GUÍA PRÁCTICA · AGOSTO 2026 · V1.6

Reglas de IA que tu equipo sí va a seguir.

Tus empleados ya usan IA, con o sin permiso. Aquí está cómo ponerle reglas: una configuración que tu administrador activa una vez, y una política de una página que tu gente firma. Al día con la nueva ley de datos personales (LFPDPPP 2025) y las guías oficiales de Anthropic, OpenAI, Google y Microsoft.

ELABORADO POR

APLICA A

Claude · ChatGPT · Gemini · Copilot

INCLUYE

Checklist + política firmable

La mitad de tu política se configura sola.

La mayoría de las políticas de IA fracasan porque le piden a la gente lo que el sistema podría garantizar solo. **Configura primero:** cuentas, retención y permisos se activan una vez en el panel y dejan de depender de la memoria de nadie. Lo que quede — lo que ninguna configuración puede imponer — eso va en la política. Por eso es una página, y por eso se cumple. El camino completo son cuatro pasos:

PASO 1 · CONTRATA

El plan seguro

Las garantías de datos vienen en el contrato del plan empresarial. Elígelo bien y la mitad del riesgo desaparece antes de escribir una sola regla.

PASO 2 · CONFIGURA

La lista del administrador

Cuentas, retención, conectores, agentes y permisos. Se activa una vez, con dueño y fecha, y queda impuesto por el sistema.

PASO 3 · FIRMA

La política de una página

El semáforo de datos y las reglas que dependen del criterio de una persona — por eso son pocas, y por eso se cumplen.

PASO 4 · CAPACITA

El despliegue

Tu gente aprende el semáforo y firma la política al concluir. Se repite cada año. Es donde el papel se convierte en comportamiento.

Las peores políticas son de dos tipos — tan restrictivas que todos las ignoran, o tan vagas que no dicen nada. Si un empleado no puede leer la suya en 5 minutos y saber qué hacer, está mal escrita. Esta guía existe para que la tuya sí se cumpla.

Elige un plan seguro: el contrato viene incluido.

Las garantías de datos existen solo en los **planes empresariales**: que tus datos no entrenen modelos, cifrado, inicio de sesión único (SSO — tu gente entra a la IA con su cuenta de la empresa) y el contrato de encargado de datos (DPA — el papel que obliga al proveedor a proteger tus datos). Los planes personales (Free, Pro, Max, Plus…) se rigen por términos de consumo, sean gratuitos o de pago.

PROVEEDOR	PLAN QUE EXIGIR	GARANTÍA CLAVE
Anthropic Claude	Team / Enterprise	Tus datos no entrenan modelos — está en el contrato. SSO y captura de dominio (toda cuenta con el correo de tu empresa queda bajo tu control) desde Team; retención configurable, registro de quién hizo qué y convenio de salud HIPAA (BAA) solo en Enterprise.
OpenAI ChatGPT	Business / Enterprise	Conversaciones excluidas de entrenamiento. SOC 2, cifrado, SSO. En cuentas personales, gratuitas o de pago, tus datos sí pueden entrenar modelos.
Google Gemini	Workspace con Gemini	Nada sale de tu dominio ni entrena modelos sin permiso. Hereda tus controles de Workspace: prevención de fugas de datos, regiones de datos.
Microsoft Copilot	Microsoft 365 Copilot	Tus datos se quedan en tu entorno de M365 y no entrenan modelos. Hereda los permisos de M365 y los controles de Purview. Ojo: Copilot muestra todo aquello a lo que el usuario ya tiene acceso — limpia los permisos internos antes de activarlo.

Verifícalo tú mismo → Los cuatro publican sus certificaciones (SOC 2 Type 2, ISO 27001; Anthropic además ISO 42001, el estándar de gestión de IA, desde enero de 2025) en trust.anthropic.com, trust.openai.com y los portales de cumplimiento de Google y Microsoft. Pide los reportes antes de firmar. La certificación cubre los controles del proveedor, no tu uso.

Dónde termina el DPA. El contrato con tu proveedor de IA cubre lo que pasa dentro de su plataforma. En cuanto conectas una aplicación de terceros — Drive, Slack, Gmail — lo que sale por ahí lo gobierna tu contrato con esa otra empresa. Un conector mueve la frontera; revísala antes de activarlo.

La lista de verificación del administrador.

Cada casilla con su razón. Se verifica con dueño y fecha; nada de esto se firma ni se capacita.

