interweb

Gerado a 21/10/2026 17:36

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

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

Segurança

CÓDIGO
RLX-MZ-KB-1934

VERSÃO
v2026.10.15

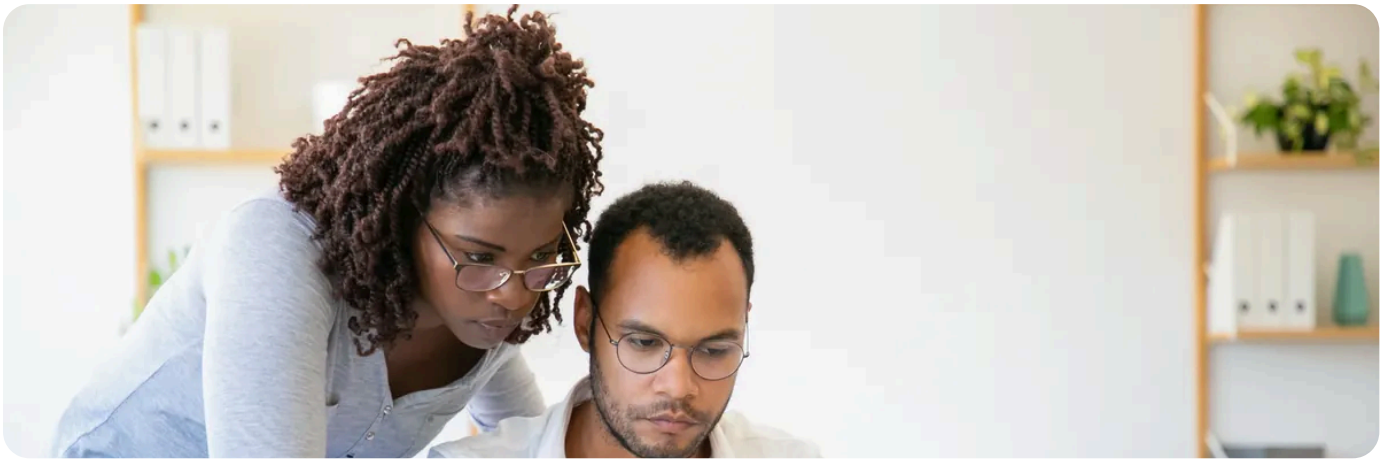
PAÍS · IDIOMA
Moçambique · Português

Interweb Moçambique
RLX Holdings, S.A. · Grupo RLX Holdings
NUIT 401 191 607 · NUEL 105 045 974 · CAE 62022

https://www.meu.interweb.co.mz/knowledgebase/1934

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

Segurança Criado em **15 de outubro de 2026** 2 min de leitura



A resposta curta: o cadeado no navegador não diz tudo. Um site pode mostrar o cadeado no seu computador e falhar noutros aparelhos por causa de uma **cadeia de certificados incompleta**, de um certificado que **não cobre o www** ou que **está a acabar**. 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 intermédios. Sem eles, alguns telemóveis 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,** carregue 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 em linha.

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

5. **Abra a página no telemóvel,** noutra 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 porquê**
- **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 activou: a validação do domínio**
- **Activar o SSL no Cloudflare sem partir o site**
- **Certificados DV, OV e EV: que tipo de certificado SSL é que realmente precisa**

interweb

Interweb Moçambique

RLX Holdings, S.A. · Grupo RLX Holdings

NUIT	401 191 607
NUEL	105 045 974
CAE	62022
SEDE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Moçambique
CONTACTOS	info@interweb.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.interweb.co.mz
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

Versão online deste documento

RLX-MZ-KB-1934 · v2026.10.15 · Gerado a 21/10/2026 17:36