con su dueño de negocio y su revisión anual.
3. **¿Cuánto nos costaría que todos pidieran lo que les corresponde?**
   Escenario de exposición con datos propios, informado aparte del neto, con fecha y supuestos; sin dato propio se dice «sin dato».
4. **¿Qué hemos probado antes de abrir el canal?**
   Escenarios con clientes sintéticos por recorrido, hallazgos con responsable y fecha, y una muestra de contactos reales para contrastar.

### QUÉ FALLA SI NO SE GOBIERNA

| QUÉ FALLA | NIVEL | QUÉ HACER |
|---|---|---|
| Concesiones pagadas que nadie mide | ALTO | Medir las concesiones que resuelve cada agente |
| Acciones del agente de un cliente que nadie puede atribuir | ALTO | Registrar cada acción con su permiso |
| Neto inflado por no restar las concesiones adicionales | ALTO | Informar la exposición como escenario aparte |
| Reglas de concesión que decide el modelo | MEDIO | Aplicar las reglas fuera del modelo |
| Agentes bloqueados sin saber qué negocio se pierde | MEDIO | Fijar la postura con datos por recorrido |
| Canal abierto sin probar contra abusos | MEDIO | Probar con clientes sintéticos antes y siempre |

### PARA SEGUIR LEYENDO

**Seguridad de IA y agentes**
Documento 35 · agentes de terceros que actúan por el cliente

**Reglas de medición del valor**
Documento 40 · exposición económica

**Tesis de IA, ambición y apetito**
Documento 13 · postura ante agentes de clientes

**When Your Customer Sends an Agent**
Bain & Company · 10-11-2026


Fernando García Varela · CC BY 4.0 · Versión 0.x, en revisión

*Ayuda genérica y gratuita, sin revisión jurídica para ningún caso concreto: cada organización la adapta, identifica la normativa que le aplica y responde de su cumplimiento. No es asesoramiento ni certificación. En la máxima medida permitida por la ley, el autor no asume responsabilidad por los efectos de su aplicación.*