Configuración de IA — [Empresa]

RESPONSABLE: [ADMINISTRADOR, CORREO] · ÚLTIMA VERIFICACIÓN: [FECHA] · PRÓXIMA: [FECHA + 6 MESES]

- ☐ **Plan empresarial y DPA vigentes** con cada proveedor — las garantías solo existen ahí. Lista de subprocesadores revisada (las otras empresas que tu proveedor usa para operar — trust.anthropic.com/subprocessors y equivalentes).
- ☐ **SSO y captura de dominio activos,** roles y límites de gasto asignados — impone "solo cuenta de la empresa" dentro de la organización; a la política le queda solo el teléfono propio.
- ☐ **Retroalimentación de entrenamiento (👍/👎) desactivada** a nivel organización — es la única vía por la que datos de un plan empresarial pueden guardarse hasta 5 años y entrenar modelos.
- ☐ **Retención definida** — cuánto tiempo se conservan las conversaciones y archivos en la plataforma, configurado según tu plan y comunicado al equipo.
- ☐ **Los dos avisos de privacidad actualizados** — el de clientes y el laboral. Ambos deben decir que usas proveedores de IA como encargados y que los datos pueden procesarse fuera de México; el laboral, además, que la IA se usa sobre datos de empleados (nómina, evaluaciones, expedientes). Con eso queda cubierta la relación jurídica que la ley pide (Art. 9–IV LFPDPPP) y esos datos dejan de necesitar permiso caso por caso. Ajuste de una vez, con tu abogado.
- ☐ **Conectores: lista aprobada y permiso mínimo** por conector — conectar el correo significa que la IA lee todo el correo; si solo necesita leer, sin escritura. Cuentas personales bloqueadas.
- ☐ **Agentes habilitados por equipo y caso de uso,** con acceso mínimo — solo las carpetas, repositorios y aplicaciones que la tarea necesita. Agentes de código en entorno aislado: sin red salvo dominios aprobados, escritura limitada al proyecto.
- ☐ **Búsqueda web de los agentes: dominios restringidos** — una página web puede darle órdenes al agente que la visita y hacerlo actuar en tu nombre. Limita a dónde puede navegar, o apágala donde no aporte.
- ☐ **Permisos de agentes: manual por defecto** — leer puede ser automático; escribir, enviar y ejecutar se aprueban; lo irreversible (borrar, enviar correos, publicar, pagar, subir a producción) siempre lo confirma una persona. Aprobación automática total solo en entornos aislados sin datos reales.
- ☐ **Llaves de API en el gestor de secretos** — nunca en el mensaje a la IA ni en archivos compartidos. Facturación centralizada.

Verificado por: _____ Fecha: _____

Con el sistema asegurado, solo un tema necesita explicación antes de la página firmable: **qué datos pueden entrar.**

El semáforo de datos.

Cuatro colores con ejemplos de tu operación. Escríbelos con los casos que tu gente vive a diario — lo específico es lo que hace la política cumplible.

VERDE — úsalo libre

- Información pública
- Borradores propios sin datos de clientes
- Plantillas y ejemplos genéricos
- Corrección, formato y traducción de texto propio

AMARILLO — solo en cuenta empresarial aprobada

- Documentos internos: propuestas, cotizaciones, minutas, márgenes y estrategia comercial
- Datos ordinarios de clientes y correos de trabajo
- Finanzas de tu empresa o de una empresa cliente — las personas morales no son titulares de datos personales
- Nómina y evaluaciones, cuando el aviso de privacidad laboral ya cubre el uso de IA
- Código propietario
- **Regla general: todo dato de una persona identificable vive aquí como mínimo**

ROJO — necesita permiso de alguien fuera de tu empresa

- Material bajo convenio de confidencialidad → lo autoriza quien firmó el convenio
- Datos sensibles de una persona — salud, información genética, origen étnico, creencias, opiniones políticas, preferencia sexual → consentimiento expreso *y por escrito* del titular (Art. 8 LFPDPPP; la lista de la ley es enunciativa, no limitativa)
- Datos financieros de una persona física — cuentas, ingresos, historial crediticio → consentimiento expreso (Art. 7)

NEGRO — nunca; no existe proceso que lo permita

- Contraseñas
- Llaves de API y tokens
- Números completos de tarjeta
- Cuentas bancarias
- Secretos de producción

Ojo con los espacios compartidos. En tu cuenta, pegar un margen es como abrir el archivo: ya tienes acceso. En un proyecto o carpeta compartida lo ve todo el equipo. El amarillo asume tu cuenta.

04 · EL SEMÁFORO DE DATOS

Por qué rojo y negro van por separado.

