
Guía de los asistentes de IA

La versión siempre actualizada, con búsqueda dentro del texto, está en el sitio web.

EN ESTA GUÍA

- | | |
|-------------------------------------|---|
| 01 Qué es | 09 Claude en la web |
| 02 Qué puede hacer | 10 Cambiar de opinión |
| 03 Primera conexión | 11 «Visible para» |
| 04 Claude Code | 12 El administrador |
| 05 Cursor | 13 Seguridad |
| 06 Claude Desktop | 14 Preguntas frecuentes |
| 07 Codex | 15 Si no funciona |
| 08 ChatGPT | |

01 Qué es un asistente conectado

Para que un asistente de IA (Claude, ChatGPT, Cursor, Codex) lea un documento, normalmente se descarga y se vuelve a subir al chat: una copia más que circula por su cuenta, sin versiones, sin permisos, sin que quede constancia de quién ha leído qué.

Con **Asistentes de IA** conectas el asistente a Flow una sola vez y, a partir de ahí, trabaja con los documentos donde ya están. Tres principios sostienen todo lo demás:

1. **Tú eliges las carpetas.** Una conexión abre solo las carpetas que indicas. Fuera de ellas, para el asistente no existe nada: no puede abrirlas, buscarlas, ni siquiera saber que existen.
2. **La empresa decide qué se puede abrir.** En los espacios de equipo es el administrador quien establece, carpeta por carpeta, qué se puede abrir y si en lectura o también en escritura. Tú eliges dentro de esa lista: puedes reducirla, nunca ampliarla.

3. **De entrada, solo lee.** Una conexión nueva está en **Solo lectura**. Puede modificar solo si tú lo eliges y solo donde el administrador lo ha permitido, y nada es definitivo: quedan la papelera y las versiones.

En tu **espacio personal** decides tú, sin pasar por el administrador.

Las conexiones se crean y se gestionan en **Cuenta → Asistentes de IA**.

Asistentes de IA depende del plan, y hoy se activa bajo petición: si en tu Cuenta no encuentras la opción, escríbenos. También es necesario que el plan lea el texto de los documentos (la misma lectura que alimenta la búsqueda en los contenidos); de lo contrario, el asistente encontraría los nombres de los archivos y no lo que hay dentro. Donde el plan no llega, el asistente lo dice: no inventa.

02 Qué puede hacer y qué no

Dentro de las carpetas que le has abierto, un asistente conectado **siempre puede leer**:

- lista el contenido de una carpeta y las propiedades de un archivo: tamaño, fechas, versión, etiquetas;
- **lee el texto** de PDF, documentos de Office e imágenes con texto. Es el texto que Flow ya ha extraído para la búsqueda, así que no hay conversiones que hacer ni límites de tamaño del archivo;
- **busca** por nombre y dentro del contenido, con filtros por carpeta, tipo y fecha;
- ve las versiones de un archivo y lo que se ha añadido, modificado o eliminado recientemente;
- ve el espacio usado y la cuota de la empresa;
- obtiene un enlace temporal, válido durante una hora, para descargar un archivo tal cual;
- ve los enlaces para compartir y de depósito que **tú** has creado en esas carpetas, no los de los compañeros.

Si la conexión es «Puede modificar», y solo en las carpetas que el administrador ha puesto en Escritura (o en tu espacio personal), también puede: crear carpetas, crear archivos de texto de hasta 5 MB, copiar, mover, renombrar, enviar a la papelera (pidiéndote confirmación) y devolver un archivo a una versión anterior.

Si un nombre ya existe, no lo sobrescribe: solo lo hace si se lo pides, y la versión antigua se conserva de todos modos en las versiones.

