



NARSIL

INTELLIGENCE

ESTUDIOS NARSIL · 01

Lo que pegas en un chat ya no es solo tuyo

Qué hacen ChatGPT, Claude, Gemini y Copilot con la información que compartes, qué arriesga tu empresa y cómo evitarlo

OCTUBRE DE 2026

Resumen

1. **El plan importa más que la marca.** En los cuatro proveedores revisados, las cuentas de empresa no entrenan con los datos del cliente por defecto e incluyen contrato de encargo de tratamiento. Las cuentas personales, gratuitas o de pago, no ofrecen ninguna de las dos cosas con esas garantías.
2. **Pagar una suscripción individual no convierte una cuenta en profesional.** ChatGPT Plus o Pro, Claude Pro o Max y los planes personales de Google siguen las condiciones de consumo.
3. **Al otro lado puede haber personas.** Google advierte expresamente de que no se introduzca información confidencial en Gemini porque parte de las conversaciones las leen revisores humanos, y conserva esas conversaciones revisadas hasta tres años.
4. **Borrar no siempre es borrar.** Una orden judicial obligó a OpenAI a conservar en 2025 conversaciones que sus usuarios habían eliminado; Anthropic puede guardar hasta cinco años los chats de quien acepta el entrenamiento.
5. **La publicidad ya ha llegado.** Desde agosto de 2026 ChatGPT muestra anuncios en sus planes Free y Go en España, elegidos según el tema de la conversación.
6. **Si son datos de clientes, responde la empresa.** Usar una cuenta personal para tratar datos de terceros deja a la organización sin contrato de encargo, con transferencias internacionales sin control y con su protección de secretos empresariales debilitada.
7. **Hay alternativa.** Los modelos abiertos ejecutados en equipos propios permiten que la información crítica no salga de la organización. La propuesta de este estudio es clasificar la información y llevar cada nivel a la herramienta que le corresponde.

01

Un gesto de cinco segundos

En cualquier oficina, a cualquier hora, alguien está pegando algo en un asistente de inteligencia artificial: un contrato para que lo resuma, una hoja de cálculo con datos de clientes para ordenarla, el borrador de un correo delicado, el acta de una reunión o un fragmento de código que no compila. Es rápido, funciona y ahorra trabajo. Por eso se ha extendido sin que casi ninguna organización se haya parado a pensar qué ocurre después.

Lo que ocurre es sencillo de enunciar. En el momento en que se pulsa «enviar», la información sale de la red de la empresa y llega a los servidores de otra compañía, que la trata según sus propias condiciones. Esas condiciones no son las mismas para todos: dependen del proveedor y, sobre todo, del tipo de cuenta. Y cambian con frecuencia.

El caso que se cita siempre es el de Samsung. En abril de 2023, varios ingenieros de la compañía pegaron en ChatGPT código fuente interno para buscar errores y la grabación de una reunión para obtener el acta. Pocas semanas después, la compañía prohibió el uso de estas herramientas en sus equipos y redes, con el argumento de que lo enviado quedaba en servidores externos, era difícil de recuperar o borrar y podía acabar expuesto. Tres años más tarde, la mayoría de las empresas sigue sin una política equivalente, y el volumen de lo que se pega en un chat es incomparablemente mayor.

Este estudio intenta responder con datos a una pregunta práctica: **qué pasa con lo que compartimos con un asistente de IA, y qué debería hacer una empresa al respecto.**

02

Qué hemos revisado y cómo

Hemos revisado las condiciones publicadas por **OpenAI** (ChatGPT y su API), **Anthropic** (Claude y su API), **Google** (Gemini en cuentas personales, en Google Workspace y en su API) y **Microsoft** (Copilot de consumo y Microsoft Copilot para organizaciones). Las fuentes son sus políticas de privacidad, centros de ayuda y de privacidad, documentación técnica y anuncios oficiales, consultados el 2 de octubre de 2026. Para los sucesos (filtraciones, la orden judicial del caso New York Times) hemos acudido a prensa de referencia y a las comunicaciones de las propias empresas. Al final del documento se recogen todas las fuentes.

