

Guía Completa: Privacidad y Seguridad en IA Generativa para Profesionales

Todo lo que necesitas saber antes de usar ChatGPT, Claude, Gemini, Copilot, Perplexity o Grok con datos de trabajo

Por Felipe Catalán - AIThinking Methodology

www.ai-thinking.io

Enero 2026

Por qué esta guía existe

Si eres gerente, consultor, o C-level, probablemente tienes NDAs firmados con clientes o acuerdos de confidencialidad con tu empleador.

Y probablemente usas (o quieres usar) herramientas de IA generativa para trabajar más rápido.

La pregunta que nadie responde claramente es:

"¿Puedo usar ChatGPT con información de mi cliente sin violar el NDA que firmé?"

Esta guía responde esa pregunta con datos concretos, no opiniones.

Analicé los Terms of Service y Privacy Policies de las 6 principales plataformas de IA generativa, comparé sus certificaciones de seguridad, documenté sus incidentes, y creé un framework de decisión que puedes usar hoy.

PARTE 1: El contexto que necesitas entender

El caso Samsung: Por qué esto importa

En abril de 2023, tres incidentes separados en Samsung Semiconductor cambiaron la industria:

1. Un ingeniero pegó **código fuente defectuoso** en ChatGPT buscando correcciones
2. Otro ingeniero subió **código propietario** para optimización
3. Un tercero transcribió y resumió una **reunión confidencial interna**

¿Qué pasó?

En ese momento, ChatGPT usaba todas las conversaciones de usuarios gratuitos para entrenar sus modelos. La información propietaria de Samsung se convirtió en datos de entrenamiento de OpenAI.

Consecuencias:

- Samsung prohibió ChatGPT inmediatamente
- Goldman Sachs, JPMorgan, Bank of America, Citigroup siguieron con restricciones similares

- OpenAI lanzó ChatGPT Enterprise con garantías contractuales de no-entrenamiento

La lección: No fue culpa de ChatGPT. Fue usar el tier equivocado para información confidencial.

El riesgo de memorización: Los datos técnicos

Investigadores de Google DeepMind publicaron en 2023 un estudio que demostró que **aproximadamente 3% del texto generado por ChatGPT está memorizado** de sus datos de entrenamiento.

Con técnicas específicas de extracción, lograron:

- Recuperar información personal identificable (PII)
- Extraer direcciones de correo electrónico
- Obtener fragmentos de código fuente
- Reproducir datos de entrenamiento verbatim

El costo del experimento: \$200 en API calls.

El resultado: 10,000+ ejemplos verbatim de datos de entrenamiento.

Esto significa que si tu información entra al entrenamiento, puede salir en respuestas a otros usuarios.

PARTE 2: La estructura de tiers que debes entender

La confusión que todos tienen

Lo que la gente cree	La realidad
"Pago \$20, tengo protección"	Los \$20 compran capacidad, no protección
"Con opt-out estoy seguro"	El opt-out es un toggle, no un contrato
"Enterprise es para grandes empresas"	Team (\$25-30/usuario) ya tiene DPA

Tabla maestra: Qué obtienes en cada tier

Aspecto	FREE	PRO ~\$20	TEAM ~\$25-30	ENTERPRISE
Precio	\$0	~\$20/mes	~\$25-30/usuario/mes	\$50+/usuario
¿Entrenan con tus datos?	Sí (opt-out)	Sí (opt-out)	NO	NO
Tipo de garantía de no-entrenamiento	Toggle	Toggle	Contractual	Contractual reforzada
DPA (Data Processing Agreement)	✗	✗	✓	✓ Personalizable

Responsabilidad máxima del proveedor	~\$100	~\$240	~12 meses fees	Negociable
¿Quién indemniza a quién?	Tú a ellos	Tú a ellos	Tú a ellos	Bidireccional
Indemnización por IP en outputs	✗	✗	✗ o parcial	✓
Admin controls	✗	✗	✓ Básicos	✓ Completos
Audit logs	✗	✗	✓	✓ Exportables
Zero Data Retention	✗	✗	✗	✓ Disponible
BAA para HIPAA	✗	✗	Algunos	✓
SLA con uptime garantizado	✗	✗	⚠ Limitado	✓ Con créditos
Garantías legales	"AS IS"	"AS IS"	Parciales	Completas

PARTE 3: Lo que dicen los Terms of Service (citas reales)

"AS IS": El término que debes entender

Todos los ToS de planes consumer (Free y ~\$20) incluyen esta cláusula:

"THE SERVICES ARE PROVIDED 'AS IS' AND 'AS AVAILABLE' WITHOUT WARRANTY OF ANY KIND"

¿Qué significa legalmente?

