— IA SEGURA PARA TU EQUIPO

Shadow AI. El riesgo que ya *vive* dentro de tu empresa.

→ Qué es, cuánto cuesta y cómo se ve en una pyme chilena.

→ La hoja de ruta en 5 pasos y una política de uso lista para copiar.

Tu equipo ya usa inteligencia artificial con cuentas personales para tareas del trabajo. Esta guía te muestra cómo pasar de ese uso invisible a un sistema controlado, con Claude como ejemplo.

AUTOR

Jorge Riquelme

Fundador · Otherway Labs

HERRAMIENTA EJEMPLO

Claude · 2026

Team · Enterprise · Gobernanza de datos

OCULTAN SU USO DE IA

57%

— INTRODUCCIÓN

Tu empresa *ya usa* IA. Aunque tú no lo sepas.

Hay una escena que se repite en casi todos los diagnósticos que hago. El dueño me dice que en su empresa todavía no usan IA. Después converso con el equipo y aparece la verdad: la mitad la usa todos los días, con cuentas personales gratuitas, para tareas del trabajo. Nadie lo reporta. Nadie lo controla.

Eso tiene nombre: **Shadow AI**. Y ojo con el diagnóstico: aquí nadie está saboteando nada. Es gente apurada resolviendo con lo que tiene a mano. El problema es lo que se va en cada prompt: precios, datos de clientes, información financiera, estrategia. Todo eso queda en servidores que tu empresa no ve ni administra.

Esta guía te muestra qué es, cuánto cuesta ignorarlo y cómo pasar del uso invisible a un sistema controlado en 5 pasos, usando **Claude** como ejemplo. Al final tienes una política de uso lista para copiar y publicar. Léela con tu equipo directivo. Son 18 minutos.

— ÍNDICE

01 Qué es el Shadow AI 03
02 El fenómeno en cifras 04
03 Lo que ya pasó 05
04 La Ley 21.719 cambia el escenario 06
05 El error de los dos extremos 07
06 La salida: cuenta empresarial 08
07 Hoja de ruta en 5 pasos 09
08 Anexo: política lista para copiar 11

Secciones	Lectura	Nivel
8	18min	Decisor

→ SECCIÓN 01

Qué es el *Shadow AI.*

Shadow AI es el uso de herramientas de inteligencia artificial por parte de tu equipo **sin aprobación ni supervisión** de la empresa. La versión típica: un trabajador abre su cuenta personal gratuita de ChatGPT, Gemini o Claude desde el navegador o el celular, y la usa para tareas del trabajo. Es la evolución del viejo "Shadow IT" (el Dropbox personal, la planilla que vivía en un correo), pero con un agravante serio.

Una app no autorizada guarda o mueve datos. Una IA los **procesa**: puede retenerlos, usarlos para entrenar sus modelos, y devuelve textos y análisis que tu gente incorpora al trabajo sin que nadie revise su calidad. El riesgo ya no es solo dónde quedó el archivo. Es qué aprendió un tercero de tu negocio y qué decisiones se están tomando con respuestas que nadie validó.

— CÓMO SE VE EN UNA PYME

Tres escenas *de cualquier martes.*

- La analista de finanzas pega la planilla de márgenes en su ChatGPT gratis para que le arme el resumen del directorio.
- El vendedor sube la lista de precios y dos cotizaciones de la competencia para redactar una propuesta "más ganadora".
- El jefe de operaciones pega el contrato de un cliente para que la IA le explique una cláusula. Con nombre, RUT y montos incluidos.

Ninguno lo hace de mala fe. Lo hacen porque funciona, porque es gratis y porque nadie les dio una alternativa oficial. Y por eso mismo nadie lo cuenta: en el estudio global de KPMG y la Universidad de Melbourne, el 57% de los empleados reconoce que **oculta** su uso de IA y presenta el resultado como trabajo propio.

→ LA IDEA

El Shadow AI no es un problema de gente floja ni desleal. Es tu mejor gente tratando de trabajar más rápido con lo que tiene a mano. Lo que falta no es castigo: es **una vía oficial**.

→ SECCIÓN 02

El fenómeno *en cifras.*

Esto no es una sensación mía. Los estudios más grandes disponibles, encuestas a decenas de miles de personas y telemetría real de tráfico corporativo, dicen lo mismo desde ángulos distintos.

57%

de los empleados oculta que usa IA en el trabajo y presenta el resultado como propio.

KPMG · U. de Melbourne, 48.000 personas en 47 países, 2025

48%

ya subió información sensible de su empresa o de clientes a herramientas públicas de IA.