Para cada proveedor y cada tipo de cuenta nos hemos hecho cuatro preguntas:

1. **¿Entrena con lo que le das?** Es decir, si las conversaciones pueden usarse para mejorar los modelos futuros.
2. **¿Cuánto tiempo lo guarda?** Incluido lo que el usuario ya ha borrado.
3. **¿Quién puede leerlo?** Revisores humanos, equipos de seguridad, subcontratistas y, llegado el caso, un tribunal.
4. **¿Qué más hace con ello?** Publicidad, memoria entre conversaciones, enlaces compartidos.

ALCANCE

Analizamos lo que los proveedores publican, no auditamos sus sistemas. Las condiciones cambian a menudo, de modo que este estudio describe la situación a fecha de octubre de 2026. Es un documento divulgativo y no sustituye al asesoramiento jurídico de cada organización.

OpenAI: ChatGPT y su API

Cuentas personales: Free, Go, Plus y Pro

En las cuentas personales, OpenAI puede usar el contenido de las conversaciones para mejorar sus modelos. El usuario puede impedirlo desactivando el ajuste **«Mejorar el modelo para todos»** en los controles de datos, o solicitándolo en su portal de privacidad. La documentación no deja claro si ese ajuste viene activado por defecto en las cuentas nuevas, así que la recomendación práctica es comprobarlo en cada cuenta.

Las conversaciones normales y archivadas permanecen guardadas en la cuenta hasta que el usuario las borra. Una vez borradas, OpenAI las programa para su eliminación definitiva en un plazo de 30 días, salvo que ya estuvieran desidentificadas y desvinculadas de la cuenta o que la empresa deba conservarlas por motivos de seguridad o legales. Los chats temporales no se usan para entrenar, pero pueden conservarse hasta 30 días por seguridad. Con la memoria ocurre algo parecido: los registros de recuerdos borrados pueden mantenerse hasta 30 días.

En cuanto a quién accede, OpenAI reconoce que un número limitado de su personal autorizado puede ver el contenido para investigar abusos o incidentes de seguridad y para dar soporte, y que comparte contenido con un grupo de proveedores de servicios de confianza.

La novedad de 2026 es la **publicidad**. OpenAI empezó a probar anuncios en Estados Unidos el 9 de febrero y el 18 de agosto los extendió a 31 países europeos, España entre ellos. Solo se muestran en los planes Free y Go; Plus, Pro, Business, Enterprise y Edu quedan fuera. Para elegir qué anuncio mostrar, el sistema usa siempre el contexto de la conversación en curso y, si la personalización está activada, también los chats anteriores, la memoria y la interacción previa con anuncios. Según OpenAI, los anunciantes no tienen acceso a las conversaciones y solo reciben datos agregados, como el número de visualizaciones o de clics.

Cuentas de empresa y API

Para ChatGPT Business, Enterprise, Edu y la plataforma de API, la posición es la contraria: **OpenAI no usa los datos de empresa para entrenar sus modelos por defecto**. En la API esa regla rige desde el 1 de marzo de 2023, salvo que el cliente decida participar expresamente. OpenAI firma **contrato de encargo de tratamiento** (DPA) para ChatGPT Business, ChatGPT Enterprise y la API.

Las conversaciones borradas en los espacios de empresa se eliminan de sus sistemas en 30 días, salvo obligación legal, y los administradores controlan los periodos de conservación. En la API, OpenAI puede conservar entradas y salidas hasta 30 días para prestar el servicio y detectar abusos. A esos datos pueden acceder empleados autorizados (para soporte técnico, investigación de abusos y cumplimiento legal) y subcontratistas especializados, sujetos a confidencialidad, solo para revisar abusos. La retención cero existe, pero solo para clientes con un caso de uso que OpenAI considere apto. La residencia de datos en Europa está disponible para clientes de API aptos y para los nuevos clientes de Enterprise y Edu.

