

QUE LA IA ACTÚE POR TI, NO SIN TI

Los asistentes y agentes de inteligencia artificial **son capaces de hacer tareas en tu nombre, desde gestionar el calendario hasta completar compras o reservas**. Antes de delegar, **pregúntate**:

- ¿Qué puede ver?
- ¿Qué puede recordar?
- ¿Qué puede hacer en mi nombre?
- ¿Dónde envía mis datos?
- ¿Afecta a alguien más?

1

¿Quién está detrás?

Revisa quién presta el servicio, qué hace con tus datos y qué controles te ofrece.

2

Accesos sí; cheques en blanco no

Que pueda leer tu agenda no significa que lo necesite o que deba enviar, modificar o borrar. Gestiona los permisos.

Leer

Enviar, borrar

3

Dale lo mínimo

Cuanto más delicados sean los datos (salud, situación económica, identidad, contraseñas), más limitado debe ser el acceso y la autonomía del agente.

* * * * *

4

Controla lo que recuerda de ti

La memoria del agente construye un perfil sobre ti. Revisa y borra su memoria desde los ajustes. Para temas delicados, usa chats temporales.

5

Dile lo que no debe hacer

Ponle límites. Decide a quién puede escribir y cuándo debe parar y preguntarte. Empieza con tareas sencillas.

6

Él prepara, tú apruebas

Si es posible, activa la confirmación previa. No concedas autorizaciones permanentes.

Cancelar

Aprobar

7

Cuidado con lo que lee

Una web o un correo pueden esconder órdenes para que el agente haga algo distinto de lo ordenado. Limita lo que el agente puede hacer si es engañado.

8

Protege los datos de los demás

Tu correo y tu agenda están llenos de datos de otras personas. Piénsalo antes de darle acceso.

9

Tu cuenta es la llave de todo

Usa una contraseña única y activa la verificación en dos pasos y los avisos de inicio de sesión.

10

Supervisa y aprende a pararlo

Revisa lo que hace y averigua cómo detenerlo antes de necesitarlo. Si algo falla, deténlo y cambia tus contraseñas.