

Guia dos assistentes de IA

A versão sempre atualizada, com pesquisa dentro do texto, está no site.

NESTE GUIA

- | | |
|-------------------------------------|---|
| 01 O que é | 09 Claude na web |
| 02 O que pode fazer | 10 Mudar de ideias |
| 03 Primeira ligação | 11 «Visível para» |
| 04 Claude Code | 12 O administrador |
| 05 Cursor | 13 Segurança |
| 06 Claude Desktop | 14 Perguntas frequentes |
| 07 Codex | 15 Se não funcionar |
| 08 ChatGPT | |

01 O que é um assistente ligado

Para um assistente de IA (Claude, ChatGPT, Cursor, Codex) ler um documento, normalmente transfere-se o documento e volta a carregar-se no chat: mais uma cópia que circula por conta própria, sem versões, sem permissões, sem que fique registo de quem leu o quê.

Com **Assistentes de IA** ligas o assistente ao Flow uma única vez, e a partir daí trabalha nos documentos onde já estão. Três princípios sustentam tudo o resto:

1. **Escolhes tu as pastas.** Uma ligação abre só as pastas que indicas. Fora delas, para o assistente não existe nada: não as pode abrir, pesquisar, nem sequer saber que existem.
2. **A empresa decide o que pode ser aberto.** Nos espaços de equipa é o administrador que estabelece, pasta a pasta, o que se pode abrir e se em leitura ou também em escrita. Tu escolhes dentro dessa lista: podes restringi-la, nunca alargá-la.
3. **À partida só lê.** Uma ligação nova está em **Só leitura**. Só pode modificar se tu o escolheres e só onde o administrador o permitiu. E nada é definitivo:

continuam a existir a reciclagem e as versões.

No teu **espaço pessoal** decides sozinho, sem passar pelo administrador.

As ligações criam-se e gerem-se em **Conta → Assistentes de IA**.

Assistentes de IA depende do plano, e atualmente é ativado a pedido: se na tua Conta não encontras a opção, escreve-nos. É também necessário que o plano leia o texto dos documentos (a mesma leitura que alimenta a pesquisa nos conteúdos), caso contrário o assistente encontraria os nomes dos ficheiros e não o que está lá dentro. Onde o plano não chega, o assistente di-lo: não inventa.

02 O que pode fazer, e o que não pode

Dentro das pastas que lhe abriste, um assistente ligado **lê sempre**:

- lista o conteúdo de uma pasta e as propriedades de um ficheiro: tamanho, datas, versão, etiquetas;
- **lê o texto** de PDF, documentos Office e imagens com texto. É o texto que o Flow já extraiu para a pesquisa, por isso não há conversões a fazer nem limites de tamanho do ficheiro;
- **pesquisa** por nome e dentro do conteúdo, com filtros por pasta, tipo e data;
- vê as versões de um ficheiro e o que foi adicionado, modificado ou eliminado recentemente;
- vê o espaço usado e a quota da empresa;
- obtém uma ligação temporária, válida durante uma hora, para transferir um ficheiro tal como está;
- vê as ligações de partilha e de depósito que **tu** criaste nessas pastas, não as dos colegas.

Se a ligação estiver em «Pode modificar», e só nas pastas que o administrador colocou em Escrita (ou no teu espaço pessoal), faz também: criar pastas, criar ficheiros de texto até 5 MB, copiar, mover, mudar o nome, enviar para a reciclagem (pedindo-te confirmação) e repor um ficheiro numa versão anterior. Se um nome já existir não o substitui: só o faz se lho pedires, e a versão antiga fica de qualquer forma nas versões.

O que não faz, nem que lho peças:

- sair das pastas que lhe abriste: isto nunca acontecerá, em caso algum;
- criar ligações de partilha ou de depósito: é o único gesto com que um erro faria sair documentos da empresa, e por agora fica de fora;
- eliminar de forma definitiva: tudo passa pela reciclagem;
- mover, mudar o nome ou enviar para a reciclagem as próprias pastas que lhe abriste;
- mexer num ficheiro que um colega tem em edição exclusiva;
- ver Dados protegidos, assinaturas, tasks e repositórios Git: vê ficheiros e pastas, e mais nada.

Se um ficheiro não tiver texto legível (um arquivo comprimido, um formato que não conhece), diz-to. Não inventa.

03 A primeira ligação

Conta → Assistentes de IA → «Nova ligação». Quatro escolhas:

1. **Nome:** serve-te a ti, para a reconheceres daqui a seis meses. «Claude no projeto Dainese» diz mais do que «Claude».
2. **O que pode fazer:** **Só leitura**, já selecionado, ou **Pode modificar**. Na dúvida deixa a primeira: muda-se quando quiseres, sem refazer nada.
3. **Validade:** nunca, 30 dias, 90 dias, 1 ano. Para uma consultoria que termina, uma validade é mais cómoda do que um lembrete.
4. **Pastas abertas:** a árvore em colunas, a mesma da sincronização seletiva. Marcas uma ou mais pastas, mesmo em espaços diferentes.