"AS IS" significa que el proveedor **no garantiza nada** sobre el servicio:

El proveedor NO garantiza que...	Implicación para ti
El servicio funcione sin interrupciones	Si se cae, no hay compensación
El servicio sea preciso o libre de errores	Si te da información incorrecta, tu problema
El servicio sea adecuado para tu propósito	Si no sirve para tu caso, tu problema
El output no infrinja derechos de terceros	Si el output viola copyright, tu problema
Tus datos estén seguros	Si hay brecha, tu problema (más allá de ~\$100-240)

Analogía simple

Comprar un auto "AS IS" = lo compras "como está". Si el motor falla al día siguiente, no puedes reclamar. No había garantía de que funcionara.

Eso es exactamente lo que aceptas con planes consumer de IA.

Limitación de responsabilidad: Los números reales

OpenAI (ChatGPT Free/Plus/Pro)

"OUR AGGREGATE LIABILITY UNDER THESE TERMS WILL NOT EXCEED THE GREATER OF THE AMOUNT YOU PAID FOR THE SERVICE THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS BEFORE THE LIABILITY AROSE OR ONE HUNDRED DOLLARS (\$100)."

Traducción: Si hay una filtración masiva, lo máximo que puedes recuperar es \$100 o lo que pagaste en 12 meses (~\$240 con Plus).

Anthropic (Claude Free/Pro)

"THE SERVICES ARE PROVIDED 'AS IS' AND 'AS AVAILABLE' WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED"

Límite similar: ~\$100 o fees pagadas en 12 meses.

Google (Gemini Consumer)

Límite: Mayor entre \$200 o fees pagadas en 12 meses

Ligeramente mejor, pero aún insignificante para pérdidas reales.

Google (Gemini Starter Edition) - Advertencia explícita:

"DO NOT SUBMIT SENSITIVE, CONFIDENTIAL, OR PERSONAL INFORMATION"

Te dicen literalmente que no pongas información confidencial.

Microsoft (Copilot Consumer)

"Copilot is for entertainment purposes only. It can make mistakes, and it may not work as intended. **Don't rely on Copilot for important advice. Use Copilot at your own risk.**"

Microsoft declara explícitamente que Copilot consumer es para "entretenimiento". No para trabajo serio.

xAI (Grok) - El más restrictivo

"UNDER NO CIRCUMSTANCES WILL XAI BE RESPONSIBLE FOR ANY DAMAGE, LOSS, OR INJURY RESULTING FROM HACKING, TAMPERING, OR OTHER UNAUTHORIZED ACCESS"

Grok explícitamente dice que si hackean sus sistemas y roban tu información, no es su responsabilidad.

La cláusula de indemnización: Quién protege a quién

En planes consumer (Free y ~\$20): TÚ los proteges a ELLOS

OpenAI (Business Terms):

"Customer agrees to indemnify... against any liabilities... arising out of a third party claim related to (a) use of the Services in violation of this Agreement, (b) Customer Applications, or (c) Input."

Microsoft (Copilot Consumer):

"You agree to indemnify us and hold us harmless (including our affiliates, employees and any other agents) from and against any claims, losses, and expenses (including attorneys' fees) arising from or relating to your use of Copilot"

¿Qué significa en la práctica?

Escenario	ToS Consumer	ToS Enterprise
TÚ usas mal el servicio y alguien demanda al proveedor	Tú los defiendes <input checked="" type="checkbox"/>	Tú los defiendes <input checked="" type="checkbox"/>
El OUTPUT infringe IP de terceros y te demandan a TI	Estás solo <input checked="" type="checkbox"/>	El proveedor te defiende <input checked="" type="checkbox"/>
Hay una BRECHA de datos del lado del proveedor	Máximo recuperas ~\$240 <input checked="" type="checkbox"/>	Límites más altos + DPA <input checked="" type="checkbox"/>

El punto clave: La indemnización por infracción de IP en outputs (cuando el proveedor te defiende si alguien te demanda por usar su output) **típicamente solo está disponible en planes Enterprise o Business avanzados**, y los detalles varían por proveedor y región.

