

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Confirmar que o HTTPS do seu site está bem: certificado, cadeia, validade e protocolos

Segurança

CÓDIGO

RLX-BR-KB-5886

VERSÃO

v2026.10.15

PAÍS · IDIOMA

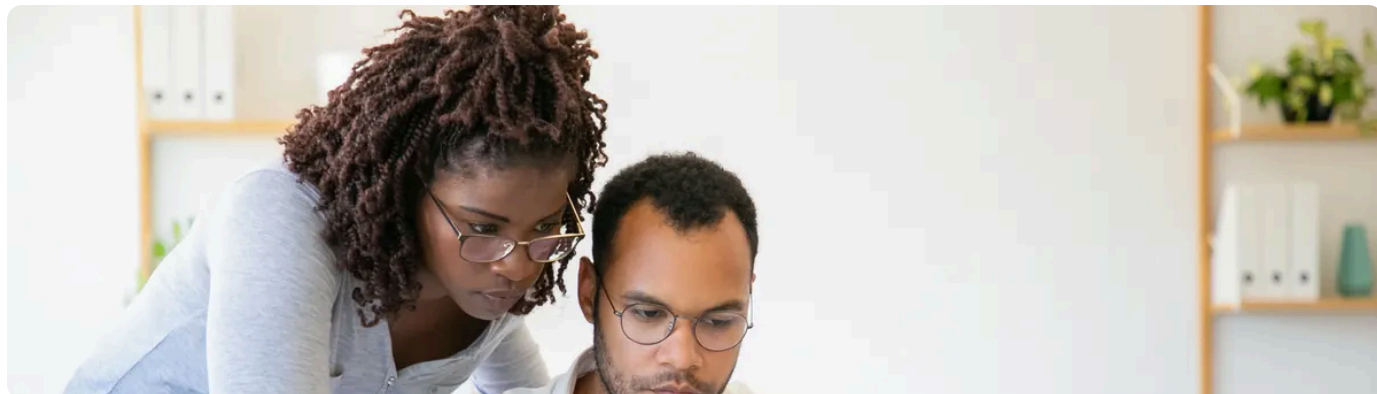
Brasil · Português (Brasil)

MozOut Brasil

RLX Holdings (Pty) Ltd. · Grupo RLX Holdings

N.º fiscal (SARS) 943 907 6234 · N.º de registo (CIPC) 2025/667953/07

<https://www.my.mozout.com/knowledgebase/5886>



A resposta curta: o cadeado no navegador não diz tudo. Um site pode mostrar o cadeado no seu computador e falhar em outros aparelhos por causa de uma **cadeia de certificados incompleta**, de um certificado que **não cobre o www** ou que **está acabando**. Cinco verificações simples apanham quase tudo.

O que verificar

Verificação	O que procurar
Para quem é o certificado	Deve cobrir o endereço com e sem www. Se cobre só um, o outro dá aviso.
Validade	A data de fim. Um certificado expirado dá o aviso vermelho a todos: Certificado expirado .
A cadeia completa	O servidor deve enviar também os certificados intermediários. Sem eles, alguns celulares e programas recusam.
Redirecionar de http para https	Quem escreve o endereço sem https deve ser levado ao seguro: Redirecionar de HTTP para HTTPS .
Conteúdo misto	Imagens ou scripts carregados por http numa página https tiram o cadeado: Conteúdo misto .

Passo a passo

1

No navegador, clique no cadeado, abra os detalhes do certificado e leia «Emitido para», «Emitido por» e as datas.

2

No cPanel, a ferramenta «Estado de SSL/TLS» mostra o estado do certificado de cada domínio e subdomínio.

3

Teste a cadeia fora do seu computador: na linha de comandos, `curl -vI https://o-seu-dominio.com` deve acabar sem um erro de certificado; ou use um teste de SSL online.

4

Abra o endereço sem https e com www e confirme que acaba sempre na versão que escolheu.

5

Abra a página no celular, em outra rede, para apanhar o que o seu computador esconde.

Um certificado é de um domínio, não do site inteiro. Se junta um subdomínio ou um domínio novo, ele também precisa de certificado. E se usa o Cloudflare, o certificado que o visitante vê é o do Cloudflare: **SSL no Cloudflare**.

Depois do HTTPS bem, o passo seguinte é reforçar: **HSTS** e **Cabeçalhos de segurança**. Qual o tipo de certificado: **DV, OV e EV**.

O certificado não ativa ou o aviso persiste? Veja **Comprei um certificado SSL e não ativou** e abra um pedido com o endereço.

Abrir pedido de suporte

VEJA TAMBÉM

A renovação do certbot falhou ou o certificado expirou: como descobrir por quê

Conteúdo misto depois de passar a HTTPS: o cadeado que não acende

HSTS explicado: forçar o https para sempre, e a armadilha de o ligar cedo demais

Comprei um certificado SSL e não ativou: a validação do domínio

Ativar o SSL no Cloudflare sem partir o site

Certificados DV, OV e EV: que tipo de certificado SSL é que realmente precisa



Versão online deste documento

A MozOut é uma empresa líder em serviços de internet, com a missão de ajudar negócios a nascerem e prosperarem por meio da tecnologia.

2020

FUNDADA

37 mil+

CLIENTES

130+

INSCRIÇÕES POR DIA

MozOut Brasil

RLX Holdings (Pty) Ltd. • Grupo RLX Holdings

N.º FISCAL (SARS)	943 907 6234
N.º DE REGISTO (CIPC)	2025/667953/07
SEDE	72 York Road, Kensington Joanesburgo 2094, Gauteng, África do Sul
CONTACTOS	info@mozout.com • +27 78 823 3325 • www.mozout.com
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado