ANDIN · CHILE

Qué se le puede pegar a un modelo de IA, y qué no

Una página para el equipo que ya está usando IA.

La regla, en una línea

No es dato sensible contra dato inocente. Es si la identificación salió del dato **antes** de que el dato saliera de la empresa.

Va sin tocar nada

- **Manual de marca** — No hay una persona identificable adentro
- **Norma o ley publicada** — Ya es pública
- **Organigrama por cargo** — Si dice cargos, no nombres
- **Plantilla en blanco** — Es estructura, no contenido
- **Política interna publicada** — Salvo que nombre personas
- **Tu propio borrador** — Lo escribiste tú, no hay un tercero adentro

No va tal como está

- **Export del CRM** — Nombres, documentos, correos y teléfonos de clientes
- **Contrato firmado** — Partes identificadas y cláusulas de confidencialidad
- **Correo reenviado** — Arrastra firmas, cadenas y destinatarios
- **Currículum** — Dato de un tercero que no consintió esto
- **Planilla de clientes** — Lo mismo, y suele arrastrar histórico
- **Caso de soporte** — El texto libre trae datos que nadie clasificó
- **Acta de reunión** — Nombres y opiniones atribuidas
- **Ficha de trabajador** — Puede traer salud, afiliación o remuneración

Las tres preguntas antes de pegar

1. ¿Hay una persona identificable adentro? Nombre, documento, correo, teléfono, dirección.
2. Si la hay, ¿alguien le sacó la identificación antes de que saliera, o le voy a pedir al modelo que no la mire?
3. ¿Queda registro en alguna parte de que esto salió?

La diferencia que importa

Pedirle al modelo que ignore un dato es una **instrucción**, y una instrucción se puede ignorar.

Sacar el dato antes de que salga es un **control**, y un control se puede auditar.

Por eso el enmascarado corre en la capa de dato y no en el prompt: es código determinista, no una decisión del modelo.

El borde, dicho

El documento de identidad, el correo y el teléfono los detecta el código. El nombre depende del contexto y va a revisión de una persona. Un proceso que no declara su borde no se puede auditar.