



Passo a passo completo

Claude sem vazar *sigilo*

O guia pra escolher a conta certa no escritório

Claude sem vazar sigilo: o guia pra escolher a conta certa no escritório

O que você vai montar

No fim desse guia você vai ter três coisas resolvidas:

1. Vai saber, sem dúvida, se a sua conta Claude atual pode ou não usar as suas conversas pra treinar modelo de IA.
2. Vai ter desligado (ou confirmado desligado) essa opção na sua conta pessoal, se for o caso.
3. Vai ter um critério claro, na ponta da língua, pra decidir quando um caso pode ir pro Claude pessoal e quando ele exige a conta corporativa do escritório.

Não é sobre parar de usar IA. É sobre usar sabendo o que está acontecendo com o dado que você digita.

Antes de começar

Você precisa de:

- Uma conta Claude ativa, de qualquer plano (Free, Pro, Max, Team ou Enterprise). Se ainda não tem, cria uma grátis em claude.ai só pra seguir os passos de checagem.
- Se você é sócio ou responsável técnico do escritório, acesso de administrador na conta, caso o escritório já tenha um plano de time.
- 10 minutos pra mexer nas configurações, sem pressa.

Não precisa saber programar. Isso aqui é configuração de conta, não código.

1. Entenda as duas contas que existem (a raiz da confusão)

A confusão que mais aparece é achar que existe "o Claude", um produto só, com uma regra só de privacidade. Não existe. Existem dois mundos com regras opostas.

1.1 Conta pessoal (Free, Pro, Max)

É a conta que qualquer pessoa cria em claude.ai com e-mail e senha, sem contrato de empresa. Desde 2025, a Anthropic mudou a política dessas contas: por padrão, ela **pode usar suas conversas e sessões de código pra treinar modelos futuros**, guardando o material por até **5 anos**. Isso vale pra chats novos e pra chats antigos que você retomar.

O ponto que pega mais gente: essa opção vem **ligada por padrão**. Aparece um pop-up de atualização de termos, com um botão grande "Accept" e um interruptor que já está em "On". Quem clica em aceitar sem olhar o interruptor, autoriza na hora.

Isso não quer dizer que sua conversa fica pública ou visível pra qualquer pessoa. Quer dizer que ela pode ser usada, de forma desidentificada, pra melhorar os modelos da empresa.

1.2 Conta corporativa (Claude for Work, Enterprise, API)

É a conta contratada pelo escritório como pessoa jurídica, ou o acesso via API (o mesmo que a maioria das rotinas automatizadas de Cowork usa por trás). Aqui a regra é o oposto: **por padrão, o dado não é usado pra treinar nenhum modelo**. Não existe um interruptor pra desligar isso porque não tem o que desligar, já vem assim no contrato comercial.

Isso é o que separa "estou testando uma ferramenta" de "estou usando uma ferramenta de trabalho".

2. Como checar e desligar o treino de modelo na sua conta pessoal

Se você usa Claude Free, Pro ou Max pra qualquer coisa que toque em dado de cliente, faça isso agora.

2.1 Onde clicar (passo a passo)

1. Entre em claude.ai e faça login normalmente.
2. No canto, clique no seu nome ou foto de perfil pra abrir o menu.
3. Clique em **Settings** (Configurações).
4. Procure a aba ou seção **Privacy** (Privacidade).

1. Ache a opção com o nome **"Help improve Claude"** (Ajude a melhorar o Claude) ou texto parecido com "Allow the use of your chats and coding sessions to train and improve Anthropic AI models".
2. Se o interruptor estiver em **On** (azul ou verde, ligado), clique pra deixar em **Off** (cinza, desligado).

2.2 O que esperar depois de desligar

- Chats novos, a partir desse momento, não entram mais na fila de treino.
- **O que já foi usado pra treinar antes de você desligar não pode ser desfeito.** A mudança vale só pra frente, não apaga o que já rolou.
- Isso não muda o histórico das suas conversas dentro do app, elas continuam salvas normalmente pra você consultar. O que muda é só se elas alimentam ou não o treino de modelo.

