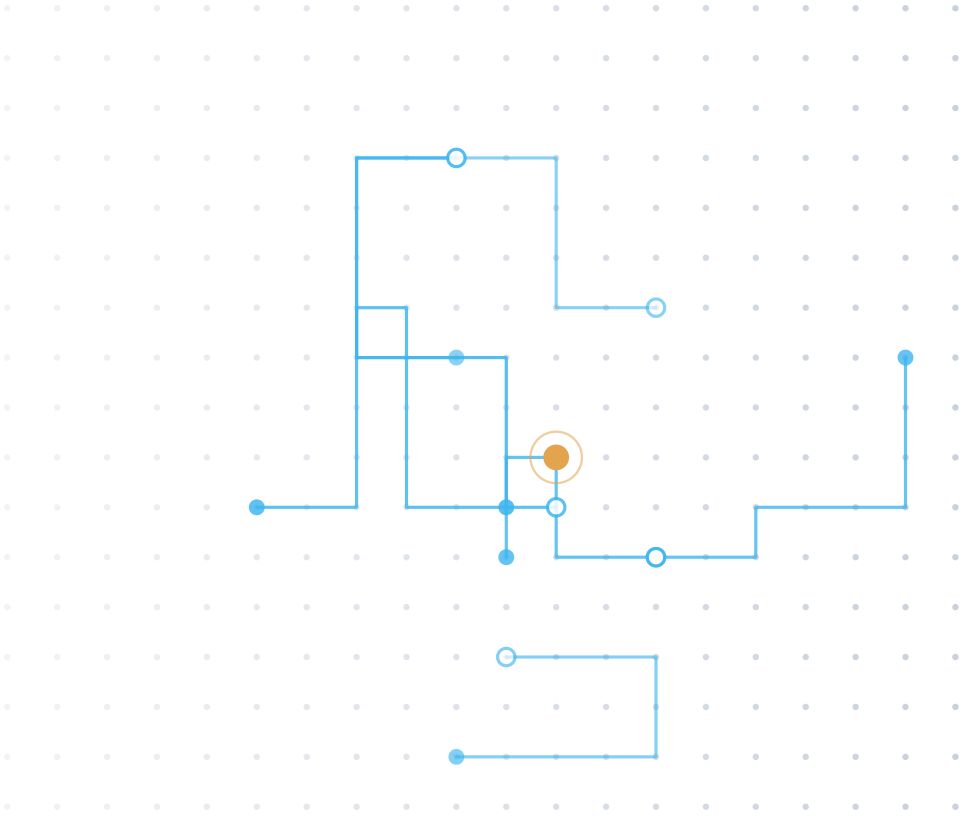


GUÍA PRÁCTICA

Checklist de privacidad para automatizaciones con datos de clientes

15 comprobaciones para que tu automatización use solo los datos que necesita y nadie vea lo que no debe.

AUTOR

Mario Chasco · Flowara AI

PARA

Dueños de negocio que manejan datos de clientes y las personas que les montan las automatizaciones

LECTURA

9 min

EDICIÓN

v2.0 · noviembre 2026

ANTES DE EMPEZAR

Qué vas a sacar de esta guía

01 Hacer en 10 minutos el inventario de datos de una tarea.

02 Decidir qué se queda en tu equipo y qué sale a la nube anonimizado.

03 Separar clientes y permisos por estructura, no por instrucciones al modelo.

04 Llegar a la conversación con tu asesor legal con los deberes hechos.

CONTENIDO

01 El problema: das más llaves de las necesarias
02 Inventario de datos en 10 minutos
03 Minimizar y anonimizar antes de que nada salga
04 Separar por cliente y por rol
05 Qué preguntar a tu proveedor de IA
06 Avisar a las personas y apuntar lo que haces
07 Ejemplo: una puerta que falla cerrada en un centro educativo
08 Checklist de privacidad y qué documentar

Para: Dueños de negocio que manejan datos de clientes y las personas que les montan las automatizaciones · 9 min de lectura