Escenario práctico: El cálculo que debes hacer

Situación: Pegas información confidencial de un cliente en ChatGPT Plus. Hay una filtración. Tu cliente te demanda por violar el NDA.

Pregunta	Respuesta
¿Cuánto perdiste con el cliente?	\$500,000 (ejemplo)
¿Cuánto puedes recuperar de OpenAI?	~\$240 (12 meses × \$20)
¿OpenAI te defiende legalmente?	No
¿Quién paga los \$499,760 restantes?	Tú

PARTE 4: Análisis detallado por plataforma

ChatGPT (OpenAI)

Estructura de tiers

Tier	Precio	¿Entrena?	DPA	Certificaciones
Free	\$0	Sí (opt-out)	<input checked="" type="checkbox"/>	No aplican
Plus	\$20/mes	Sí (opt-out)	<input checked="" type="checkbox"/>	No aplican
Pro	\$200/mes	Sí (opt-out)	<input checked="" type="checkbox"/>	No aplican

Team	\$25-30/usuario	NO	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Enterprise	Negociado	NO	<input checked="" type="checkbox"/> Completo	<input checked="" type="checkbox"/> Todas
API	Por uso	NO por defecto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Cómo activar opt-out (Free/Plus/Pro)

Settings → Data Controls → "Improve the model for everyone" → OFF

Política de Team

"Content submitted to ChatGPT Team is not used to train our models."

Garantía contractual, no solo un toggle.

Certificaciones (Enterprise/API únicamente)

- SOC 2 Type II
- ISO 27001/27017/27018/27701
- HIPAA con BAA (Healthcare tier)

Importante: Las certificaciones NO aplican a Free, Plus, o Pro.

Retención de datos

- Estándar: 30 días post-eliminación
- Enterprise: Zero Data Retention disponible para API

Incidentes documentados

- Memorización: ~3% de outputs pueden contener datos de entrenamiento
- Bug marzo 2023: Títulos de conversaciones de otros usuarios visibles temporalmente

Claude (Anthropic)

Estructura de tiers

Tier	Precio	¿Entrena?	DPA
Free	\$0	Solo si OPT-IN activo	<input checked="" type="checkbox"/>
Pro	\$20/mes	Solo si OPT-IN activo	<input checked="" type="checkbox"/>
Team	\$25-30/usuario	NO	<input checked="" type="checkbox"/>
Enterprise	Negociado	NO	<input checked="" type="checkbox"/> Completo
API	Por uso	NO	<input checked="" type="checkbox"/>

El diferenciador clave: Enfoque histórico hacia opt-in

Anthropic ha sido la plataforma más alineada con un modelo **opt-in** en sus canales Enterprise y API, donde tus datos NO se usan para entrenamiento a menos que lo autorices explícitamente.

Modelo	Cómo funciona	Plataformas
Opt-out	Tus datos SE USAN por defecto. Debes desactivarlo.	ChatGPT, Gemini, Copilot, Perplexity, Grok
Opt-in (Enterprise/API)	Tus datos NO se usan. Debes activarlo tú.	Claude Enterprise, Claude API

Nota importante: En planes consumer (Free/Pro), Anthropic introdujo cambios en 2025 que permiten entrenamiento. Verifica siempre la configuración actual de tu cuenta.

Cambio de agosto 2025

Los ToS Consumer ahora permiten entrenamiento con opt-in. Si activas el entrenamiento: **5 años de retención** (vs 30 días sin).

Política comercial explícita

"Anthropic may not train models on Customer Content from Services."

