Mozout

Gerado a 28/10/2026 09:54

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

O que é um agente de IA e o que ainda não consegue fazer de forma fiável

IA e Agentes

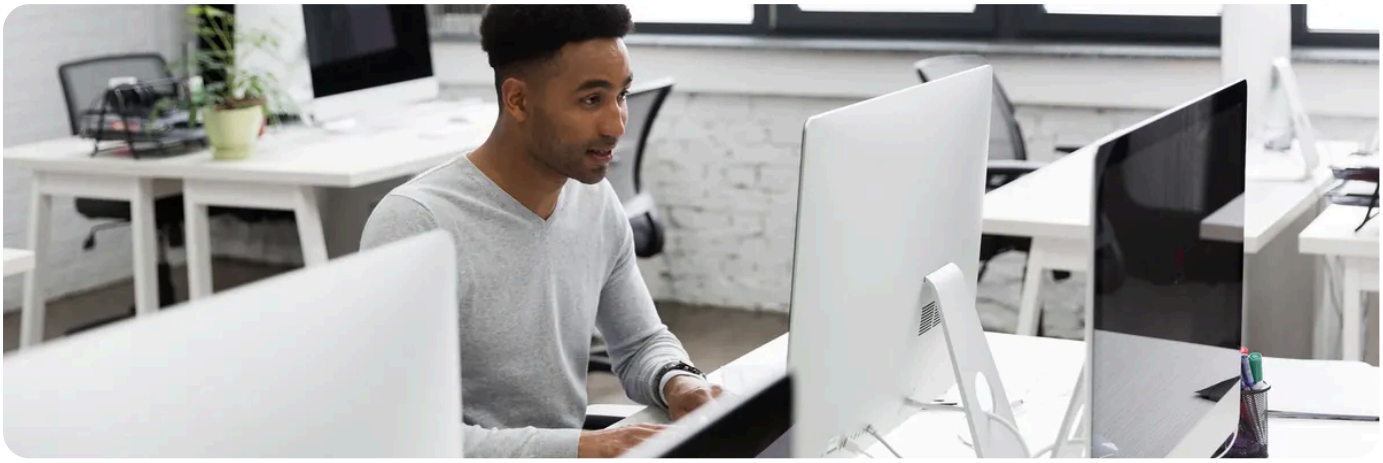
CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-4896	v2026.10.10	Angola · Português

MozOut Angola
RLX Angola, Lda. · Grupo RLX Holdings
NIF 500 260 5724 · Matrícula 26464-25/250724

https://www.my.mozout.com/knowledgebase/4896

O que é um agente de IA e o que ainda não consegue fazer de forma fiável

IA e Agentes Criado em **10 de outubro de 2026** 3 min de leitura



Um **agente de IA** é um modelo ligado a ferramentas (ler ficheiros, pesquisar, escrever, enviar mensagens, executar comandos) que trabalha em ciclo: pensa, usa uma ferramenta, vê o resultado e decide o passo seguinte, até dar a tarefa por feita. Um chat só responde; um agente **age**. É por isso que rende mais e que corre mais riscos.

Onde um agente ajuda e onde falha

Tipo de tarefa	Resultado típico	Porquê
Curta, bem definida, com critério claro («organiza estes ficheiros por data»)	Costuma correr bem	Pouco espaço para desvios, fácil de verificar.
Longa, com muitos passos	Os erros somam-se	Um passo errado no início contamina os seguintes, e o agente segue em frente com confiança.
Que exige conhecer a empresa, o cliente ou o contexto	Fraco	Só sabe o que lhe deram. O resto inventa ou deixa por fazer.
Com consequências difíceis de desfazer (apagar, pagar, enviar)	Perigoso sem aprovação	Não distingue bem uma acção reversível de uma irreversível.
Aberta e vaga («faz crescer o meu negócio»)	Dispersa	Sem critério de sucesso, nunca sabe quando parar.

Os limites que não mudam com a próxima versão

1. **Pode estar errado com certeza.** Escreve com a mesma confiança quando acerta e quando inventa. Veja **como verificar uma resposta**.

2 **Pode entrar em ciclo** e gastar sem produzir nada. Cada volta custa tokens. Veja **como se contam os tokens**.

3 **Pode ser desviado por texto alheio.** Uma página ou um e-mail com instruções escondidas pode mudar o que ele faz. Veja **prompt injection**.

4 **Só tem os poderes que lhe der.** Isto é um limite bom: quanto menos acesso, menos estragos.

5 **Não assume a responsabilidade.** Quem responde é quem o pôs a trabalhar.

Como usar um agente com cuidado

Medida	Como
Acesso mínimo	Uma conta só para ele, com permissões só para o que precisa. Nunca a sua conta de administrador.
Aprovação humana	Ele propõe, uma pessoa confirma tudo o que seja enviar, pagar, apagar ou publicar.
Tecto de gasto	Um limite no fornecedor do modelo, antes de o deixar correr sozinho.
Registos	Guarde o que ele fez e porquê, para poder rever e voltar atrás.
Ensaio	Primeiro num ambiente de teste, sem dados importantes.

Se a ideia é pôr um agente a falar com clientes, pergunte primeiro o que acontece quando ele se engana à frente deles. Se a resposta é «um cliente zangado», o que precisa provavelmente é de um fluxo com aprovação humana, não de um agente solto.

! **Um agente que corre num servidor tem acesso a esse servidor.**
Num VPS não gerido, a instalação, a segurança e a manutenção da aplicação são suas: a MozOut não instala nem repara agentes de terceiros. Veja **até onde vai o nosso suporte**.

Para começar, escolha **uma tarefa pequena e reversível**, dê-lhe só leitura, e compare o que ele faz com o que faria. Só depois lhe dê poder de escrever.

RECOMENDADO

Quer um servidor onde experimentar, com acesso root? Veja os planos de VPS.

Ver planos de VPS →

VEJA TAMBÉM

- Um agente de IA precisa de um VPS, não de hospedagem partilhada →
- Segurança do OpenClaw: o que alcança e como o limitar →
- O que é um servidor MCP →
- Planos de VPS →

Mozout

MozOut Angola

RLX Angola, Lda. · Grupo RLX Holdings

NIF	500 260 5724
MATRÍCULA	26464-25/250724
SEDE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACTOS	info@mozout.com · +244 942 011 191 · www.mozout.com
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

Versão online deste documento

RLX-AO-KB-4896 · v2026.10.10 · Gerado a 28/10/2026 09:54