

Checklist: 15 controles antes de dar acceso a un agente de IA

Para pymes y autónomos que van a conectar un agente o una automatización con IA a su correo, CRM, facturación o redes. Revísalo antes de activarlo y cada vez que le des un permiso nuevo.

Cómo usarlo: marca cada punto que ya tengas resuelto. Si no puedes marcar alguno de los bloques 2 y 3, el agente todavía no debería poder ejecutar acciones por sí solo: déjalo en modo «solo preparar».

1. Antes de conectar nada

☐ **Tarea concreta y medible.**

Sabes qué tarea hará el agente, cuánto tiempo te cuesta hoy y cómo medirás si mejora.

☐ **Inventario de datos.**

Sabes a qué datos tendrá acceso (clientes, facturas, salud, menores...) y si alguno es especialmente sensible.

☐ **Proveedor revisado.**

Has leído dónde guarda los datos, si los usa para entrenar sus modelos y si ofrece contrato de encargado del tratamiento (RGPD).

2. Permisos mínimos

☐ **Solo lo que necesita.**

El agente tiene acceso únicamente a las cuentas, carpetas y listas imprescindibles para su tarea.

☐ **Lectura antes que escritura.**

Empieza con permisos de solo lectura y amplía después, cuando hayas visto cómo funciona.

☐ **Cuenta o clave propia.**

Usa una cuenta o clave de API exclusiva para el agente, nunca tu usuario personal ni la del administrador.

☐ **Límites de gasto y volumen.**

Hay un tope de gasto mensual en la API y un máximo de acciones por día (correos, mensajes, registros).

3. Aprobación humana

☐ **Acciones de alto impacto con aprobación.**

Pagos, borrados, contratos, precios y mensajes a clientes requieren que una persona los apruebe antes de ejecutarse.

☐ **Responsable con nombre.**

Hay una persona concreta que revisa lo que el agente prepara y responde de ello.

☐ **Contenido público revisado.**

Nada de lo que genere la IA se publica (web, redes, newsletter) sin una revisión humana.

4. Registro y supervisión

☐ **Historial consultable.**

Puedes ver qué hizo el agente, cuándo y con qué datos (historial de ejecuciones, logs).

☐ **Avisos de error.**

Si una ejecución falla, te llega un aviso por correo o mensaje; no te enteras por un cliente.

☐ **Revisión periódica.**

Revisas una muestra de resultados cada semana durante el primer mes, y cada mes después.

5. Plan B

☐ **Interruptor de emergencia.**

Sabes desactivar el agente en menos de 5 minutos (pausar el workflow, revocar la clave) y está apuntado.

☐ **Proceso manual de respaldo.**

Si el agente se para, la tarea se puede seguir haciendo a mano sin que el negocio se bloquee.

¿Cuántos has marcado?

13–15: buena base. Puedes ir ampliando la autonomía del agente poco a poco.

8–12: úsalo solo para preparar borradores y propuestas, sin ejecutar acciones.

Menos de 8: no lo conectes todavía a sistemas reales. Empieza por los bloques 2 y 3.

¿Quieres revisar estos controles con tu caso concreto? Escríbenos en ianegocios.tech/contacto · Este documento es orientativo y no sustituye el asesoramiento legal.