KPMG · U. de Melbourne, 2025

80%

de los usuarios de IA en pymes lleva su propia herramienta al trabajo, sin pasar por la empresa.

Microsoft & LinkedIn, Work Trend Index

3 días

es cada cuánto un empleado promedio pega datos sensibles en una IA. Medido en tráfico real, no en encuestas.

Cyberhaven, AI Adoption & Risk Report 2026

— QUÉ SE ESTÁ FILTRANDO

18,7%	Código fuente y desarrollos propios
17,1%	Investigación y desarrollo
10,7%	Ventas, marketing y datos de clientes

Composición de los datos sensibles enviados a IA · Cyberhaven 2025. Netskope 2026 suma: la organización promedio registra 223 incidentes de datos sensibles hacia IA al mes.

→ TRADUCCIÓN Si tienes más de 5 personas en tu equipo, la probabilidad de que hoy **nadie** esté pegando datos de tu empresa en una IA personal es cercana a cero.

→ SECCIÓN 03

Lo que *ya pasó.*

3.1 Samsung, 2023: el caso que abrió los ojos

Tres fugas en 20 días. Ingenieros de Samsung pegaron en ChatGPT código fuente de semiconductores y la transcripción de una reunión interna. La empresa terminó prohibiendo toda IA externa. Fue el primer caso grande y documentado de Shadow AI, y dejó una lección incómoda: pasó en una de las empresas más sofisticadas del mundo, con gente técnica que sabía perfectamente qué era un modelo de lenguaje.

3.2 El historial también se roba

Lo que pegas en una cuenta personal queda en el historial de esa cuenta. Y las cuentas se roban: Group-IB identificó más de **101.000 dispositivos** infectados con malware que robó credenciales de ChatGPT, vendidas después en la dark web. En 2024 se detectaron otras 225.000 a la venta. Súmale un detalle de 2025: unas 4.500 conversaciones de ChatGPT que sus usuarios "compartieron por link" terminaron indexadas por Google, con datos personales visibles. Ninguna de esas filtraciones necesitó hackear a la empresa: bastó la cuenta personal de un empleado.

3.3 Las respuestas inventadas también cuestan plata

Air Canada tuvo que pagar por una tarifa que su chatbot inventó: el tribunal dijo que la empresa responde por lo que dice su IA. Deloitte Australia devolvió parte de un contrato de AU$440.000 por un informe con citas fabricadas. Cuando tu equipo usa IA sin reglas de revisión, esos errores salen con la firma de tu empresa.

---

1 de 5
organizaciones

ya sufrió una brecha de seguridad ligada a Shadow AI, según IBM. Y las brechas en organizaciones con mucho Shadow AI costaron en promedio **USD 670.000 más** que en las que tienen poco o nada. El riesgo dejó de ser teórico: es una línea nueva en el presupuesto de quien lo ignora.

IBM, Cost of a Data Breach Report 2025 · Costo promedio global de una brecha: USD 4,44 millones

→ OJO No necesitas ser Samsung. Para una pyme, que la lista de precios o la base de clientes quede en manos ajenas puede doler **más** que a una multinacional: no hay departamento legal que amortigüe el golpe.

→ SECCIÓN 04 · CHILE

La Ley 21.719 *cambia el escenario.*

Hasta ahora, filtrar datos de clientes en Chile salía casi gratis: la ley de datos vigente era de 1999 y no tenía quién la fiscalizara. Eso se acabó. La nueva Ley 21.719 de protección de datos personales entra en **plena vigencia el 1 de diciembre de 2026**, y trae dos cosas que no existían: una Agencia de Protección de Datos con poder real de fiscalizar y multar, y la obligación de notificar las brechas de seguridad.

Qué exige la ley

Tratar los datos personales de clientes y trabajadores con una base legal, con medidas de seguridad y con trazabilidad. Si hay una brecha, hay que reportarla. El "no sabía que mi equipo hacía eso" deja de servir como defensa: el deber de seguridad es de la empresa.

Dónde entra el Shadow AI

Cada vez que alguien de tu equipo pega el RUT, el correo o el historial de compras de un cliente en una cuenta personal de IA, tu empresa está tratando datos personales en un servidor que no controla, sin contrato, sin registro y sin posibilidad de auditar ni de borrar. Exactamente lo que la nueva agencia viene a sancionar.

— RANGOS DE MULTA

Infracciones leves	Graves	Gravísimas
5.000 UTM	10.000 UTM	20.000 UTM
hasta ~CLP 350 millones	hasta ~CLP 700 millones	hasta ~CLP 1.400 millones

Ley 21.719, publicada en diciembre de 2024 · Montos referenciales según valor UTM 2026

→ EL PLAZO Diciembre de 2026. Te quedan **meses**, no años, para ordenar cómo se usan los datos de tus clientes dentro de la IA. Ordenarlo hoy cuesta una fracción de la multa más chica.