Lo que no hace, ni aunque se lo pidas:

- salir de las carpetas que le has abierto: esto no ocurrirá nunca, en ningún caso;
- crear enlaces para compartir o de depósito: es el único gesto con el que un error haría salir documentos de la empresa, y de momento queda fuera;
- eliminar de forma definitiva: todo pasa por la papelera;
- mover, renombrar o enviar a la papelera las propias carpetas que le has abierto;
- tocar un archivo que un compañero tiene en edición exclusiva;
- ver Datos protegidos, firmas, tasks y repositorios Git: ve archivos y carpetas, nada más.

Si un archivo no tiene texto legible (un archivo comprimido, un formato que no conoce), te lo dice. No inventa.

03 La primera conexión

Cuenta → Asistentes de IA → «Nueva conexión». Cuatro opciones:

1. **Nombre:** te sirve a ti, para reconocerla dentro de seis meses: «Claude en el proyecto Dainese» dice más que «Claude».
2. **Qué puede hacer:** **Solo lectura**, ya seleccionada, o bien **Puede modificar**. En caso de duda, deja la primera: se cambia cuando quieras, sin rehacer nada.
3. **Caducidad:** nunca, 30 días, 90 días, 1 año. Para una consultoría que termina, una caducidad es más cómoda que un recordatorio.
4. **Carpetas abiertas:** el árbol en columnas, el mismo de la sincronización selectiva. Marcas una o varias carpetas, también en espacios distintos.

Para las carpetas vale una sola regla, y conviene tenerla presente: **marcar una carpeta abre todo lo que contiene**. No se puede excluir una parte de dentro: si una subcarpeta no debe verse, marcas sus carpetas hermanas y no la carpeta madre.

En los espacios de equipo, lo que el administrador no ha abierto lleva un **candado** («No se puede abrir a los asistentes: lo decide el administrador») y las carpetas en las que un asistente también podrá escribir llevan un **lápiz**. En tu espacio personal marcas lo que quieras.

Encima de las carpetas siempre queda escrito: *«Los documentos que lee el asistente se envían al proveedor de ese asistente (Anthropic, OpenAI...). Abre solo las carpetas necesarias.»* Es el motivo por el que conviene abrir poco.

Al confirmar aparecen la **clave de acceso**, la **dirección del servidor** y un bloque listo para copiar para cada asistente.

La clave se muestra una sola vez. Cópiala ahora: después nadie puede recuperarla, ni siquiera nosotros. Si la pierdes, no pasa nada: revocas la conexión y creas otra en un minuto.

04 Conectar Claude Code

Claude Code se conecta desde el **terminal**. En la página de la conexión, bajo «Cómo conectarlo», el primer bloque ya está listo con tu clave dentro: se copia y se pega en el terminal tal cual.

Después, dentro de Claude Code, el comando `/mcp` lista los servidores conectados: entre ellos debe aparecer **flow**. A partir de ese momento puedes preguntar «¿qué ves en Flow?» y el asistente responde con las carpetas que le has abierto.

MCP es el estándar con el que los asistentes se conectan a una fuente de datos. Lo mencionamos porque es la palabra que encontrarás escrita en los ajustes de los asistentes.

Copia el bloque que te da Flow, no un ejemplo leído en otro sitio: el de Flow ya contiene la clave real. Un bloque con el marcador de posición en lugar de la clave se instala igualmente, y luego el asistente responde que no sabe nada de Flow.

05 Conectar Cursor

En Cursor, el bloque listo va en uno de estos dos sitios, a elegir:

- **Settings → MCP → Add server;**

- o bien el archivo `.cursor/mcp.json` del proyecto, si prefieres que la conexión se quede junto al proyecto.

El bloque que hay que pegar es el segundo de los que te muestra la página de la conexión, y ya contiene la clave. Después de guardarlo, Cursor muestra **flow** entre los servidores disponibles.

Vale el aviso de siempre: copia el bloque que te da Flow, no un ejemplo encontrado en otro sitio: un marcador de posición en lugar de la clave pasa desapercibido y luego el asistente no encuentra nada.