01

El problema: das más llaves de las necesarias

Cuando dejas el coche en el taller, entregas la llave del coche, no la de tu casa. Con las automatizaciones solemos hacer lo contrario. Para que la IA conteste un correo le damos acceso a todo el buzón; para resumir una ficha, a toda la base de clientes. Funciona, hasta el día en que algo se cuela donde no debía.
Los problemas de privacidad en automatizaciones rara vez vienen de un ataque sofisticado. Vienen de tres descuidos: meter datos que la tarea no necesitaba, mezclar clientes en el mismo sitio y confiar en que una instrucción al modelo ("no menciones esto") hace de cerradura. No la hace.

Por eso trato la privacidad como una parte del diseño y no como una promesa. Se decide qué dato entra, dónde vive y quién llega a él antes de escribir la primera línea, y la estructura lo hace cumplir aunque el modelo se equivoque.

Esta guía es para quien tiene los datos y para quien construye la automatización. No es asesoramiento legal y no te dice si cumples el RGPD o cualquier otra norma de protección de datos que te aplique. Para eso, consulta a un profesional; lo que sí hace es que llegues a esa conversación con los deberes hechos.

> ✦ **REGLA**
>
> El dato más seguro es el que nunca entra en la automatización.

02

Inventario de datos en 10 minutos

Antes de hablar de herramientas, apunta qué entra de verdad en la automatización. Coge la tarea concreta, por ejemplo confirmar citas por WhatsApp en una clínica, y responde por cada dato:

DATO	¿LO NECESITA LA TAREA?	DÓNDE VIVE	QUIÉN LO VE HOY
Nombre del cliente	A veces	Agenda	Recepción
Teléfono	Sí, para responder	Móvil del negocio	Recepción y dueño
Notas internas	No	Cuaderno u hoja	Dueño
Salud o datos de menores	Casi nunca	Fichas	Persona responsable
Datos de pago	No	Banco o datáfono	Dueño y gestoría

Tres preguntas cierran el inventario. ¿Qué datos llegan sin que los pidas? Un adjunto o la firma de un correo traen a menudo más de lo que parece. ¿Dónde se copian por el camino: registros, copias de seguridad u hojas intermedias? ¿Cuánto tiempo se guardan?

Todo lo que marques en rojo sale de la automatización antes de empezar. Lo que está en ámbar entra solo cuando el caso concreto lo pide.

EN UNA FRASE

Si no sabes qué datos entran, no puedes saber cuáles salen.

03

Minimizar y anonimizar antes de que nada salga

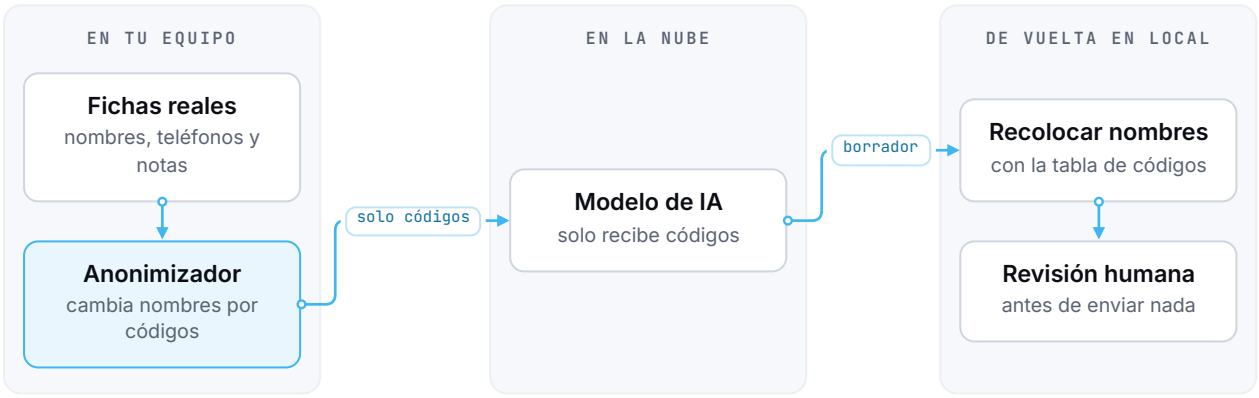
Los dos primeros verbos van en este orden.