→ SECCIÓN 05

El error de los *dos extremos.*

Frente al Shadow AI, la mayoría de las empresas elige uno de dos caminos. Los dos salen caros.

Extremo 1: prohibir

No funciona. El 45% de los trabajadores reconoce que se salta los bloqueos, y el 57% simplemente esconde el uso. Prohibir no elimina el riesgo: elimina tu **visibilidad** sobre el riesgo. El uso sigue, pero ahora desde el celular personal, donde ningún control de la empresa llega. Y de paso renuncias a la productividad que la competencia sí está capturando.

Extremo 2: dejarla suelta

Tampoco funciona. Es todo lo que viste en las secciones anteriores: datos sensibles saliendo cada 3 días, historiales corporativos viviendo en cuentas que se van con el empleado, respuestas inventadas firmadas por tu empresa, y desde diciembre de 2026, exposición directa ante la Ley 21.719.

> *"No les puedo decir a los chiquillos que no la ocupen, pero la empresa tampoco puede quedarse atrás."*

Subgerente de una empresa que maneja información sensible de precios, en un diagnóstico reciente. Ese es el dilema exacto. Y tiene salida.

— LA DIFERENCIA DE FONDO

Cuenta personal versus *cuenta empresarial.*

Cuenta personal (gratis o pagada)

- Tus datos pueden usarse para entrenar modelos, según el proveedor y la configuración de cada usuario.
- El historial vive fuera de la empresa y se va con el empleado.
- Nadie sabe qué se pegó ni cuándo.

Cuenta empresarial

- El proveedor no entrena con tus datos por defecto.
- Un administrador de tu empresa controla accesos, roles y gasto.
- Las cuentas y los datos son de la empresa, no de la persona que se va.

Y esto es transversal: ChatGPT personal entrena con tus conversaciones salvo que lo desactives. Gemini personal también, y una parte de los chats pasa por revisores humanos. Claude personal te pregunta al crear la cuenta, y si aceptas, guarda tus chats hasta 5 años. Las versiones empresariales de los tres no entrenan por defecto. El problema no es el proveedor. Es el **tipo de cuenta**.

→ SECCIÓN 06

La salida: *cuenta empresarial.*

La solución no es bloquear: es dar la herramienta correcta de forma segura. Uso Claude como ejemplo porque es la que implemento con mis clientes, pero la lógica sirve para cualquier proveedor serio.

> *"By default, we will not use your inputs or outputs from our commercial products to train our models."*

Anthropic, Privacy Center. En simple: por defecto, nada de lo que tu equipo escribe o recibe en un plan comercial se usa para entrenar los modelos. Tus datos quedan tuyos. Respaldado por certificaciones SOC 2 Type II, ISO 27001 e ISO/IEC 42001 (gestión de sistemas de IA), verificables en trust.anthropic.com.

— CLAUDE TEAM

Desde 5 asientos. El punto de partida para una pyme.

- Asiento Estándar: **USD 25**/mes por persona (USD 20 con pago anual).
- Asiento Premium: USD 125/mes (USD 100 anual), 5 veces más uso que el Estándar. Se pueden mezclar.
- Incluye todos los modelos, Projects compartidos, Claude Code y conectores a Drive, Slack, Microsoft 365 y GitHub.
- Administración central: asientos, facturación, SSO y límites de gasto.

— CLAUDE ENTERPRISE

Desde 20 asientos. Para empresas más grandes o reguladas.

- USD 20 por asiento más el uso, cobrado a tarifas de API. Con equipo de ventas desde 50 asientos.
- Agrega SCIM (altas y bajas automáticas), audit logs y roles a medida.
- Compliance API: conecta el uso de Claude con tus herramientas de seguridad.
- Retención de datos personalizada e inferencia solo en EE.UU. si la necesitas.

Precios verificados en claude.com/pricing y support.claude.com, julio 2026. Pueden cambiar: revisa antes de contratar.

→ LA CUENTA

Un equipo de 5 personas parte en **USD 100 al mes** con pago anual. Compáralo con el sobrecosto promedio de una brecha con Shadow AI: USD 670.000. La cuenta empresarial no es un gasto de software, es un seguro con productividad incluida.

→ SECCIÓN 07 · HOJA DE RUTA

IA segura en *5 pasos.*

Este es el orden que aplico con mis clientes. No necesitas un departamento de TI: necesitas un responsable, un par de semanas y la decisión de hacerlo.