El precedente del caso New York Times

En 2025, dentro del pleito por derechos de autor que el New York Times mantiene contra OpenAI, un tribunal de Nueva York ordenó a la compañía **conservar los registros de conversaciones que de otro modo habría borrado**. La orden afectó a ChatGPT Free, Plus, Pro y Team y a la API sin retención cero; quedaron fuera Enterprise, Edu y los clientes con retención cero. La obligación terminó el 26 de septiembre de 2025, pero OpenAI sigue conservando, con acceso restringido a un pequeño equipo legal y de seguridad, datos de usuarios de abril a septiembre de 2025.

El caso ilustra algo que conviene tener presente con cualquier proveedor: lo que dicen sus condiciones de conservación puede quedar en suspenso por una decisión judicial en otro país, sin que el usuario pueda hacer nada.

04

Anthropic: Claude

Cuentas de consumo: Free, Pro y Max

El 28 de agosto de 2025 Anthropic cambió sus condiciones de consumo. Desde entonces, los usuarios de Claude Free, Pro y Max, incluido Claude Code desde esas cuentas, deciden si permiten que sus conversaciones se usen para mejorar los modelos; tuvieron hasta el 8 de octubre de 2025 para elegir. El ajuste se llama **«Mejora del modelo»** en la configuración de privacidad. Las conversaciones en modo incógnito no se usan para entrenar aunque el ajuste esté activado.

La elección tiene consecuencias en la conservación. Quien acepta el entrenamiento permite que sus datos se guarden **desidentificados hasta cinco años** en los procesos de entrenamiento. Quien no lo acepta mantiene el régimen anterior: las conversaciones borradas se eliminan de los sistemas de Anthropic en 30 días. Hay además plazos específicos para lo que los sistemas de seguridad marcan como posible infracción de la política de uso: las entradas y salidas se guardan hasta dos años y las puntuaciones de clasificación, hasta siete. Las valoraciones que el usuario envía voluntariamente se conservan cinco años.

En el terreno comercial, Anthropic se comprometió públicamente en febrero de 2026 a que **Claude no tenga anuncios**, con la salvedad de que, si alguna vez revisa esa postura, lo explicará.

Cuentas comerciales y API

Las condiciones de consumo no se aplican a los productos comerciales (Claude para equipos y empresas, la API, Claude para Gobierno y para Educación). En ellos, **Anthropic no usa por defecto las entradas ni las salidas para entrenar**, y el contrato de encargo de tratamiento, con cláusulas contractuales tipo, está incorporado a las condiciones comerciales.

En la API, Anthropic elimina entradas y salidas en un plazo de 30 días, con excepciones por acuerdo con el cliente, por aplicación de su política de uso o por obligación legal. La retención cero existe para algunos clientes y requiere aprobación. Aquí hay una novedad de 2026 que conviene conocer: desde el

9 de junio, para los modelos que Anthropic considera de capacidades más avanzadas, **entradas y salidas se conservan 30 días en todas las plataformas donde se ofrecen**, también para las organizaciones que tenían retención cero.

Sobre la ubicación, la API de Anthropic permite hoy elegir entre inferencia en Estados Unidos o global, y el almacenamiento de los espacios de trabajo solo está disponible en Estados Unidos. No hay opción europea en su plataforma propia; para mantener el tratamiento en Europa hay que recurrir a los grandes proveedores de nube que distribuyen sus modelos, con sus propias condiciones.

05

Google: Gemini

Cuentas personales

Google es, de los cuatro, el más explícito sobre la revisión humana. Su centro de privacidad de Gemini lo dice sin rodeos:

«No introduzcas información confidencial que no querrías que viera un revisor o que Google usara para mejorar sus servicios.»