Certificaciones destacadas

- SOC 2 Type II
- ISO 27001
- ISO 42001 - Primer AI en obtener esta certificación de gestión de sistemas de IA
- HIPAA con BAA (Enterprise + ZDR)

Retención

- Base: 30 días
- Si permite entrenamiento: hasta 5 años en formato de-identificado

Incidentes documentados

- No hay brechas de plataforma reportadas
- Casos de uso malicioso externo (no responsabilidad de Anthropic)

Google Gemini

Estructura de tiers

Tier	Precio	¿Entrena?	Revisión humana	DPA
Free	\$0	Sí (opt-out)	Sí	
Advanced	\$20/mes	Sí (opt-out)	Sí	

Workspace	\$12-25/usuario+	NO	No	<input checked="" type="checkbox"/> CDPA
-----------	------------------	----	----	--

Cómo activar opt-out

Gemini Activity → Desactivar

Advertencia crítica: Revisión humana

Los datos revisados por humanos se retienen **hasta 3 años** independientemente del setting de Gemini Activity.

Esto significa que un empleado de Google puede potencialmente leer tu conversación.

Gemini for Workspace (Cloud Data Processing Addendum)

"Workspace does not use customer data for training models without customer's prior permission."

Certificaciones (Workspace)

- SOC 1/2/3
- ISO 27001/27017/27018/27701
- ISO 42001 (primero en productividad)
- FedRAMP High
- HIPAA con BAA

Nota: NotebookLM y Gemini en Chrome NO tienen estas certificaciones.

Vulnerabilidades parcheadas 2025

Se han reportado vulnerabilidades relacionadas con inyección de prompts y exfiltración de datos durante 2025, que fueron parcheadas. Consulta los avisos de seguridad oficiales de Google si esto es crítico para tu organización.

Microsoft Copilot

Estructura de tiers

Tier	Precio	¿Entrena?	DPA
Free (web)	\$0	Sí (opt-out)	<input checked="" type="checkbox"/>
Pro	\$20/mes	Sí (opt-out)	<input checked="" type="checkbox"/>
Microsoft 365 Copilot	\$30/usuario	NO	<input checked="" type="checkbox"/> Completo

La declaración que debes conocer

Microsoft advierte explícitamente en sus ToS que Copilot consumer puede cometer errores, no debe usarse como base única para decisiones importantes, y debe usarse bajo tu propio riesgo. El mensaje es claro: **no confíes en Copilot consumer para trabajo serio.**

Microsoft 365 Copilot (Business)

"Prompts, responses, and data accessed through Microsoft Graph aren't used to train foundation LLMs."

Microsoft actúa como **data processor**, no controller, bajo el DPA.

Exclusiones automáticas de entrenamiento (Copilot consumer)

Algunos usuarios están excluidos automáticamente:

- Cuentas organizacionales
- Menores de 18 años
- Residentes de: Brasil, China, Israel, Corea del Sur, Nigeria, Vietnam

Retención

- Consumer: 18 meses
- Enterprise: configurable vía Microsoft Purview

HIPAA/BAA cubre:

- M365 Copilot
- Copilot Studio
- Security Copilot
- Web search queries (crítico para organizaciones de salud)

Vulnerabilidades 2024-25

Se han reportado vulnerabilidades de severidad alta relacionadas con exfiltración de datos vía emails y ataques de re-prompting, que fueron parcheadas. La Cámara de Representantes de EE.UU. prohibió Copilot temporalmente en marzo 2024. Consulta los avisos de seguridad oficiales de Microsoft si esto es crítico para tu organización.

Perplexity

Estructura de tiers

Tier	Precio	¿Entrena?	DPA
Free	\$0	Sí (opt-out)	<input checked="" type="checkbox"/>
Pro	\$20/mes	Sí (opt-out)	<input checked="" type="checkbox"/>
Enterprise Pro	Negociado	NO	<input checked="" type="checkbox"/>
API Sonar	Por uso	NO (ZDR estricto)	<input checked="" type="checkbox"/>

Limitaciones importantes

- **Data residency:** Solo AWS Norteamérica - no hay opciones EU
- Retención de archivos adjuntos: 7 días auto-delete

Certificaciones

- SOC 2 Type II
- ISO 27001 No verificado en fuentes oficiales
- HIPAA con BAA (Enterprise, requiere negociación)

Incidentes 2025

Se han reportado vulnerabilidades en el browser Comet relacionadas con prompt injection, así como problemas de seguridad en la app Android (SSL, API keys). También ha habido controversias por ignorar robots.txt en scraping. Consulta los avisos oficiales si esto es crítico para tu organización.

Grok (xAI) - EL MÁS RIESGOSO

Estructura de tiers

Tier	Precio	¿Entrena?	DPA
Free (X Premium)	Incluido en X	Sí (opt-out)	
SuperGrok	\$30/mes	Sí (opt-out)	Limitado
Enterprise	Negociado	NO	

ToS más restrictivos de todas las plataformas

Cambios de noviembre 2025:

Aspecto	Antes	Ahora
Período para demandas federales	2 años	1 año
Jurisdicción	Variable	Solo Tarrant County, Texas
Asimetría legal	-	xAI puede demandarte donde sea, tú solo en Texas

Exclusión explícita de responsabilidad por hacking

"UNDER NO CIRCUMSTANCES WILL XAI BE RESPONSIBLE FOR ANY DAMAGE, LOSS, OR INJURY RESULTING FROM HACKING, TAMPERING, OR OTHER UNAUTHORIZED ACCESS"

Si hackean xAI y roban tu información: no es su problema.

Integración con X (Twitter)

Tus prompts y outputs ahora son "Content" bajo licencia de X:

"You grant X a worldwide, non-exclusive, royalty-free license... to use, copy, reproduce, process, adapt, modify, publish, transmit, display, and distribute such Content **for any purpose**, including training ML/AI models."

Incidentes graves 2025

1. Agosto 2025: ~370,000 conversaciones de usuarios fueron **indexadas públicamente** en Google, Bing y

DuckDuckGo. Se expusieron: contraseñas, consultas médicas, instrucciones para actividades ilegales.

2. **Mayo 2025:** Sistema hackeado, prompts modificados para spam político.
3. **Julio 2025:** API keys expuestas en GitHub público por empleados de DOGE, otorgando acceso a 52+ modelos xAI.
4. **Diciembre 2025-Enero 2026:** Crisis de CSAM/deepfakes - investigaciones abiertas por UK Ofcom y California AG.

GDPR

Investigación activa por Ireland DPC desde abril 2025. Posibles multas de **4% de ingresos globales**.

Recomendación

Organizaciones risk-averse deberían evitar Grok.

PARTE 5: Certificaciones de seguridad explicadas

¿Qué significan y cuánto importan?

Certificación	Qué verifica	Nivel de confianza	Quién la tiene
SOC 2 Type II	Controles de seguridad funcionaron durante 6-12 meses	★★★★★ Alto	ChatGPT Enterprise, Claude, Gemini, Copilot, Perplexity
SOC 2 Type I	Controles existen en un momento específico	★★★★ Medio	Grok (declarado)
ISO 27001	Sistema de gestión de seguridad de información	★★★★★ Alto	ChatGPT Enterprise, Claude, Gemini, Copilot
ISO 27017	Seguridad específica para servicios cloud	★★★★★ Alto	ChatGPT Enterprise, Claude, Gemini, Copilot
ISO 27018	Protección de datos personales en cloud	★★★★★ Alto	ChatGPT Enterprise, Claude, Gemini, Copilot
ISO 27701	Gestión de información de privacidad (ayuda con GDPR)	★★★★★ Alto	ChatGPT Enterprise, Claude, Gemini, Copilot
ISO 42001	Gestión de sistemas de IA (nuevo 2023)	★★★★★★ Muy alto	Solo Claude y Gemini
FedRAMP High	Máximo nivel gobierno US para cloud	★★★★★★ Muy alto	Gemini Workspace, M365 Copilot
HIPAA/BAA	Cumplimiento para información de salud en EE.UU.	Requerido para salud	Todos en tiers Enterprise

ISO 42001: La certificación que diferencia

ISO 42001 es el **nuevo estándar internacional para gestión de sistemas de IA** (publicado 2023).

Solo **Claude y Gemini** lo tienen actualmente.