Nas pastas vale uma única regra, e convém tê-la presente: **marcar uma pasta abre tudo o que contém**. Não se retira uma parte lá de dentro: se uma subpasta não deve ser vista, marcas as pastas irmãs e não a pasta mãe.

Nos espaços de equipa, o que o administrador não abriu tem um **cadeado** («Não pode ser aberta aos assistentes: decidido pelo administrador»), e as pastas em que um assistente também poderá escrever têm um **lápiz**. No teu espaço pessoal marcas o que quiseres.

Por cima das pastas fica sempre escrito: *«Os documentos que o assistente lê são enviados ao fornecedor desse assistente (Anthropic, OpenAI...). Abre só as pastas necessárias.»* É o motivo pelo qual convém abrir pouco.

Ao confirmar aparecem a **chave de acesso**, o **endereço do servidor** e um bloco pronto a copiar para cada assistente.

A chave só se vê uma vez. Copia-a agora: depois já não pode ser recuperada por ninguém, nem por nós. Se a perderes não é grave: revogas a ligação e crias outra num minuto.

04 Ligar o Claude Code

O Claude Code liga-se a partir do **terminal**. Na página da ligação, em «Como ligar», o primeiro bloco já está pronto com a tua chave lá dentro: copia-se e cola-se no terminal tal como está.

Depois, dentro do Claude Code, o comando `/mcp` lista os servidores ligados: entre eles deve aparecer **flow**. A partir desse momento podes perguntar «o que vês no Flow?» e o assistente responde com as pastas que lhe abriste.

MCP é o padrão com que os assistentes se ligam a uma fonte de dados. Referimo-lo porque é a palavra que vais encontrar escrita nas definições dos assistentes.

Copia o bloco que o Flow te dá, não um exemplo lido noutro sítio: o do Flow já contém a chave verdadeira. Um bloco com o marcador de posição no lugar da chave instala-se na mesma, e depois o assistente responde que não sabe nada do Flow.

05 Ligar o Cursor

No Cursor o bloco pronto vai para um destes dois sítios, à escolha:

- **Settings → MCP → Add new MCP server;**
- ou o ficheiro `.cursor/mcp.json` do projeto, se preferires que a ligação fique junto com o projeto.

O bloco a colar é o segundo dos que a página da ligação te mostra, e já contém a chave. Depois de o guardares, o Cursor mostra **flow** entre os servidores disponíveis.

Vale o aviso de sempre: copia o bloco que o Flow te dá, não um exemplo encontrado noutro sítio: um marcador de posição no lugar da chave passa

despercebido e depois o assistente não encontra nada.

06 Ligar o Claude Desktop

O Claude Desktop guarda as ligações num ficheiro de configuração. Chega-se lá a partir da app: **Settings** → **Developer** → **Edit Config**, que abre

`claude_desktop_config.json`.

Nesse ficheiro cola-se o bloco que a página da ligação indica para o Claude Desktop, e depois **reinicia-se o Claude Desktop**: as ligações são lidas no arranque.

Não precisas de instalar nada no Flow. O Claude Desktop, para comunicar com a chave, usa uma pequena ponte que se transfere sozinha da primeira vez: se a primeira resposta demorar alguns segundos, é por isso.

07 Ligar o Codex

No Codex o bloco vai para o ficheiro `~/.codex/config.toml`. Na app chegas lá com **Settings** → **Configuration**; no terminal existe também o comando `codex mcp add`.

Depois de guardares o ficheiro, **reinicia o Codex**. No chat, `/mcp` lista os servidores ligados: entre eles **flow**.

Dois avisos, ambos aprendidos à custa de erros:

- a opção «**Connections**» das definições do Codex é outra coisa (o controlo remoto do computador) e não tem nada a ver com os assistentes ligados ao Flow;
- se colares um bloco de exemplo deixando o marcador de posição no lugar da chave, o Codex escreve na mesma «**Authenticated**», mas depois o assistente responde que não tem ferramentas do Flow. O bloco certo é o que te dá a página da ligação, com a chave já lá dentro.

08 Ligar o ChatGPT

O ChatGPT segue outro caminho: **nenhuma chave a copiar**. Dás-lhe apenas o endereço do teu Flow e o ChatGPT abre uma página do Flow onde entras,

escolhes as pastas e confirmas. A ligação aparece sozinha em Conta → Assistentes de IA, com o nome do assistente, e a partir daí gere-se como todas as outras.