Si metes todo en "nunca", quien necesita trabajar con esos datos lo hará de todos modos: en cuenta externa y a escondidas. El rojo obliga a conseguir **el permiso que el dato pide**: el del titular cuando es información de una persona, el de quien firmó cuando es material bajo convenio. Ese permiso es de *entrada* — quién mete el dato; la revisión humana de la política es de *salida* — qué sale de la empresa. Revisar la propuesta final no borra que el expediente quedó en un historial: se necesitan las dos compuertas. Con salud, verifica también el plan (Anthropic solo cubre el convenio HIPAA en Enterprise y API, no en Team), y si tu cliente te transfiere requisitos de cumplimiento por contrato, tus herramientas de IA los heredan.

Seudonimiza cuando puedas

La ley pide tratar solo los datos que la finalidad necesita, y saca del requisito de consentimiento a los datos que pasan por un procedimiento de disociación (Art. 9–III LFPDPPP). Si "Cliente A" funciona igual para la tarea, úsalo. Y si el dato viene de un cliente con contrato o convenio de confidencialidad, verifica primero que permita compartir con subprocesadores — el proveedor de IA lo es.

La regla que resuelve el resto

Ningún semáforo cubre todos los casos. Para lo que no esté en tus listas, la política lleva una sola instrucción: **si no sabes de qué color es algo, pregunta antes de pegarlo.** Es más útil que cualquier definición, y convierte cada duda en una mejora de tus listas.

La política: una página, se firma.

Política de uso de IA — [Empresa]

APLICA A: TODO EL PERSONAL Y CONTRATISTAS · VIGENTE DESDE: [FECHA] · RESPONSABLE: [NOMBRE, CORREO]

Aviso de 100x — bórralo antes de publicar tu política. Este es un modelo de referencia, no un documento legal terminado. 100x no es una firma de abogados y no presta asesoría jurídica; entregarte esta plantilla no crea relación de asesoría. Se proporciona "tal cual", sin garantía de exactitud, vigencia o idoneidad para tu caso. Antes de adoptarla debes adaptarla a tu operación y someterla a revisión de tu asesor legal, en particular respecto de la LFPDPPP, tu Reglamento Interior de Trabajo y la normativa de tu sector. El uso de este documento es bajo tu propia responsabilidad.

1. Herramientas aprobadas. Solo [Claude Team / ChatGPT Business / Gemini Workspace / Microsoft 365 Copilot] con la cuenta asignada por la empresa. Cualquier cuenta externa a la empresa — personal, gratuita o de pago, aunque sea la misma herramienta — está prohibida para trabajo. ¿Quieres otra herramienta? Pídela a [responsable].

2. Datos.
🟢 Libre: información pública, borradores propios, plantillas.
🟡 Solo en cuenta corporativa: documentos internos (propuestas, cotizaciones, minutas, márgenes y estrategia comercial), datos ordinarios de clientes y correos de trabajo, finanzas de la empresa, nómina y evaluaciones, código propietario. Todo dato de una persona identificable vive aquí como mínimo.
🔴 Necesita permiso de fuera de la empresa: material bajo convenio de confidencialidad (lo autoriza quien firmó); datos sensibles de una persona — salud, información genética, origen étnico, creencias, opiniones políticas, preferencia sexual — (consentimiento expreso y por escrito del titular); datos financieros de una persona física, como cuentas, ingresos o historial crediticio (consentimiento expreso).
⛔ Nunca: contraseñas, llaves y tokens, tarjetas, cuentas bancarias, secretos de producción.
Si la tarea no necesita el nombre real, usa seudónimos ("Cliente A"). **Si no sabes de qué color es algo, pregunta a [responsable] antes de pegarlo.**

3. Revisión humana. Todo lo que sale de la empresa (correos, propuestas, código, publicaciones) lo revisa una persona antes de enviarse. En temas legales, médicos, financieros o de empleo, revisa y firma un profesional del área; si ese contenido llega al consumidor, se divulga que hubo IA. Verifica datos y citas: los modelos se equivocan con confianza.

4. Prohibido. Suplantar personas o generar contenido engañoso. Decisiones automatizadas sobre personas (contratación, despido, crédito) sin revisión humana. Subir datos negros, o rojos sin la aprobación o consentimiento que piden. Vigilancia de empleados o terceros. Entregar resultados de IA como trabajo verificado sin revisarlos.

5. Agentes y conectores. No actives IA que ejecute acciones por sí misma ni conectes aplicaciones sin autorización de [responsable]. Las acciones irreversibles (borrar, enviar, publicar, pagar) siempre las confirma una persona.

6. Propiedad del contenido. Lo generado con cuentas corporativas pertenece a la empresa. No uses IA para reproducir material de terceros con derechos de autor. Contenido de alto valor (marcas, campañas, código crítico) pasa revisión antes de publicarse.