Demuestra que la empresa tiene procesos formales para:

- Gestión responsable de IA
- Evaluación de riesgos de IA
- Transparencia en sistemas de IA

PARTE 6: Ranking de plataformas

Para uso con información confidencial

Posición	Plataforma	Fortalezas	Debilidades	Veredicto
1	Microsoft 365 Copilot	Mejor integración enterprise, track record maduro, EU Boundary, FedRAMP High	Requiere ecosistema Microsoft, precio más alto	<input checked="" type="checkbox"/> Mejor si ya usas M365
2	Claude Enterprise	ISO 42001, enfoque histórico opt-in, certificaciones robustas, sin incidentes de plataforma	Data residency US base, menos integraciones	<input checked="" type="checkbox"/> Mejor para privacidad-first
3	ChatGPT Enterprise	Track record más largo post-Samsung, mayor ecosistema	Modelo opt-out, memorización documentada	<input checked="" type="checkbox"/> Más versátil
4	Gemini Workspace	Certificaciones Google Cloud, FedRAMP High, ISO 42001	Retención larga en consumer (3 años), revisión humana	<input checked="" type="checkbox"/> Si usas Google Workspace
5	Perplexity Enterprise	Bueno para research, ZDR en API	Solo data residency NA, documentación incompleta	 Emergente
6	Grok	Integración X/Twitter	Múltiples incidentes graves, ToS restrictivos, investigación GDPR	 No recomendado

Para planes de ~\$20/mes (si no puedes pagar Team)

Posición	Plataforma	Por qué
1	Claude Pro	Históricamente más orientado a opt-in. Verifica configuración actual. 30 días retención base.
2	ChatGPT Plus	Opt-out claro. Proceso de eliminación documentado.

3	Gemini Advanced	Límite \$200 (vs \$100). Pero retención hasta 3 años y revisión humana.
4	Copilot Pro	Declara "entretenimiento". Al menos las expectativas son claras.
5	Perplexity Pro	Menor transparencia en políticas.
6	Grok Premium	ToS más restrictivos. Historial de incidentes. Evitar.

PARTE 7: Framework de decisión

Paso 1: Clasifica tu información

Nivel	Ejemplos	Tier mínimo
Pública	Investigación de info pública, aprendizaje, contenido para publicar	Free OK
Semi-confidencial	Borradores, research general, docs técnicos no propietarios	Pro (~\$20) + opt-out
Confidencial estándar	Estrategias internas, análisis financieros no públicos, propuestas	Team (~\$25-30)
Altamente confidencial	M&A, patentes, código core, datos de clientes identificables, NDA estricto	Enterprise + ZDR

Paso 2: Verifica tu configuración

Si usas Free o ~\$20/mes:

Plataforma	Verificar
ChatGPT	Settings → Data Controls → "Improve the model" → OFF
Claude	Verifica en Settings → Privacy si el entrenamiento está desactivado
Gemini	Gemini Activity → Desactivado
Copilot	Settings → Privacy → Desactivado
Perplexity	Settings → Data Privacy → Desactivado
Grok	Settings → Privacy → OFF + usar Private Chat

Si usas Team o Enterprise:

- ¿Tengo el DPA firmado?
- ¿Están los audit logs activos?
- ¿Está configurada la retención mínima?
- ¿Tengo documentada la política interna de uso?

Paso 3: Antes de pegar información de trabajo

Checklist rápido

1. ¿Qué tier estoy usando?

- Free/Pro → Solo info pública o semi-confidencial
- Team → Info confidencial estándar OK
- Enterprise → Todo OK con configuración correcta

2. ¿Puedo anonimizar?

- Quitar nombres de clientes/empresas
- Quitar datos identificables
- Usar placeholders: "[CLIENTE]", "[EMPRESA]"

3. ¿Realmente necesito incluir esta información?

- A veces puedes reformular la pregunta sin datos sensibles
- Describe el problema en abstracto

4. ¿Qué pasa si esto se filtra?

- Si la respuesta te preocupa, probablemente necesitas tier más alto

PARTE 8: Glosario completo

Términos de privacidad

Término	Qué significa	Ejemplo
Opt-in	Debes ACTIVAR explícitamente para que aplique	Claude Enterprise/API: NO entran a menos que lo autorices
Opt-out	Está ACTIVADO por defecto, debes desactivarlo	ChatGPT: Sí entran a menos que TÚ lo desactives
Zero Data Retention (ZDR)	No almacenan nada después de procesar	Máxima seguridad. Solo Enterprise/API.
Data Residency	Dónde se almacenan físicamente tus datos	Importante para GDPR (datos EU en EU)
AS IS	Sin garantías de ningún tipo	"Como está". Si falla, tu problema.