Exemplo de texto que você vai ver na tela, mais ou menos assim:

```
Allow the use of your chats and coding sessions  
to train and improve Anthropic AI models  
[ Toggle: On ] ← clique pra mudar pra Off
```

Como conferir que funcionou: volte na mesma tela de Privacidade depois de fechar e abrir o app de novo. O interruptor tem que continuar em Off. Se voltar pra On sozinho, é sinal de bug ou de uma atualização de termos nova pedindo pra você decidir de novo, o que já aconteceu antes.

3. Como saber quando migrar pra conta corporativa

Você não precisa contratar plano de empresa pra tudo. Mas alguns sinais dizem que já passou da hora.

3.1 Sinais de que você precisa

- Você cola trecho de petição, contrato ou e-mail com **nome, CPF ou dado identificável do cliente** direto na conversa.
- Você já monta ou pretende montar uma **rotina automatizada** (tipo a de planilha de propostas ou de leitura de e-mail) que roda sozinha, sem você revisando cada entrada.

- Mais de uma pessoa do escritório usa Claude pro mesmo tipo de trabalho, e você não tem controle centralizado do que cada um está colando lá.
- Você já assinou ou pretende assinar um **termo de confidencialidade** com um cliente que exige saber onde o dado dele circula.

Se dois ou mais desses pontos são verdade pro seu escritório, a conta pessoal já não é a ferramenta certa, mesmo com o treino desligado.

3.2 Como conversar isso com o financeiro do escritório

O argumento que funciona não é "por segurança", que soa abstrato. É prático: **o plano corporativo já vem sem a decisão manual de desligar treino, sem risco de um "Accept" clicado sem querer por um estagiário, e com contrato que você pode mostrar pro cliente se ele perguntar onde o dado dele fica.** Isso é um argumento de compliance que se paga sozinho na primeira vez que um cliente perguntar.

4. O que muda na prática pro seu dia a dia com clientes

4.1 O que é seguro colocar em qualquer conta

- Estrutura de peça processual sem nome de cliente (o esqueleto, os artigos, a lógica do argumento).
- Perguntas conceituais de direito, sem colar trecho de processo real.
- Rascunho de e-mail genérico, sem dado identificável.

4.2 O que só deveria ir pra conta corporativa

- Qualquer trecho colado direto de um processo real, com nome das partes.
- Planilhas ou rotinas que leem pasta de cliente inteira (tipo a rotina de propostas do Cowork).
- Qualquer coisa que, se vazasse, você teria que explicar pro cliente por que vazou.

Erros comuns

Erro 1: achar que desligar o treino apaga o que já foi treinado. Causa: confundir "parar de coletar dado novo" com "apagar dado antigo". Correção: a mudança só vale daqui pra frente. Se você colou dado sensível antes de desligar, já foi.

Erro 2: achar que conta corporativa nunca guarda nada, em nenhuma hipótese. Causa: ignorar que desde junho de 2026 existe uma retenção de 30 dias específica pros modelos mais avançados (a linha Mythos, que inclui o Fable 5), mesmo em contrato de zero retenção. Correção: saber que esses 30 dias existem só pra análise de segurança (detectar ataque, abuso, uso malicioso em padrão que só aparece olhando várias conversas juntas), com acesso restrito a um time pequeno de revisores e log de auditoria. Depois de 30 dias, apaga sozinho. Não é treino, não é público.

Erro 3: confundir "usar pra treinar modelo" com "tornar público". Causa: o termo "treinar IA" soa assustador e parece que a conversa vira algo visível. Correção: mesmo quando um dado entra pra treino, ele é desidentificado e processado internamente, ninguém acessa sua conversa individual publicamente.

Erro 4: usar o Claude Code de graça (plano Free) achando que código de cliente ali é seguro. Causa: achar que "é código, não é texto sensível". Correção: o Claude Code no plano de consumo (Free, Pro, Max) segue a mesma regra de treino das outras contas pessoais. Se o código toca em lógica de negócio ou dado de cliente, o mesmo cuidado da seção 2 vale aqui.

Próximo nível

Depois de resolver a conta, o próximo passo natural é migrar as rotinas que você já roda (a de planilha de proposta, a de leitura de e-mail) pra rodarem dentro de uma conta corporativa desde o início, em vez de testar na pessoal e migrar depois. Isso evita o retrabalho de reconfigurar tudo quando o escritório crescer, e já deixa você com resposta pronta se um cliente perguntar, com contrato na mão, onde o dado dele fica.