O percurso, dentro do ChatGPT:

1. **Settings → Security and access**, no fundo, **Developer mode**: ativa-o. O ChatGPT assinala-o como «alto risco»: é o aviso que mostra a qualquer pessoa que adicione um servidor próprio, e serve para isso.
2. **Settings → Plugins → Browse plugins**.
3. No canto superior direito, o botão **+**, que abre o formulário «New plugin».
4. Nome **Flow**; na ligação, o endereço do teu Flow seguido de `/mcp`, por exemplo `https://flow.kaigrid.ai/mcp`; autenticação **OAuth**; marca «I understand and want to continue»; **Create**.
5. **Sign in with Flow**: abre-se a página do Flow «... pede acesso ao Flow», onde escolhes entre Só leitura e Pode modificar, marcas as pastas e lêes o aviso sobre os dados. **Permitir** (ou **Não permitir**, e não acontece nada).
6. Num chat novo escolhe o Flow entre os plugins e experimenta: «o que vês no Flow?».

Na página de consentimento, nos espaços de equipa vês **só** as pastas que o administrador abriu: nenhum cadeado, nenhuma lista para decifrar.

O ChatGPT muda com frequência os nomes das suas opções: até há pouco tempo os plugins chamavam-se conectores. Se uma opção já não tiver esse nome, procura-a pelo que faz.

09 Ligar o Claude na web

O Claude na web segue o mesmo caminho do ChatGPT: **nenhuma chave a copiar**. Dás-lhe o endereço do teu Flow e o Claude abre uma página do Flow onde entras, escolhes as pastas e confirmas.

No Claude: **Settings → Connectors → «Add custom connector»**, e como endereço o endereço do teu Flow seguido de `/mcp`, por exemplo `https://flow.kaigrid.ai/mcp`.

A partir daí é idêntico: abre-se a página «... pede acesso ao Flow», onde escolhes entre Só leitura e Pode modificar, marcas as pastas e lêes o aviso sobre os dados.

Ao confirmar, a ligação aparece sozinha em **Conta → Assistentes de IA**, com o nome do assistente, e gere-se como todas as outras: mudas as pastas, mudas o que pode fazer, revogas.

Vale também aqui o que vale para o ChatGPT: nos espaços de equipa, na página de consentimento, vês **só** as pastas que o administrador abriu.

10 Mudar de ideias

Nada do que escolheste é para sempre, e **nunca se refaz a chave**.

- **As pastas:** em Conta → Assistentes de IA abres a ligação e mudas as marcações. As novas pastas valem a partir do pedido seguinte do assistente, e no assistente não precisas de mexer em nada.
- **O que pode fazer:** passa-se de Só leitura a «Pode modificar» e vice-versa da mesma forma.
- **Revogar:** o assistente deixa **de imediato** de ver o Flow. Usa-se quando um projeto termina, quando se perde um computador, ou simplesmente quando terminaste.

A página indica, para cada ligação, quando a criaste, **o último uso** e a validade: se uma não é usada por ninguém há meses, nota-se.

Se o assistente tentar fazer algo que a ligação não permite (uma modificação com uma ligação em só leitura, ou numa pasta onde o administrador não colocou Escrita), recebe uma recusa que explica o que falta, e transmite-ta em vez de falhar em silêncio.

11 Quem trabalha na pasta sabe

Uma pasta aberta a um assistente não é um assunto privado de quem criou a ligação: quem trabalha nela tem de poder sabê-lo.

Por isso, ao lado do nome das pastas e dos ficheiros que um assistente vê, há um **pequeno ícone**; passando o cursor por cima, indica a que ligação. No painel de informações do ficheiro a mesma coisa aparece escrita por extenso: **«Visível para: Claude no projeto Dainese»**. Veem-na todos os que trabalham ali, não só tu.

No **registo de atividade** fica registo de tudo: quando uma ligação é criada, quando mudam as suas pastas, quando é revogada, **cada leitura de conteúdo** (que ligação, que ficheiro, quando), cada ligação de transferência e cada modificação. O registo dos assistentes está sempre ativo.

O que o registo **não** contém é a conversa: o administrador vê que ficheiros o assistente leu, não o que lhe perguntaste.

12 O que decide o administrador

Nos espaços de equipa é a empresa que estabelece o que se pode abrir a um assistente. O administrador fá-lo em **Consola de administração → Assistentes de IA**, com «Editar a lista»: a mesma árvore em colunas, onde cada espaço e cada pasta tem uma caixa com **três estados**, que se percorrem com um clique.

- **Não** (caixa vazia): os assistentes não a veem. É o estado inicial de tudo: uma empresa que não abre nada não expõe nada.
- **Leitura** (o olho): os assistentes podem lê-la.
- **Escrita** (o lápis): podem também modificá-la, se a ligação estiver em «Pode modificar».