Paso 1 Descubre lo que ya está pasando

Antes de comprar nada, mide tu Shadow AI real. Haz una encuesta corta con **amnistía explícita**: nadie será sancionado por lo que declare. Tres preguntas bastan: qué herramientas de IA usas, para qué tareas, y qué tipo de datos has pegado. Complementa con dos revisiones simples: los gastos de tarjeta de la empresa (buscando suscripciones de IA que alguien ya paga por su cuenta) y con qué apps se está iniciando sesión usando los correos corporativos.

El resultado te va a sorprender: en el estudio de UpGuard, el 81% de los empleados reconoce usar IA no aprobada. Pero esa lista de usos reales es oro puro: son los casos de uso que tu plan oficial tiene que cubrir primero.

> → TIP Amnistía significa amnistía. Si castigas al primero que confiesa, la encuesta muere ahí y el Shadow AI vuelve a esconderse. La información vale más que el castigo.

Paso 2 Contrata la cuenta empresarial

Con la lista del paso 1 en la mano, contrata el plan que corresponde a tu tamaño. Para la mayoría de las pymes es Claude Team: mínimo 5 asientos, contratación online con tarjeta, listo el mismo día. Parte por las personas que ya usan IA a diario (las de tu encuesta), no por organigrama. Ellas van a adoptar la herramienta al tiro y se convierten en tus primeros referentes internos.

Sobre el pago anual: conviene (USD 20 versus USD 25 por asiento), pero actívalo cuando ya validaste el uso. Un mes o dos en mensual primero no te va a quebrar.

> → TIP No compres 40 asientos el día uno. Parte con 5 o 10 donde ya hay uso real y crece con la demanda. Los asientos se agregan en dos clics; el entusiasmo perdido no.

Paso 3 Configura el control antes de invitar gente

La gracia de la cuenta empresarial es la consola de administración. Úsala antes de repartir accesos. En Claude, los roles son cuatro:

Primary Owner	Uno solo, idealmente el dueño o gerente general. El único que puede exportar los datos y transferir la cuenta.
Owner	Socios o gerencia. Gestionan admins, facturación y configuración.
Admin	El responsable operativo: invita y remueve miembros, asigna asientos, habilita integraciones.
User	El resto del equipo. Usa Claude con todo su potencial, sin tocar la configuración.

Tres configuraciones que valen la pena el primer día: **domain capture** (cualquiera que se registre con el dominio de tu empresa cae dentro de la cuenta corporativa, no en una personal), límites de gasto por usuario y por organización, y los conectores a Drive o Slack solo cuando la política ya esté publicada.

Paso 4 Lanza con piloto, capacitación y champions

Un piloto de 30 a 60 días con 2 o 3 casos de uso concretos, cada uno con un dueño y una métrica (horas ahorradas, propuestas enviadas, tickets resueltos). El MIT midió que la gran mayoría de los pilotos de IA muere sin llegar a producción; los que sobreviven tienen dueño y métrica, no entusiasmo general. Nombra un champion por cada 15 o 20 personas: alguien del equipo que resuelve dudas y junta los aprendizajes. Y capacita a todos en una sola cosa antes que nada: qué datos se pueden pegar y cuáles no.

Paso 5 Publica la política y revisa cada trimestre

Copia la política del anexo, ajústala y publícala. Después, una revisión trimestral de 30 minutos: qué casos de uso nuevos aparecieron, quién necesita asiento, qué dice el reporte de uso de la consola. Incluye en la revisión la IA que viene **embebida** en el software que ya pagas (Notion AI, Grammarly, los copilotos de tu CRM): es el punto ciego que más crece. Gartner encontró que las organizaciones que auditan su IA con regularidad tienen 3 veces más probabilidad de sacarle valor real.

→ REGLA DE ORO

Herramienta oficial + política publicada + revisión trimestral. Con esas tres piezas, el Shadow AI deja de ser una amenaza invisible y se convierte en tu **pipeline** de casos de uso.

→ ANEXO

Política de uso de IA, *lista para copiar.*

Reemplaza los campos entre corchetes, ajusta lo que haga falta y publícala. Una página basta: una política que nadie lee no protege a nadie.

POLÍTICA DE USO DE INTELIGENCIA ARTIFICIAL · [EMPRESA] · Versión 1.0 · [FECHA]

1. Objetivo. Esta política regula el uso de herramientas de inteligencia artificial en [Empresa]. Queremos que el equipo use IA para trabajar mejor, protegiendo los datos de la empresa, de nuestros clientes y de nuestros trabajadores.