06 Conectar Claude Desktop

Claude Desktop guarda las conexiones en un archivo de configuración. Se llega a él desde la app: **Settings → Developer → Edit Config**, que abre `claude_desktop_config.json`.

Dentro de ese archivo se pega el bloque que la página de la conexión indica para Claude Desktop, y luego **se reinicia Claude Desktop**: las conexiones las lee al arrancar.

No tienes que instalar nada en Flow. Claude Desktop, para comunicarse con la clave, usa un pequeño puente que se descarga solo la primera vez: si la primera respuesta tarda unos segundos, es por eso.

07 Conectar Codex

En Codex, el bloque va en el archivo `~/.codex/config.toml`. Desde la app llegas con **Settings → Configuration**; desde el terminal también existe el comando `codex mcp add`.

Una vez guardado el archivo, **reinicia Codex**. En el chat, `/mcp` lista los servidores conectados: entre ellos, **flow**.

Dos avisos, los dos aprendidos a base de errores:

- la opción **«Connections»** de los ajustes de Codex es otra cosa (el control remoto del ordenador) y no tiene que ver con los asistentes conectados a Flow;

- si pegas un bloque de ejemplo dejando el marcador de posición en lugar de la clave, Codex muestra igualmente **«Authenticated»**, pero luego el asistente responde que no tiene herramientas de Flow. El bloque correcto es el que te da la página de la conexión, con la clave ya dentro.

08 Conectar ChatGPT

ChatGPT sigue otro camino: **no hay clave que copiar**. Solo le das la dirección de tu Flow; ChatGPT abre una página de Flow donde entras, eliges las carpetas y confirmas. La conexión aparece sola en Cuenta → Asistentes de IA, con el nombre del asistente, y desde ahí se gestiona como todas las demás.

El recorrido, dentro de ChatGPT:

1. **Settings → Security and access**, al final, **Developer mode**: actívalo. ChatGPT lo señala como «riesgo elevado»: es el aviso que muestra a cualquiera que añada un servidor propio, y sirve para eso.
2. **Settings → Plugins → Browse plugins**.
3. Arriba a la derecha, el botón **+**, que abre el formulario «New plugin».
4. Nombre **Flow**; en la URL, la dirección de tu Flow seguida de `/mcp`, por ejemplo `https://flow.kaigrid.ai/mcp`; autenticación **OAuth**; marca «I understand and want to continue»; **Create**.
5. **Sign in with Flow**: se abre la página de Flow «... pide acceso a Flow», donde eliges entre Solo lectura y Puede modificar, marcas las carpetas y lees el aviso sobre los datos. **Permitir** (o **No permitir**, y no ocurre nada).
6. En un chat nuevo elige Flow entre los plugins y prueba: «¿qué ves en Flow?».

En la página de consentimiento, en los espacios de equipo ves **solo** las carpetas que el administrador ha abierto: sin candados, sin una lista que descifrar.

ChatGPT cambia a menudo los nombres de sus opciones: hasta hace poco los plugins se llamaban conectores. Si una opción ya no se llama así, búscala por lo que hace.

09 Conectar Claude en la web

Claude en la web sigue el mismo camino que ChatGPT: **no hay clave que copiar**. Le das la dirección de tu Flow; Claude abre una página de Flow donde entras,

eliges las carpetas y confirmas.

En Claude: **Settings** → **Connectors** → «**Add custom connector**», y como dirección, la dirección de tu Flow seguida de `/mcp`, por ejemplo `https://flow.kaigrid.ai/mcp`.

A partir de ahí es idéntico: se abre la página «... pide acceso a Flow», donde eliges entre Solo lectura y Puede modificar, marcas las carpetas y lees el aviso sobre los datos. Al confirmar, la conexión aparece sola en **Cuenta** → **Asistentes de IA**, con el nombre del asistente, y se gestiona como todas las demás: cambias las carpetas, cambias lo que puede hacer, revocas.