O estado vale para tudo o que a pasta contém, e uma subpasta pode ter um **diferente**: prevalece sempre o mais próximo. O espaço «Clientes» em Leitura pode ter lá dentro «Rascunhos» em Escrita; uma pasta em Escrita pode ter lá dentro «Contratos» só em Leitura. As subpastas mostram atenuado o nível que herdaram: um clique muda-o só ali, outro repõe-no como estava.

Há uma coisa que não se pode fazer: **voltar a pôr «Não» dentro de uma pasta aberta**. Nada de buracos invisíveis: se uma subpasta não deve ser vista, abrem-se as pastas irmãs e não a pasta mãe.

Os **espaços pessoais** não estão nessa lista: cada utilizador decide por si.

Retirar ou baixar uma entrada **vale de imediato**, também para as ligações que já existem. Para que não seja uma surpresa, ao lado de cada entrada a página indica quantas ligações a estão a usar. Na mesma página está a lista das **ligações da empresa**: de quem são, em que pastas, o último uso.

13 Segurança e confidencialidade

Os documentos lidos saem para o fornecedor do assistente. Quando o assistente lê um ficheiro, esse texto chega a quem fornece o assistente (Anthropic, OpenAI ou outro), com o contrato que tu ou a tua empresa têm com esse fornecedor. O Flow não envia nada por iniciativa própria: envia o que o assistente pede, dentro das pastas que lhe abriste. É o motivo pelo qual convém abrir poucas pastas e escolhê-las bem.

Um documento pode conter instruções dirigidas ao assistente: linhas escritas de propósito para que as leia e as execute. Vale para qualquer assistente, e o Flow aplica quatro defesas: à partida a ligação só lê; o texto chega ao assistente marcado como conteúdo de um documento, não como uma ordem; o assistente não pode criar ligações para o exterior; e tudo o que modifica pode ser desfeito a partir da reciclagem e das versões.

Uma chave perdida revoga-se num clique, e a ligação pode ter uma validade desde o início. A página mostra o último uso de cada uma.

Um assistente nunca vê mais do que tu. A ligação vive dentro das tuas permissões: se te retirarem um espaço, as tuas ligações perdem-no no mesmo instante. E vale só para os assistentes: com essa chave não se entra no resto do Flow.

14 Perguntas frequentes

O assistente vê todos os meus ficheiros? Não: só as pastas que marcaste na ligação.

Um colega pode abrir a um assistente uma pasta reservada? Só se ele próprio já vir essa pasta, e só se o administrador a tiver tornado possível de abrir.

Posso mudar de ideias depois? Sim: mudas as pastas ou revogas quando quiseses, e vale de imediato. A chave continua a mesma.

O assistente pode eliminar os meus ficheiros? Só se escolheste «Pode modificar» e só onde o administrador colocou Escrita. E mesmo assim vão para a reciclagem, de onde se restauram.

Como sei se uma pasta está aberta a um assistente? Tem um pequeno ícone ao lado do nome, e o painel de informações do ficheiro indica «Visível para», com o

nome da ligação.

Perdi a chave. Não pode ser recuperada: revoga a ligação e cria uma nova.

Funciona com o ChatGPT? Sim, pela web. E com Claude Code, Claude Desktop, Cursor e Codex.

É preciso instalar alguma coisa? No Flow não, nada. O Claude Desktop usa uma pequena ponte que se transfere sozinha no primeiro arranque.

O administrador vê o que peço ao assistente? Não. Vê que ficheiros o assistente leu ou modificou, não a conversa.

15 Se algo não funcionar

O assistente diz que não tem ferramentas do Flow, ou não sabe o que é. Quase sempre é o bloco colado à mão, com o marcador de posição que ficou no lugar da chave. Alguns assistentes, nesse caso, escrevem na mesma «Authenticated». Copia de novo o bloco da página da ligação, que já contém a chave, e reinicia o assistente.

O assistente não vê uma pasta que eu tinha marcado. Verifica a ligação em Conta → Assistentes de IA: se essa pasta tiver um **cadeado**, o administrador fechou-a aos assistentes, e o fecho vale de imediato, também nas ligações já criadas.

Diz que não pode modificar. Ou a ligação está em **Só leitura**, e mudas isso na respetiva ficha, ou essa pasta não tem o **lápiz**: nos espaços de equipa é o administrador que o coloca.

A ligação expirou. As validades são as que escolheste tu na criação. Uma ligação expirada não se prolonga: cria-se outra.

O ChatGPT não vê as funções novas. O ChatGPT guarda em memória a lista de operações do momento em que criaste o plugin, e não a volta a ler sozinho. Abre a ficha do plugin Flow e carrega em **Refresh**; se não existir, elimina o plugin e cria-o de novo. Depois abre um **chat novo**. As permissões, pelo contrário, valem sempre de imediato, independentemente do que o ChatGPT tenha em memória.

Revoguei por engano. Não se restaura: cria-se uma ligação nova e repete-se o percurso no assistente. Demora um minuto.