Centro de privacidad de las aplicaciones de Gemini, consultado el 2-10-2026

Con la actividad de Gemini activada, Google puede usar las conversaciones para entrenar sus modelos, y una parte de ellas la revisan personas, en algunos casos de proveedores externos. Antes de enviarlas a revisión las desvincula de la cuenta del usuario, pero **las conversaciones revisadas se conservan hasta tres años**. La actividad se borra automáticamente a los 18 meses por defecto; el usuario puede cambiarlo a 3 o 36 meses o desactivar el borrado. Si desactiva la actividad, las conversaciones se guardan 72 horas para responderle y por seguridad, y no se usan para entrenar salvo que envíe valoraciones. No hemos encontrado condiciones de privacidad distintas para los planes personales de pago.

Google Workspace y la API de Gemini

En las ediciones de Workspace para empresas, educación y sector público, Google se compromete a que las conversaciones y los archivos subidos a Gemini **no los revisen personas ni se usen para entrenar sin permiso** del cliente. Los datos se rigen por el anexo de tratamiento de datos de su nube (CDPA). El administrador decide si la actividad se borra a los 3, 18 o 36 meses; por defecto, a los 18.

En la API, la diferencia entre lo gratuito y lo de pago es tajante. En los servicios gratuitos, Google pide literalmente que no se envíe información sensible, confidencial o personal, porque personas pueden revisar entradas y salidas. En los de pago, no usa las peticiones ni las respuestas para mejorar sus productos y solo las registra para detectar usos prohibidos.

Microsoft: Copilot

Muchas empresas españolas trabajan sobre Microsoft 365, así que conviene distinguir sus dos Copilot.

Copilot de consumo

Con una cuenta personal de Microsoft, **las conversaciones con Copilot se usan para entrenar por defecto**, salvo que el usuario lo desactive o pertenezca a alguno de los grupos excluidos (cuentas de organización, menores, usuarios sin sesión iniciada y residentes de algunos países). Microsoft guarda la actividad de conversación 18 meses por defecto, y algunas conversaciones pasan por revisión automática y humana para mejorar el producto y por seguridad. Si la personalización y los anuncios personalizados están activados, el historial de conversaciones puede usarse para personalizar la publicidad.

Microsoft Copilot para organizaciones

Con una cuenta de organización, el panorama cambia. Microsoft afirma que **las peticiones, las respuestas y los datos a los que accede a través de Microsoft Graph no se usan para entrenar los modelos fundacionales**, que las interacciones se tratan y guardan con los mismos compromisos contractuales que el resto del contenido de Microsoft 365, y que Copilot ha renunciado a la vigilancia de abusos con revisión humana que ofrece Azure OpenAI. Los administradores pueden fijar la conservación con Microsoft Purview, y, para los usuarios europeos, el tratamiento se mantiene dentro de la frontera de datos de la UE.

UN MATIZ IMPORTANTE

Microsoft Copilot permite usar modelos de Anthropic como subencargado. Según la propia Microsoft, esos modelos quedan, por ahora, fuera de la frontera de datos de la UE. Las búsquedas web que Copilot lanza en Bing tampoco están cubiertas por ella.

07

Comparativa

La tabla resume lo anterior. La conclusión que salta a la vista es que la línea divisoria no pasa entre proveedores, sino entre cuentas personales y cuentas de empresa.

	¿Entrena con tus datos?	Conservación	Revisión humana	Contrato de encargo
ChatGPT personal Free, Go, Plus, Pro	Sí, salvo que se desactive	Hasta que se borra; borrado definitivo en 30 días	Personal autorizado por abuso, seguridad o soporte	No
ChatGPT empresa y API	No, por defecto	Configurable por el administrador; API, hasta 30 días	Empleados y subcontratistas, por abuso	Sí (Business, Enterprise, API)
Claude personal Free, Pro, Max	Solo si el usuario lo acepta	Borrados, 30 días; con entrenamiento, hasta 5 años	Contenido marcado por seguridad, hasta 2 años	No
Claude empresa y API	No, por defecto	API, 30 días; retención cero con aprobación	Contenido marcado por la política de uso	Sí, incorporado
Gemini personal	Sí, con la actividad activada	18 meses por defecto; revisados, hasta 3 años	Sí, una muestra	No
Gemini en Workspace	No, sin permiso del cliente	3, 18 o 36 meses, según el administrador	No, sin permiso del cliente	Sí (CDPA)
Copilot de consumo	Sí, salvo que se desactive	18 meses por defecto	Sí, en algunas conversaciones	No
Microsoft Copilot (organización)	No	Según las políticas de la organización	No (renuncia a la vigilancia con revisión humana)	Sí (DPA de Microsoft)

Condiciones publicadas por cada proveedor, consultadas el 2 de octubre de 2026. Simplificación: el detalle y las excepciones están en los apartados 03 a 06.

08

Cuando las cosas salen mal

Las condiciones de un proveedor describen lo que hace con los datos cuando todo funciona. Los incidentes de los últimos años muestran lo que ocurre cuando no.

Lo compartido acaba en los buscadores. En el verano de 2025, conversaciones de ChatGPT que sus usuarios habían compartido con la opción «hacer este chat descubrible» empezaron a aparecer en Google, Bing, DuckDuckGo y Brave. OpenAI retiró la opción el 1 de agosto; su responsable de seguridad

reconoció que daba «demasiadas oportunidades para compartir por accidente cosas que no se pretendía». Semanas después ocurrió algo mayor con Grok, el asistente de xAI: **más de 370.000 conversaciones** compartidas mediante enlace quedaron indexadas en los buscadores, sin que sus autores lo supieran. Algunas contenían nombres, documentos, hojas de cálculo y al menos una contraseña.

Lo borrado sigue existiendo. La orden del caso New York Times obligó a conservar durante meses conversaciones que los usuarios habían eliminado. Que el proveedor tenga buena voluntad no impide que un tribunal le obligue a guardar, ni que otro le obligue después a entregar.

Lo que se pega no se recupera. El caso de Samsung no fue un ataque: fue gente haciendo su trabajo con la herramienta que tenía a mano. Es el escenario más probable en cualquier empresa, y el que menos se vigila.

09

Qué arriesga la empresa

Cuando un empleado pega en un asistente de IA información propia, el riesgo es sobre todo de confidencialidad. Cuando lo que pega son **datos personales de clientes, pacientes, empleados o proveedores**, el riesgo pasa a ser también legal, y quien responde es la organización.

Protección de datos

Según el Reglamento General de Protección de Datos, la empresa que decide para qué y cómo se tratan unos datos personales es la **responsable del tratamiento**, y solo puede confiarlos a un tercero que actúe como **encargado** mediante un contrato con las garantías del artículo 28. Una cuenta personal de un asistente de IA no ofrece ese contrato. Introducir en ella datos de clientes supone, en la práctica, comunicarlos a un tercero sin la cobertura que exige la ley, a menudo con una transferencia fuera del Espacio Económico Europeo que nadie ha evaluado. Si los datos son de salud, ideología, origen o cualquier otra categoría especial, la situación es todavía más delicada.

Las multas del RGPD tienen dos tramos. Los incumplimientos de las obligaciones del responsable y del encargado, como la falta de contrato de encargo o de medidas de seguridad, pueden llegar a **10 millones de euros o el 2 %** de la facturación mundial anual. Los que afectan a los principios del tratamiento, a su base jurídica, a los derechos de los interesados o a las transferencias internacionales pueden llegar a **20 millones de euros o el 4 %**. En ambos casos se aplica la cifra mayor.

Si esos datos quedan expuestos (por un enlace compartido que acaba en un buscador, por ejemplo), se trata de una **violación de la seguridad de los datos personales**, y la empresa tiene **72 horas** desde que la conoce para notificarla a la autoridad de control, además de informar a los afectados cuando el riesgo sea alto.