7. Capacitación. Obligatoria al ingresar y al menos una vez al año. Esta política se firma al concluirla.

8. Incidentes. ¿Subiste algo que no debías o viste un mal uso? Repórtalo a [responsable] el mismo día. Si involucra datos personales, [responsable] evalúa de inmediato el deber de notificar a los titulares (Art. 19 LFPDPPP). Reportar no se sanciona; ocultar sí.

9. Incumplimiento y revisión. Se sanciona conforme al Reglamento Interior de Trabajo y la Ley Federal del Trabajo; para externos, conforme a su contrato. Esta política se actualiza cada [6 / 12] meses. Versión: [n.º — fecha].

Firma / acuse: _____

¿Por qué tan corta la lista de prohibidos? Cada regla extra diluye las cinco que importan. Lo que no cabe en la política, cabe en el semáforo o en la lista del administrador. Resiste la tentación del anexo legal — y recuerda que el punto 4 no tiene excepciones: el EU AI Act clasifica la IA en decisiones de empleo como alto riesgo.

06 · EL DESPLIEGUE

La política se firma al final de la capacitación.

Así lo dice la cláusula 7 de tu propia política — y es el paso donde el papel se convierte en comportamiento. El semáforo, la revisión antes de enviar y el reporte de incidentes dependen del criterio de cada persona, y el criterio se entrena.

Qué cubre

- El semáforo de datos, con ejemplos reales de tu empresa — qué es verde, amarillo, rojo y negro en tu operación, con los casos que tu gente vive a diario.
- Qué se revisa antes de que algo salga de la empresa — correos, propuestas, código, publicaciones.
- Cuándo y cómo reportar un incidente — y que reportar es seguro.

Cuándo

Al ingresar y al menos una vez al año. Cada persona firma la política al concluir; el acuse anual renueva el compromiso y mantiene viva la regla.

Cómo sabes que funcionó

Tu gente pregunta antes de meter un dato rojo. Los incidentes se reportan el mismo día. El acuse anual se completa sin perseguir a nadie.

El lugar de este paso en el sistema → Contratar protege los datos. Configurar impone lo automático. Firmar documenta el acuerdo. Capacitar es lo que hace que el semáforo se use un martes a las 4pm, con un cliente esperando la propuesta.

07 · MANTENIMIENTO

Corta y viva.

- → **Un dueño por capa:** la configuración (TI/administrador) y la política (RH/dirección), cada una con nombre y correo para dudas e incidentes.
- → **Revisa las dos juntas cada 6–12 meses** o al cambiar de herramienta o de plan. Al subir de plan, pasa reglas de la política a la configuración. La IA cambia rápido; una política de 2024 hoy es ficción.
- → **Acuse anual:** cada empleado firma la política; el administrador marca su lista de verificación. Sin acuse, ninguna de las dos existe.

FUENTES OFICIALES

ANTHROPIC

Política de uso — anthropic.com/legal/aup · Términos comerciales — anthropic.com/legal/commercial-terms · DPA — anthropic.com/legal/data-processing-addendum · Portal de confianza — trust.anthropic.com

OPENAI

Enterprise privacy — openai.com/enterprise-privacy · Agent approvals & security — developers.openai.com/codex/agent-approvals-security · Running Codex safely — openai.com/index/running-codex-safely

GOOGLE

Gemini for Workspace FAQ — knowledge.workspace.google.com · Generative AI Prohibited Use Policy — support.google.com/gemini/answer/16625148 · AI Privacy Hub — workspace.google.com/security/ai-privacy

MICROSOFT

Data, Privacy and Security for Microsoft 365 Copilot — learn.microsoft.com · Enterprise data protection — learn.microsoft.com/copilot/enterprise-data-protection · Purview para IA generativa — learn.microsoft.com/purview/ai-microsoft-purview

MÉXICO

LFPDPPP (nueva ley, DOF 20-mar-2025; última reforma DOF 14-11-2025) — diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf · Arts. 7 (financieros o patrimoniales: consentimiento expreso), 8 (sensibles: expreso y por escrito), 9 (excepciones al consentimiento — III disociación, IV relación jurídica), 19 (vulneraciones: notificación inmediata a titulares)

La configuración es el candado.
La política es el papel.
La adopción es el trabajo.

En 100x llevamos la IA a empresas mexicanas: 50+ proyectos en 15+ industrias. Si quieres que tu equipo use IA bien, hablemos.

bueno@100x.mx · 100x.mx

Pide la plantilla editable en Word y te la mandamos el mismo día.