Contratos y acuerdos

Sigla	Nombre	Qué es	Cuándo lo necesitas
NDA	Non-Disclosure Agreement	Prohíbe compartir info confidencial	Ya lo tienes con clientes
DPA	Data Processing Addendum	Contrato de cómo manejan tus datos	Obligatorio GDPR. Solo Team+.
BAA	Business Associate Agreement	Contrato HIPAA para info de salud	Obligatorio para PHI en EE.UU.
SCCs	Standard Contractual Clauses	Cláusulas EU para transferir datos fuera	Transferencias US-EU
ToS	Terms of Service	Condiciones de uso	Free y Pro solo tienen esto

Regulaciones

Sigla	Nombre	Alcance	Multas
GDPR	General Data Protection Regulation	Datos de ciudadanos EU, sin importar dónde operes	Hasta 4% ingresos globales
HIPAA	Health Insurance Portability and Accountability Act	Info médica en EE.UU.	Variables, pueden ser criminales
CCPA	California Consumer Privacy Act	Residentes de California	Hasta \$7,500 por violación intencional

Certificaciones

Certificación	Qué verifica	Tiempo de validez
SOC 2 Type I	Controles EXISTEN	Momento específico
SOC 2 Type II	Controles FUNCIONAN	6-12 meses
ISO 27001	Sistema de gestión de seguridad	3 años (auditorías anuales)
ISO 42001	Sistema de gestión de IA	3 años
FedRAMP	Seguridad cloud gobierno US	Continuo

PARTE 9: Resumen ejecutivo

Los 5 puntos que debes recordar

1. Pagar \$20/mes NO te protege

Los planes Pro/Plus/Advanced compran capacidad, no protección. Las políticas de privacidad son esencialmente iguales a Free.

2. "AS IS" significa sin garantías

Todos los ToS consumer dicen que no garantizan nada: ni que funcione, ni que sea preciso, ni que sea seguro, ni confidencialidad.

3. El salto real está en Team (~\$25-30/usuario)

Por \$5-10 más que Pro, obtienes DPA, garantía contractual de no-entrenamiento, y audit logs. Es el mínimo para información confidencial.

4. Claude ha sido el más alineado con opt-in

Anthropic ha sido históricamente la plataforma más orientada a opt-in, especialmente en Enterprise y API. Verifica siempre la configuración actual de tu plan específico.

5. Grok es el más riesgoso

Múltiples incidentes graves en 2025, ToS más restrictivos, investigación GDPR activa. Evitar para uso profesional.

Tabla de decisión final

Si tu información es...	Usa como mínimo...	Configuración
Pública	Free	Cualquier plataforma OK
Semi-confidencial	Pro ~\$20	Con opt-out activado. Preferir Claude.
Confidencial	Team ~\$25-30	Con DPA. ChatGPT Team, Claude Team, M365 Copilot
Altamente confidencial	Enterprise	Con ZDR. Evitar Grok.

La respuesta a la pregunta inicial

"¿Puedo usar ChatGPT con información de mi cliente sin violar el NDA que firmé?"

Depende:

- **Free o ~\$20 sin opt-out:** Probablemente lo estás violando
- **~\$20 con opt-out:** Zona gris legal (mejor, pero sin garantía contractual)
- **Team con DPA:** Probablemente cumples (tienes compromisos contractuales)
- **Enterprise con ZDR:** Maximiza tus probabilidades de cumplimiento (siempre sujeto al texto específico de tu NDA y asesoría legal)

La diferencia entre violar un NDA y cumplirlo puede ser **\$5-10 más por usuario al mes.**

¿Tienes preguntas específicas sobre tu situación? Contáctame en www.ai-thinking.io

Felipe Catalán - AIThinking Methodology

www.ai-thinking.io

Última actualización: Enero 2026

Disclaimer: Este documento es informativo y no constituye asesoría legal. Los ToS y políticas cambian frecuentemente. Para situaciones con información confidencial, consulta con un abogado.