2. Herramientas aprobadas. La herramienta oficial es [Claude Team], con la cuenta corporativa de [Empresa]. Queda prohibido usar cuentas personales de cualquier IA para tareas del trabajo. Si necesitas una herramienta que no está en la lista, pídela a [Responsable]: la respuesta llega en máximo [5 días hábiles].

3. Qué datos se pueden usar. (a) Información pública: se puede usar en cualquier herramienta aprobada. (b) Información interna (procedimientos, borradores, minutas): solo en la herramienta oficial. (c) Información confidencial (precios, márgenes, contratos, estrategia): solo en la herramienta oficial y solo si tu rol lo requiere. (d) Información restringida: datos personales de clientes y trabajadores, credenciales y claves, información financiera no pública. Esta categoría no se ingresa a ninguna IA sin autorización expresa de [Responsable] y sin anonimizar.

4. Usos prohibidos. Tomar decisiones sobre personas (contratación, despido, crédito, evaluación) basadas solo en una IA; enviar a clientes contenido legal, contractual o financiero generado por IA sin revisión de un responsable; ingresar datos de terceros protegidos por acuerdos de confidencialidad.

5. Revisión humana. Todo material generado con IA que salga de la empresa lo revisa y aprueba una persona. La responsabilidad por el contenido es de quien lo envía, no de la herramienta.

6. Transparencia. Usar IA está bien y no se castiga. Declarar que un trabajo se hizo con ayuda de IA no tiene consecuencias negativas. Lo que sí se sanciona es ocultar el uso de herramientas no aprobadas o el mal uso de datos.

7. Incidentes. Si ingresaste datos que no correspondían, o sospechas una filtración, avisa a [Responsable] dentro de 24 horas. Reportar a tiempo no tiene sanción. Ocultarlo, sí.

8. Vigencia y revisión. Responsable de esta política: [Nombre y cargo]. Se revisa cada [6] meses o cuando cambien las herramientas aprobadas. Rige desde su publicación para todo el equipo, incluidos externos con acceso a información de [Empresa].

→ TIP Preséntala en una reunión de 20 minutos, con ejemplos reales de qué se puede y qué no. Una política que llega por correo y no se conversa es papel mojado.

— ÚLTIMO PASO

Ahora que lo ves, *contrólalo.*

El Shadow AI no se arregla con un correo prohibiendo cosas. Se arregla dando una vía oficial mejor que la clandestina: una herramienta empresarial que no entrena con tus datos, una política que cabe en una página y una revisión trimestral que no toma más de media hora.

La diferencia entre una empresa que adopta IA en serio y una que la tiene de juguete personal filtrando datos no es el presupuesto. Es que alguien tomó la decisión de ordenarlo. Esta semana puedes dejar andando los primeros cuatro puntos de la lista.

— CHECKLIST DE ACTIVACIÓN · ESTA SEMANA

01 Pregunta a tu equipo qué IA usan hoy y para qué. Con amnistía declarada.

02 Revisa los gastos de tarjeta buscando suscripciones de IA que ya existen.

03 Cotiza el plan empresarial para quienes ya usan IA a diario (claude.com/pricing).

04 Define quién será el administrador y quién el Primary Owner.

05 Copia la política del anexo y ajusta los campos entre corchetes.

06 Agenda la primera revisión trimestral en el calendario. Hoy.



— SOBRE EL AUTOR

Jorge *Riquelme.* Fundador · Otherway Labs

Ayudo a pymes y equipos a adoptar IA de forma **segura y útil**: diagnóstico, implementación de Claude y capacitación práctica. Comparto lo que aprendo en cada proyecto en Instagram y en otherwaylabs.cl.

— PRÓXIMOS PASOS

Tres formas *de seguir avanzando.*

— PARA EMPRESAS
Sesión gratuita

¿Quieres saber cuánto Shadow AI *hay en tu empresa*?

Agenda un diagnóstico gratuito: revisamos tu situación, el riesgo real y el plan para implementar IA segura en tu equipo.

Agenda en otherwaylabs.cl →

— PARA EQUIPOS
Capacitación

Forma a tu equipo para que *use IA todos los días*.

Capacitación práctica en Claude para equipos: desde la política de uso hasta los flujos de trabajo de cada área.

Conoce más en otherwaylabs.cl →

— RECURSOS GRATIS
WhatsApp

Recibe recursos como este *antes que nadie*.

Únete al grupo de WhatsApp exclusivo. Te llegan las guías y skills gratis directo, antes de que las publique en redes.

Únete en chat.whatsapp.com →