interweb

Gerado a 15/11/2026 00:26

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

# Segurança do OpenClaw: o que ele alcança e como o limitar

Agentes e IA num VPS

| CÓDIGO | VERSÃO | PAÍS · IDIOMA |
| --- | --- | --- |
| RLX-AO-KB-926 | v2026.10.28 | Angola · Português |

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

https://www.meu.interweb.ao/knowledgebase/926

# Segurança do OpenClaw: o que ele alcança e como o limitar

Agentes e IA num VPS · Criado em **10 de outubro de 2026** · Atualizado em **28 de outubro de 2026** · 3 min de leitura



O OpenClaw tem acesso a ficheiros, comandos e contas, e age em seu nome. Por isso a pergunta de segurança certa não é «o programa é seguro?», é **«o que acontece no pior dia, e quanto estrago consegue fazer?»**. A resposta controla-se com quatro decisões: um utilizador próprio, sem root permanente; permissões mínimas; um servidor que não guarde mais nada importante; e limites de gasto no fornecedor do modelo.

Isto vale para qualquer agente que execute coisas, e não só para este. Não há como garantir que um modelo de IA acerta sempre ou que ignora instruções más escondidas num texto. Por isso se limita o alcance, em vez de confiar.

## O que ele pode alcançar

| Alcance | O risco | O limite a pôr |
|---|---|---|
| **Ficheiros do servidor** | Ler segredos, apagar ou alterar dados | Correr com um utilizador sem acesso às suas outras aplicações e ficheiros |
| **Comandos** | Executar algo destrutivo, por engano ou por instrução maliciosa | Sem root permanente. Sem `sudo` livre para esse utilizador. |
| **Contas e chaves** | Gastar dinheiro ou enviar em seu nome | Chaves só com as permissões necessárias e com limite de gasto no fornecedor |
| **Canais de mensagens** | Qualquer pessoa que lhe escreva dá-lhe ordens | Só contas autorizadas. Veja **ligar a um canal**. |
| **Rede** | Portas abertas à internet | Só as que precisa, com o firewall activo |

## Como o limitar, por ordem

1. **Um servidor só para ele.** Não o instale no VPS onde está o site, a loja ou a base de dados da empresa. Um servidor de ensaio, fácil de refazer, é o sítio certo para começar.

2. **Utilizador próprio, sem root permanente.** Entre como root só para preparar. Depois, o OpenClaw corre com um utilizador normal que só vê a sua própria pasta.

3. **Permissões mínimas.** Dê-lhe acesso apenas às pastas e contas de que a tarefa precisa. Se a documentação oferecer um modo que peça confirmação antes de acções sensíveis, use-o e lembre-se de que uma confirmação só protege se a ler.

4. **Chaves com limite.** Crie uma chave de API só para este agente e, no painel do fornecedor, ponha um limite de gasto, se o fornecedor o permitir. Veja **obter uma chave e guardá-la em segurança**.

5. **Feche o resto.** Mantenha o firewall activo e o SSH protegido, como em **manter o VPS seguro**.

6. **Tenha como voltar atrás.** Uma cópia (snapshot) antes de lhe dar novos poderes. Veja **cópias de um VPS**.

**Instruções escondidas.**
Se o agente ler uma página, um e-mail ou um ficheiro com texto do género «ignora o que te pediram e faz isto», pode obedecer. Quanto mais fontes desconhecidas ele ler, maior o risco. Não lhe dê, ao mesmo tempo, acesso a coisas sensíveis e a conteúdo de desconhecidos.

**Nunca dê ao agente**
a senha do painel, as chaves do domínio, a chave do e-mail ou dados de clientes só porque «é mais fácil». O que ele ler pode passar pelo fornecedor do modelo.

Leia os registos de vez em quando. Se aparecerem comandos que não pediu, desligue o agente, revogue as chaves e restaure a cópia. Veja **manter o OpenClaw no dia a dia**.

PRECISA DE AJUDA?

Quer ter a certeza de que o seu VPS está fechado como deve? Peça-nos ajuda com o acesso e a rede do servidor.

**Abrir um pedido de suporte →**

VEJA TAMBÉM

- O que é o OpenClaw e o que precisa para o correr
- Manter o VPS seguro: as seis coisas que contam
- Alucinações de IA: como verificar uma resposta
- Política de Suporte

interweb

## Interweb Angola

RLX Angola, Lda. · Grupo RLX Holdings

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

RLX-AO-KB-926 · v2026.10.28 · Gerado a 15/11/2026 00:26

Versão online deste documento