Secretos empresariales

La Ley 1/2019 de Secretos Empresariales solo protege como secreto la información que, además de ser secreta y tener valor por serlo, ha sido objeto de **medidas razonables por parte de su titular para mantenerla en secreto**. Si una empresa permite, sin ninguna política ni control, que su personal pegue planos, fórmulas, precios o estrategias en un servicio de consumo de un tercero, le costará demostrar ante un juez que tomó esas medidas. El riesgo no es solo que la información se filtre: es perder la protección legal cuando se filtre.

Compromisos con los clientes

Muchas relaciones profesionales incluyen cláusulas de confidencialidad, y algunas profesiones están sujetas a deber de secreto. Un despacho que resume un expediente en una cuenta personal de ChatGPT, o una clínica que redacta un informe con los datos de un paciente en un asistente gratuito, pueden estar incumpliendo esos compromisos aunque nadie llegue a enterarse nunca.

10

Lo que resuelven los planes de empresa, y lo que no

Los planes de empresa resuelven lo más grave. No entrenan con los datos del cliente por defecto, firman contrato de encargo, limitan la revisión humana a la vigilancia de abusos y dan a los administradores control sobre la conservación. Para trabajar con información de la organización en la nube, **son el mínimo exigible**, y cualquier empresa que hoy use cuentas personales para trabajo debería empezar por ahí.

Pero no lo resuelven todo. La información sigue saliendo de la red de la empresa y queda en manos de un proveedor, casi siempre estadounidense, sujeto a su propia legislación y a sus tribunales. Se conserva un tiempo para vigilar abusos, y la retención cero es una excepción que el proveedor concede o no. Las condiciones cambian: en 2026 Anthropic ha pasado a exigir 30 días de conservación para sus modelos más avanzados, incluso a quien tenía retención cero. Y la ubicación de los datos no siempre se puede elegir: la API propia de Anthropic no ofrece hoy alojamiento en Europa, y los modelos de Anthropic integrados en Microsoft Copilot quedan fuera de la frontera de datos de la UE.

Para la mayor parte de la información de una empresa, eso es aceptable. Para una parte, no.

11

La alternativa: que el dato no salga de casa

Hasta hace poco, la única forma de usar un modelo de lenguaje competente era enviar los datos a la nube de quien lo había entrenado. Eso ha cambiado. Hoy existen **modelos abiertos** de calidad que cualquier organización puede descargar y ejecutar en su propia infraestructura. El ejemplo más llamativo lo dio la propia OpenAI, que en agosto de 2025 publicó gpt-oss-120b y gpt-oss-20b con

licencia Apache 2.0, que permite su uso comercial. El mayor de los dos, según OpenAI, se acerca en razonamiento a uno de sus modelos comerciales de entonces y cabe en una sola tarjeta gráfica de 80 GB.

El hardware también ha bajado al escritorio. Existen ya equipos de sobremesa con **128 GB de memoria unificada** que, según su fabricante, permiten ejecutar modelos de hasta 200.000 millones de parámetros. No sustituyen a un centro de datos, pero dan para que un departamento o una pequeña organización tenga su propio asistente, su buscador documental y sus agentes sin que un solo dato salga de su red.

Con un modelo local desaparecen de golpe casi todas las preguntas de este estudio. Nadie entrena con los datos, nadie los revisa, no hay plazos de conservación ajenos, ni anuncios, ni órdenes judiciales dirigidas a un tercero. La trazabilidad de quién preguntó qué y con qué documentos queda dentro de la organización.

Lo que un modelo local no resuelve por sí solo

Sería un error presentarlo como una solución mágica. Un modelo local exige una inversión inicial en equipos, una puesta en marcha y un mantenimiento continuo: actualizar modelos, aplicar parches, vigilar el rendimiento. En las tareas más complejas, los mejores modelos de la nube siguen por delante. Y, sobre todo, **un modelo en casa no es seguro por defecto**: necesita control de acceso, cifrado, registros de actividad y la misma protección frente a instrucciones maliciosas escondidas en documentos que cualquier otro sistema de IA. Traer la IA dentro de la organización traslada la responsabilidad de la seguridad al propio equipo, que tiene que estar preparado para asumirla.