01 **Minimizar.** Usa solo los datos que la tarea necesita. Para confirmar una cita basta un código y una hora, no el historial del cliente.

02 **Anonimizar.** Si el modelo tiene que leer un texto, cambia nombres y señas por códigos antes de que le llegue. Hazlo en una copia aparte, nunca sobre los datos reales. Y recuerda que renombrar no es anonimizar: el contexto también delata a una persona.

En la práctica, eso divide el sistema en dos zonas. Lo sensible se queda en tu equipo, y a la nube solo sale texto con códigos. Cuando vuelve el borrador, los nombres se recolocan en local y una persona lo revisa antes de enviarlo. Los datos de salud o de menores ni siquiera salen anonimizados si la tarea puede hacerse sin ellos. Y la tabla que une cada código con su nombre real vive solo en el equipo del negocio, nunca en la nube.

FIGURA 1 **A la nube solo salen códigos**



EN UNA FRASE

Lo que nunca sale de tu equipo no se puede filtrar desde fuera.

04 Separar por cliente y por rol

El tercer verbo es separar, y aquí la estructura hace el trabajo. Cada automatización se organiza en tres capas que nunca se mezclan:

01 **Núcleo:** el código común, igual para todos los clientes.

02 **Configuración del cliente:** horarios, textos y reglas, sin secretos.

03 **Secretos:** claves y contraseñas, con el mínimo permiso. Nunca en documentos, chats, registros ni repositorios, ni en ninguna nube a la que la IA pueda llegar.

Y **un contenedor por cliente**: su carpeta, sus claves y sus conexiones. Si algo falla, falla dentro de una sola habitación. La prueba de fuego es sencilla: desde dentro de un cliente, pide a la IA que lea los archivos de otro. Cualquier respuesta que no sea una negativa es una fuga.

> *La privacidad la decide la estructura del sistema, no lo que se le pide al modelo.*
>
> PRINCIPIO DE DISEÑO DE FLOWARA AI

Dentro de cada negocio, los permisos van por rol y se deciden antes de construir. Una automatización actúa con los permisos de quien la conectó, no con los de quien la usa. Si el dueño la conecta con su cuenta, cualquiera que hable con ella llega a todo lo que ve el dueño.

FIGURA 2 **Quién ve qué, por rol**

	VE	NO VE
RECEPCIÓN	**Agenda del día** nombre y teléfono del cliente	**Notas y pagos** ni notas internas ni cobros
DUEÑO	**Todo el negocio** es su información	**Claves en claro** tampoco el dueño
AGENTE DE IA	**Campos de su tarea** y nada más	**Otros clientes** ni secretos ni pagos
PROVEEDOR TÉCNICO	**Configuración** y registros enmascarados	**Datos reales** de clientes finales, ni en pruebas

Aplica la regla del primer día: ¿le darías este acceso a alguien que empieza hoy? Si no, tampoco a la IA. Una clave por agente, con el mínimo permiso y en solo lectura mientras no necesite escribir.

EN UNA FRASE

Da a la IA el acceso de un empleado nuevo, nunca el del dueño.

05

Qué preguntar a tu proveedor de IA

Cada servicio de IA que uses procesa los datos que le envías. Antes de conectarlo, pide respuestas por escrito a estas preguntas:

01 **Retención:** ¿cuánto tiempo guardan lo que envío? ¿Se puede reducir al mínimo?

02 **Región:** ¿en qué país se procesan y almacenan los datos? ¿Puedo elegir la Unión Europea?

03 **Entrenamiento:** ¿usan mis datos o los de mis clientes para entrenar sus modelos? ¿Viene desactivado o tengo que pedirlo?

