

COPILOT AGENTS: CÓMO HACER QUE FUNCIONEN

Dado que los Agentes aún presentan errores importantes aquí va una solución que ya estamos aplicando con éxito

¿Qué son los Copilot Agents y por qué nos interesan?

Microsoft ha lanzado una herramienta muy prometedora llamada **Copilot Agents**, diseñada para ayudarnos a automatizar tareas complejas conversando con una inteligencia artificial.

La idea es sencilla, pero potente: tener un asistente virtual que pueda hacer cosas por nosotros, como leer datos, analizarlos, cruzar información de distintos documentos y darnos respuestas útiles, todo a través de una conversación en lenguaje natural.

¿Qué problema hemos detectado?

Cuando intentamos usar estos agentes en tareas reales (por ejemplo, analizar dos tablas de Excel y sacar conclusiones), nos encontramos con algo que no esperábamos:

- El agente a veces falla en tareas muy simples.
- Da respuestas diferentes aunque le demos los mismos datos.
- Se olvida de cosas que le hemos dicho hace un momento.
- Se confunde cuando le damos demasiada información a la vez.

Esto, lógicamente, genera **desconfianza**, especialmente si queremos usarlo para trabajo serio o compartir resultados con un cliente.

¿Por qué pasa esto?

Después de muchas pruebas y análisis con el equipo técnico, descubrimos lo siguiente:

1. El agente no lo recuerda todo: solo puede procesar una cierta cantidad de información por turno. Si se le da demasiado, olvida partes importantes y se queda sin tiempo para finalizar la tarea.
2. No es 100% preciso: aunque usa inteligencia artificial, sus respuestas se generan de forma probabilística, lo que significa que a veces improvisa, incluso con instrucciones claras.
3. No tiene estructura interna: al no estar diseñado como una aplicación paso a paso, hace todo de golpe, y eso puede provocar errores, sobre todo si las instrucciones son largas o complejas.

Nuestra solución: paso a paso y con control

Tenemos que analizar dos Excel de forma combinada, por ejemplo un listado de ventas y otro con los costes de producto para ver qué margen de beneficio nos deja cada producto. En lugar de pedirle todo de una vez, lo que hicimos fue dividir el proceso en tres etapas simples, para que el agente no se atasque y podamos validar cada paso antes de continuar.

Así lo hacemos:

1.  Primero analizamos la primera tabla. El agente la resume y nos da un primer análisis.
2.  Luego le damos la segunda tabla, que analiza por separado.
3.  Por último, le pedimos que combine ambos análisis y nos dé una visión final.

Cada paso se hace por separado, con confirmación del usuario, lo que permite:

- Detectar errores a tiempo.
- Evitar que se olvide de lo que ya dijo.
- Reducir la carga de información en cada turno.
- Generar una conversación fluida y controlada.

Y lo mejor: el usuario no tiene que repetir nada ni copiar resultados entre pasos. Todo queda guardado automáticamente.

¿Qué hemos conseguido?

Aplicando este enfoque:

- El agente responde con más claridad y precisión.
- El proceso es mucho más estable y confiable.
- Podemos usarlo en entornos reales de trabajo sin miedo a errores graves.
- Se convierte en una herramienta útil de verdad, no solo una demo tecnológica.

Conclusión

¿Por qué fallan? Tienen restringidos la capacidad de proceso (tokens) y el tiempo de proceso. Se quedan sin tiempo para responder si la petición involucra mucho trabajo.

Los Copilot Agents son una herramienta muy prometedora, pero todavía NO están en fase de madurez y seguramente Microsoft tampoco tiene suficiente capacidad de proceso.

Hemos encontrado una forma eficaz de trabajar con ellos, dividiendo el proceso en pasos claros y validables (le damos tiempo para pensar), lo que nos permite sacar su máximo potencial sin comprometer la fiabilidad.