12

Cada dato, donde le corresponde

La respuesta, por tanto, no es «todo a la nube» ni «todo en local». En NARSIL Intelligence defendemos una **arquitectura por criticidad**: clasificar la información de la organización y llevar cada nivel a la herramienta que le corresponde.

CRÍTICO Datos personales de clientes, pacientes o empleados; expedientes; secretos industriales; estrategia. Modelo local, en la infraestructura propia.	INTERNO Documentación de trabajo, procedimientos y comunicaciones sin datos personales ni secretos. Nube con plan de empresa y contrato de encargo.	PÚBLICO Información ya publicada o sin valor reservado: búsquedas, borradores de comunicación externa. Cualquier herramienta, con sentido común.
---	--	---

Llevado a casos concretos: un despacho de abogados puede usar un asistente en la nube con plan de empresa para revisar el estilo de un contrato tipo, pero los expedientes de sus clientes deberían consultarse con un modelo local. Una clínica puede apoyarse en la nube para redactar la comunicación

de su web, pero no para resumir historias clínicas. Una empresa industrial puede usar la nube para su documentación comercial y reservar el modelo local para sus planos y su know-how.

El paso que casi todas las organizaciones se saltan es el primero: **clasificar la información antes de elegir la herramienta**. Sin esa clasificación, cualquier decisión tecnológica es una apuesta.

13

Diez medidas para empezar mañana

1. **Averiguar qué se está usando.** Preguntar a los equipos qué asistentes de IA usan, con qué cuentas y para qué. Suele haber sorpresas.
2. **Prohibir por escrito los datos de clientes en cuentas personales**, sean gratuitas o de pago, y explicar por qué.
3. **Contratar un plan de empresa** del proveedor que se vaya a usar en la nube y firmar su contrato de encargo de tratamiento.
4. **Revisar la configuración de cada herramienta:** entrenamiento desactivado, conservación acotada, memoria y enlaces compartidos bajo control.
5. **Clasificar la información** en, al menos, tres niveles: crítica, interna y pública.
6. **Llevar lo crítico a un entorno propio**, con un modelo local, y documentar quién accede y para qué.
7. **Desactivar o vigilar los enlaces compartidos**, que son la vía de exposición más tonta y más frecuente.
8. **Formar al personal** en lo que puede y no puede pegar en un chat, con ejemplos de su propio trabajo.
9. **Revisar contratos y compromisos de confidencialidad** con clientes para comprobar que el uso de IA es compatible con ellos.
10. **Volver a mirar las condiciones cada seis meses.** Como demuestra este estudio, cambian.

14

Conclusión

Los asistentes de IA han llegado a las empresas por la puerta de atrás: los trajo cada empleado, en su cuenta, para hacer mejor su trabajo. Esa forma de llegar explica por qué tantas organizaciones tratan con más cuidado una memoria USB que lo que su personal pega cada día en un chat.

Las condiciones de los proveedores dejan claro que la diferencia decisiva está entre las cuentas personales y las de empresa, y que ni siquiera las segundas garantizan que la información no salga. Para la información que no puede salir, existe hoy una alternativa real: ejecutar la IA dentro de la organización. El trabajo consiste en saber qué información es cuál y en construir, para cada nivel, el sistema adecuado.

Ese es el trabajo que hacemos en NARSIL Intelligence. Con este estudio abrimos una serie con la que queremos contribuir a que las organizaciones adopten la inteligencia artificial con criterio: aprovechándola al máximo y sabiendo, en cada momento, dónde está su información.



NARSIL INTELLIGENCE

Diseñamos, construimos e implantamos sistemas de inteligencia artificial en la infraestructura de cada organización, y formamos a los equipos que los usan.

[NARSILINTELLIGENCE.COM](https://narsilintelligence.com)

Anexo

Fuentes

Todas las páginas se consultaron el 2 de octubre de 2026, salvo las noticias, fechadas en su publicación.