04 **Subencargados:** ¿qué otras empresas tocan los datos, como alojamiento, soporte o monitorización? ¿Avisan si cambia la lista?

05 **Contrato:** ¿ofrecen un acuerdo de tratamiento de datos que pueda firmar?

06 **Borrado:** si me voy, ¿cómo y en cuánto tiempo lo borran todo?

> ⚠ CUIDADO
>
> Que un proveedor sea conocido no responde a ninguna de estas preguntas. Las condiciones cambian según el plan: la versión gratuita y la de empresa pueden tratar los datos de forma distinta.

Si una respuesta no te queda clara, vuelve a preguntar hasta tenerla en una frase que entiendas. Guarda las respuestas con fecha y revísalas una vez al año o cuando cambies de plan.

EN UNA FRASE

Si el proveedor no responde por escrito, tus datos no deben ir ahí.

06

Avisar a las personas y apuntar lo que haces

Quien llama o escribe a tu negocio tiene que saber con qué está hablando. Al empezar una llamada, el asistente dice que es un asistente y si la llamada puede grabarse. En WhatsApp o en el chat de la web, lo mismo en el primer mensaje.

> **EJEMPLO**
>
> "Hola, te atiende el asistente de la peluquería. Puedo darte cita o pasarte con una persona. Te aviso de que esta llamada puede grabarse." La redacción exacta, que la revise tu asesor antes de ponerla en marcha.

Además, por cada cliente para el que montas algo, apunta en una página qué haces con sus datos:

01 **Qué datos** trata la automatización.

02 **Para qué** los usa, con la tarea concreta.

03 **Cuánto tiempo** se guardan y cuándo se borran.

04 **Qué otras empresas** los tocan, empezando por el proveedor de IA.

05 **Dónde están**: en qué equipo, servicio y país.

Es tu registro de tratamientos para ese cliente. Si la normativa te obliga a llevar uno, y eso te lo dirá un profesional, ya lo tienes medio hecho. Si no, te sirve igual para contestar cuando un cliente te pregunte qué pasa con sus datos.

EN UNA FRASE

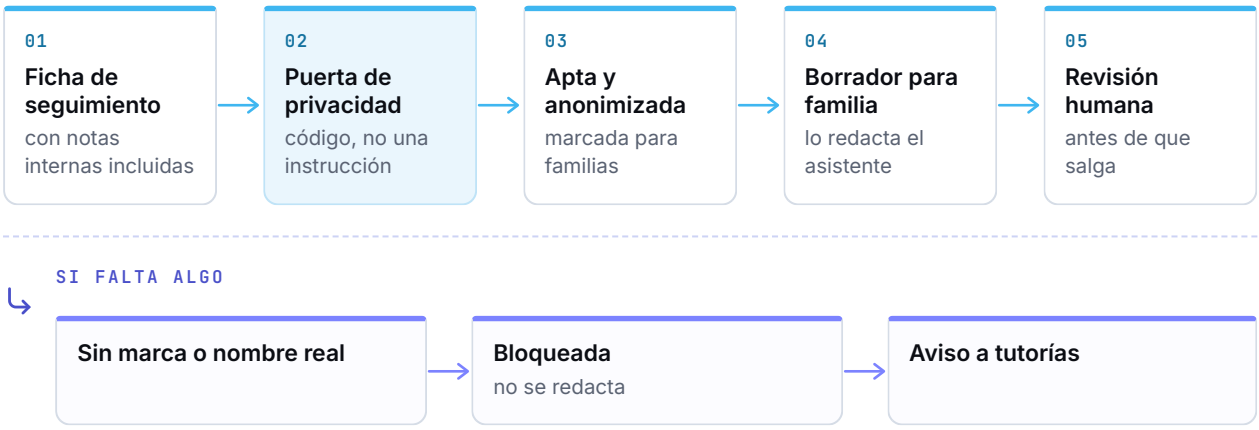
Lo que no está apuntado no se puede revisar ni explicar.