Aquí vale lo mismo que para ChatGPT: en los espacios de equipo, en la página de consentimiento, ves **solo** las carpetas que el administrador ha abierto.

10 Cambiar de opinión

Nada de lo que has elegido es para siempre, y **nunca hay que rehacer la clave**.

- **Las carpetas:** desde Cuenta → Asistentes de IA abres la conexión y cambias las marcas. Las nuevas carpetas valen desde la siguiente petición del asistente, y en el asistente no tienes que tocar nada.
- **Qué puede hacer:** se pasa de Solo lectura a «Puede modificar» y viceversa de la misma manera.
- **Revocar:** el asistente deja de ver Flow **al instante**. Se usa cuando un proyecto termina, cuando se pierde un ordenador o, simplemente, cuando has terminado.

La página indica, para cada conexión, cuándo la creaste, **el último uso** y la caducidad: si nadie usa una desde hace meses, se ve.

Si el asistente intenta hacer algo que la conexión no permite (una modificación con una conexión en solo lectura, o en una carpeta donde el administrador no ha puesto Escritura), recibe un rechazo que explica qué falta, y te lo comunica en lugar de fallar en silencio.

11 Quien trabaja en la carpeta lo sabe

Una carpeta abierta a un asistente no es un asunto privado de quien ha creado la conexión: quien trabaja en ella tiene que poder saberlo.

Por eso, junto al nombre de las carpetas y de los archivos que ve un asistente, hay un **pequeño icono**; al pasar el ratón por encima indica a qué conexión. En el panel de información del archivo, lo mismo aparece escrito completo: **«Visible para: Claude en el proyecto Dainese»**. Lo ven todas las personas que trabajan ahí, no solo tú.

En el **registro de actividad** queda constancia de todo: cuándo se crea una conexión, cuándo cambian sus carpetas, cuándo se revoca, **cada lectura de contenido** (qué conexión, qué archivo, cuándo), cada enlace de descarga y cada modificación. El registro de los asistentes siempre está activo.

Lo que el registro **no** contiene es la conversación: el administrador ve qué archivos ha leído el asistente, no qué le has pedido.

12 Qué decide el administrador

En los espacios de equipo es la empresa quien establece qué se puede abrir a un asistente. El administrador lo hace en **Consola de administración → Asistentes de IA**, con «Editar la lista»: el mismo árbol en columnas, donde cada espacio y cada carpeta tiene una casilla con **tres estados**, que se recorren con un clic.

- **No** (casilla vacía): los asistentes no la ven. Es el estado inicial de todo: una empresa que no abre nada no expone nada.
- **Lectura** (el ojo): los asistentes pueden leerla.
- **Escritura** (el lápiz): también pueden modificarla, si la conexión es «Puede modificar».

El estado vale para todo lo que contiene la carpeta, y una subcarpeta puede tener uno **distinto**: siempre gana el más cercano. El espacio «Clientes» en Lectura puede tener dentro «Borradores» en Escritura; una carpeta en Escritura puede tener dentro «Contratos» en solo Lectura. Las subcarpetas muestran atenuado el nivel que heredan: un clic lo cambia solo ahí, otro lo devuelve a como estaba.

Hay una cosa que no se puede hacer: **volver a poner «No» dentro de una carpeta abierta**. Sin huecos invisibles: si una subcarpeta no debe verse, se abren sus carpetas hermanas y no la carpeta madre.

Los **espacios personales** no están en esa lista: los decide cada usuario.

Quitar o bajar una entrada **vale al instante**, también para las conexiones que ya existen. Para que no sea una sorpresa, junto a cada entrada la página indica cuántas conexiones la están usando. En la misma página está la lista de las **conexiones de la empresa**: de quién son, sobre qué carpetas, el último uso.