1. OpenAI. *Enterprise privacy at OpenAI* (actualizada el 8-1-2026). openai.com/enterprise-privacy
2. OpenAI. *Data Controls FAQ*. help.openai.com/en/articles/7730893-data-controls-faq
3. OpenAI. *How OpenAI handles data in consumer services*. help.openai.com/en/articles/7039943
4. OpenAI. *Chat and file retention policies in ChatGPT*. help.openai.com/en/articles/8983778
5. OpenAI. *Memory FAQ*. help.openai.com/en/articles/8590148-memory-faq
6. OpenAI. *Your data* (documentación de la API). developers.openai.com/api/docs/guides/your-data
7. OpenAI. *Data residency and inference residency for ChatGPT*. help.openai.com/en/articles/9903489
8. OpenAI. *Ads in ChatGPT*. help.openai.com/en/articles/20001047-ads-in-chatgpt
9. OpenAI. *ChatGPT ads expands across Europe* (18-8-2026). openai.com/index/chatgpt-ads-expands-across-europe
10. OpenAI. *How we're responding to The New York Times' data demands* (actualizada el 22-10-2025). openai.com/index/response-to-nyt-data-demands
11. Anthropic. *Updates to our consumer terms* (28-8-2025). anthropic.com/news/updates-to-our-consumer-terms
12. Anthropic. *How long do you store my data?* privacy.claude.com/en/articles/10023548
13. Anthropic. *Is my data used for model training?* privacy.claude.com/en/articles/10023580 y [7996868](https://privacy.claude.com/en/articles/7996868)
14. Anthropic. *How long do you store my organization's data?* privacy.claude.com/en/articles/7996866
15. Anthropic. *Data retention practices for covered models* (en vigor desde el 9-6-2026). privacy.claude.com/en/articles/15425996
16. Anthropic. *Zero data retention*. privacy.claude.com/en/articles/8956058
17. Anthropic. *Data Processing Addendum*. privacy.claude.com/en/articles/7996862
18. Anthropic. *Data residency* (documentación de la API). platform.claude.com/docs/en/manage-claude/data-residency
19. Anthropic. *Claude is a space to think* (4-2-2026). anthropic.com/news/claude-is-a-space-to-think
20. Google. *Gemini Apps Privacy Hub*. support.google.com/gemini/answer/13594961
21. Google. *Generative AI in Google Workspace Privacy Hub*. knowledge.workspace.google.com/admin/generative-ai/generative-ai-in-google-workspace-privacy-hub
22. Google. *Gemini API Additional Terms of Service* (modificadas el 28-4-2026). ai.google.dev/gemini-api/terms
23. Microsoft. *Data, Privacy, and Security for Microsoft Copilot*. learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy
24. Microsoft. *Enterprise data protection in Microsoft Copilot*. learn.microsoft.com/en-us/copilot/microsoft-365/enterprise-data-protection
25. Microsoft. *Privacy FAQ for Microsoft Copilot*. support.microsoft.com/en-us/microsoft-copilot/privacy-faq-for-microsoft-copilot
26. Bloomberg. *Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak* (2-5-2023).
27. The Register. *OpenAI removes ChatGPT self-doxing option* (1-8-2025).
28. Forbes. *Elon Musk's xAI Published Hundreds Of Thousands Of Grok Chatbot Conversations* (20-8-2025); Fortune (22-8-2025).
29. OpenAI. *gpt-oss-120b & gpt-oss-20b Model Card* (5-8-2025). arxiv.org/abs/2508.10925
30. NVIDIA. *DGX Spark*, especificaciones. nvidia.com/en-us/products/workstations/dgx-spark
31. Reglamento (UE) 2016/679, General de Protección de Datos, artículos 4, 9, 28, 33, 44 y 83.
32. Ley 1/2019, de 20 de febrero, de Secretos Empresariales, artículo 1. boe.es/buscar/act.php?id=B0E-A-2019-2364