07

Ejemplo: una puerta que falla cerrada en un centro educativo

Un centro educativo usa un asistente que redacta informes para las familias a partir de las fichas de seguimiento. Algunas fichas tienen notas internas que nunca deben salir.
La solución es una **puerta de privacidad que falla cerrada**: un trozo de código, no una instrucción al modelo, que revisa cada ficha antes de que el asistente la lea. Solo pasa lo marcado expresamente como apto para familias y anonimizado. Si falta la marca, si aparece un nombre real donde debería haber un código o si la ficha no se puede leer bien, la puerta no deja pasar nada y avisa.

FIGURA 3 **Una puerta de privacidad que falla cerrada**



Con la ficha sintética de "Alumno Alfa, código ALU-001", el asistente redacta. Si alguien pega una ficha con un nombre completo, el asistente se niega a redactar y explica qué falta.

Lo que importa es el orden. La puerta va antes que el modelo, así que el asistente nunca llega a leer lo que no debía; no depende de que el modelo obedezca.

EN UNA FRASE

Ante la duda, la puerta se cierra: mejor un borrador que no sale que uno que filtra.

08

Checklist de privacidad y qué documentar

Repasa estas quince comprobaciones antes de conectar una automatización a datos reales:

Antes de conectar datos reales

15 PUNTOS

- [ ] Tengo el inventario de datos de la tarea y sé dónde vive cada uno
- [ ] Cada dato que la tarea no necesita está fuera
- [ ] Lo sensible se queda en local o sale anonimizado y se anonimiza en una copia
- [ ] Núcleo, configuración y secretos están separados
- [ ] Cada cliente tiene su contenedor y sus claves
- [ ] He probado a leer un cliente desde otro y la IA se ha negado
- [ ] Ningún secreto está al alcance de la IA ni en documentos, chats o repositorios
- [ ] Los permisos van por rol y cada agente tiene su clave mínima
- [ ] Una puerta de privacidad en código falla cerrada
- [ ] Los registros enmascaran los datos personales
- [ ] El proveedor ha respondido por escrito retención, región, entrenamiento, subencargados
- [ ] Llamadas y mensajes avisan de que atiende un asistente y de si se graba
- [ ] Hay un registro de tratamientos por cliente revisado con un profesional
- [ ] Las demos y las pruebas usan solo datos sintéticos
- [ ] Una persona con nombre responde de la privacidad

Qué documentar para el cliente: el inventario de datos, el reparto de permisos por rol, las respuestas del proveedor con fecha, el registro de tratamientos, cómo funciona la puerta de privacidad y a quién avisar si algo falla. Basta con un par de páginas, siempre que las pueda leer alguien que no es técnico.

SIGUIENTE PASO

Diagnóstico gratuito (20 min)

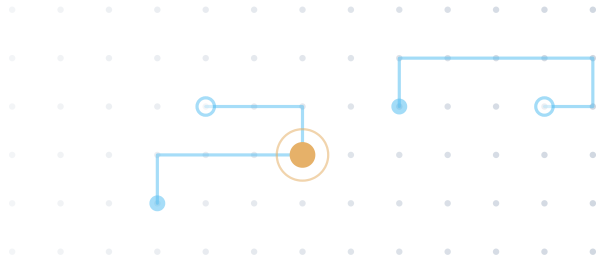
Si quieres ver qué parte de tu negocio se puede automatizar con el riesgo bajo control, reserva un diagnóstico gratuito de 20 minutos.

Reservar diagnóstico ›

flowaraai.com/es/contacto

RECURSOS RELACIONADOS

- Plantilla pública de secretaría con puerta de privacidad ↗
- Casos reales de automatización ↗



Mario Chasco · Flowara AI

Sistemas de IA en producción para negocios pequeños.

flowaraai.com
github.com/mariochasco78557
youtube.com/@mariochasco_AI
linkedin.com/in/mario-adrian-chasco-frauca

Puedes compartir esta guía tal cual, citando flowaraai.com.