13 Seguridad y confidencialidad

Los documentos leídos salen hacia el proveedor del asistente. Cuando el asistente lee un archivo, ese texto llega a quien proporciona el asistente (Anthropic, OpenAI u otros), con el contrato que tú o tu empresa tenéis con ese proveedor. Flow no envía nada por iniciativa propia: envía lo que el asistente pide, dentro de las carpetas que le has abierto. Es el motivo por el que conviene abrir pocas carpetas y elegir las bien.

Un documento puede contener instrucciones dirigidas al asistente: líneas escritas a propósito para que las lea y las ejecute. Vale para cualquier asistente, y Flow pone cuatro defensas: de entrada, la conexión solo lee; el texto llega al asistente marcado como contenido de un documento, no como una orden; el asistente no puede crear enlaces hacia el exterior; y todo lo que modifica se deshace desde la papelera y las versiones.

Una clave perdida se revoca en un clic, y la conexión puede tener una caducidad desde el principio. La página muestra el último uso de cada una.

Un asistente nunca ve más que tú. La conexión vive dentro de tus permisos: si te quitan un espacio, tus conexiones lo pierden en ese mismo instante. Y vale solo para los asistentes: con esa clave no se entra en el resto de Flow.

14 Preguntas frecuentes

¿El asistente ve todos mis archivos? No: solo las carpetas que has marcado en la conexión.

¿Un compañero puede abrir a un asistente una carpeta reservada? Solo si esa carpeta ya la ve él, y solo si el administrador la ha hecho abrible.

¿Puedo cambiar de opinión después? Sí: cambias las carpetas o revocas cuando quieras, y vale al instante. La clave sigue siendo la misma.

¿El asistente puede eliminar mis archivos? Solo si has elegido «Puede modificar» y solo donde el administrador ha puesto Escritura. E incluso entonces van a la papelera, desde donde se restauran.

¿Cómo sé si una carpeta está abierta a un asistente? Tiene un pequeño icono junto al nombre, y el panel de información del archivo indica «Visible para», con el nombre de la conexión.

He perdido la clave. No se puede recuperar: revoca la conexión y crea una nueva.

¿Funciona con ChatGPT? Sí, desde la web. Y con Claude Code, Claude Desktop, Cursor y Codex.

¿Hay que instalar algo? En Flow no, nada. Claude Desktop usa un pequeño puente que se descarga solo en el primer arranque.

¿El administrador ve lo que le pregunto al asistente? No. Ve qué archivos ha leído o modificado el asistente, no la conversación.

15 Si algo no funciona

El asistente dice que no tiene herramientas de Flow, o no sabe qué es. Casi siempre es el bloque pegado a mano, con el marcador de posición en lugar de la clave. Algunos asistentes, en ese caso, muestran igualmente «Authenticated». Vuelve a copiar el bloque desde la página de la conexión, que ya contiene la clave, y reinicia el asistente.

El asistente no ve una carpeta que había marcado. Revisa la conexión en Cuenta → Asistentes de IA: si esa carpeta tiene un **candado**, el administrador la ha cerrado a los asistentes, y el cierre vale al instante, también para las conexiones ya creadas.

Dice que no puede modificar. O la conexión está en **Solo lectura**, y la cambias desde su ficha, o esa carpeta no tiene el **lápiz**: en los espacios de equipo es el administrador quien lo pone.

La conexión ha caducado. Las caducidades son las que elegiste tú al crearla. Una conexión caducada no se prolonga: se crea otra.

ChatGPT no ve las funciones nuevas. ChatGPT guarda en memoria la lista de operaciones del momento en que creaste el plugin, y no la vuelve a leer por sí



solo. Abre la ficha del plugin Flow y pulsa **Actualizar**; si no aparece, elimina el plugin y vuelve a crearlo. Después abre un **chat nuevo**. Los permisos, en cambio, siempre valen al instante, tenga ChatGPT lo que tenga en memoria.

He revocado por error. No se puede restaurar: se crea una conexión nueva y se repite el proceso en el asistente. Se tarda un minuto.