

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

TLS ou cifra ponta a ponta no e-mail: o que protege cada uma, e quando precisa dela

Comparações e alternativas

CÓDIGO

RLX-MZ-KB-2079

VERSÃO

v2026.10.20

PAÍS · IDIOMA

Moçambique · Português

MozOut Moçambique

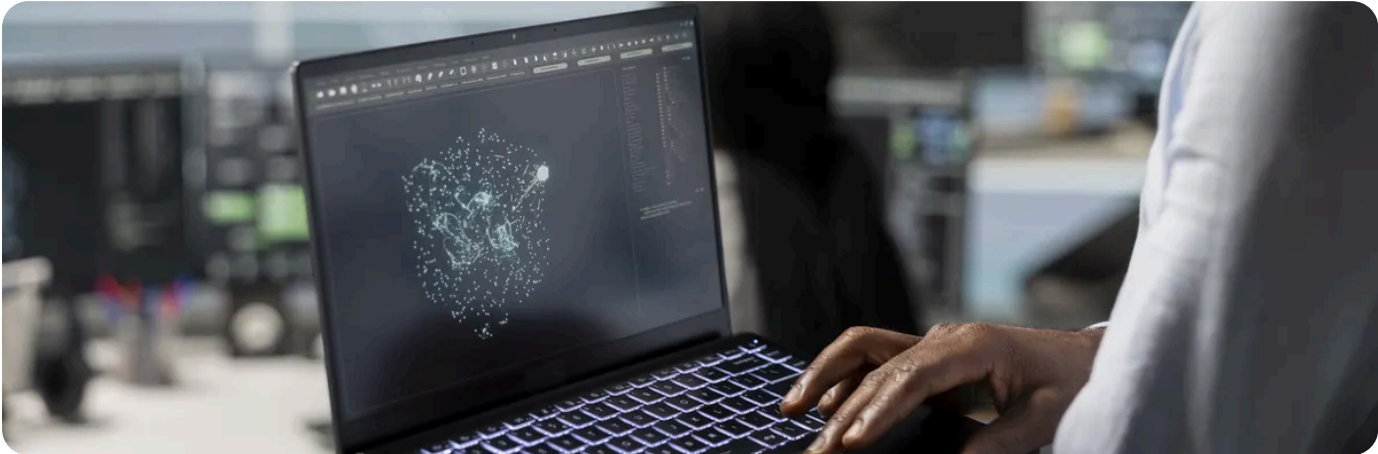
RLX Holdings, S.A. · Grupo RLX Holdings

NUIT 401 191 607 · NUEL 105 045 974 · CAE 62022

<https://www.meu.mozout.co.mz/knowledgebase/2079>

TLS ou cifra ponta a ponta no e-mail: o que protege cada uma, e quando precisa dela

 Comparações e alternativas  Criado em 16 de outubro de 2026  Atualizado em 20 de outubro de 2026
 4 min de leitura



A resposta curta: o **TLS** cifra a mensagem **pelo caminho**: entre o seu aparelho e o nosso servidor, e entre servidores quando os dois lados o aceitam. Quando chega, a mensagem fica legível nas caixas de quem a enviou e de quem a recebeu. A **cifra ponta a ponta** (S/MIME ou OpenPGP) cifra o **conteúdo**, e só o destinatário o abre, mas obriga os dois lados a prepará-la. Para o dia-a-dia o TLS chega; para documentos sensíveis, pense na ponta a ponta ou numa alternativa mais simples.

O que cada uma protege

Tipo	O que protege	O que não protege
TLS entre o seu aparelho e o nosso servidor	A palavra-passe e as mensagens enquanto viajam, por exemplo numa rede Wi-Fi pública. Está ligado quando a aplicação usa SSL/TLS ou STARTTLS.	A mensagem guardada no servidor e no aparelho.
TLS entre o nosso servidor e o do destinatário	A passagem de um servidor para o outro, quando os dois aceitam a ligação cifrada.	Não depende só de nós nem de si: depende também do servidor do destinatário. E a cópia que lá fica é legível.
S/MIME	O conteúdo e os anexos, com um certificado por pessoa. Também permite assinar, para provar quem enviou.	Normalmente o assunto, o remetente, os destinatários e as datas continuam visíveis. Os dois lados precisam de certificado.
OpenPGP	O conteúdo e os anexos, com um par de chaves por pessoa.	O mesmo que o S/MIME, e cada destinatário tem de ter a sua chave pública trocada antes.

Tipo	O que protege	O que não protege
Ficheiro protegido com palavra-passe	O documento anexado, se a palavra-passe seguir por outro canal.	O texto do e-mail, e o assunto.

➞ O que fazer na prática

- 1 Confirme que todas as aplicações usam ligação cifrada:** IMAP na 993 com SSL/TLS, SMTP na 465 com SSL/TLS ou na 587 com STARTTLS. Nunca escolha «Nenhuma» na segurança. Veja **portas SMTP 465, 587 e 25**.
- 2 Abra o webmail só pelo endereço com https** e o cadeado no navegador: **como aceder ao webmail**.
- 3 Para documentos sensíveis, veja se a ponta a ponta compensa.** Os dois lados precisam de certificado ou chaves, e de programas que os usem: o Outlook, o Apple Mail e o Thunderbird suportam S/MIME, e o Thunderbird traz OpenPGP. No webmail e nos telemóveis o suporte varia.
- 4 A alternativa simples:** mande o documento num ficheiro protegido com palavra-passe e dê a palavra-passe por outro canal, por telefone ou por mensagem.
- 5 Se usar ponta a ponta, guarde a chave privada ou o certificado num sítio seguro.** Sem eles, as mensagens antigas cifradas deixam de abrir, mesmo para si.

! O cadeado não torna a mensagem secreta para sempre.
Depois de entregue, fica legível na caixa do destinatário e em todos os aparelhos que a sincronizam. Não mande palavras-passe, dados de cartão ou documentos de identificação por e-mail só porque a ligação é cifrada. E desconfie de mensagens que lhe pedem: **como reconhecer phishing**.

💡 Um ficheiro protegido e a palavra-passe por outro canal
resolvem a maior parte dos casos sem que nenhum dos lados tenha de instalar certificados.

🗨️ PRECISA DE AJUDA?

Dúvidas sobre se a sua aplicação está a usar ligação cifrada? Diga-nos qual usa e envie-nos uma imagem das definições da conta, sem a palavra-passe.

 **Abrir pedido de suporte ➞**

Onde ver na sua conta

- ✓ **As definições certas:** no cPanel, em **Contas de e-mail**, o botão **Connect Devices** ao lado de cada conta mostra as definições seguras: o servidor de entrada e de saída, IMAP na 993, POP3 na 995 e SMTP na 465, todas com SSL/TLS, e o nome de utilizador, que é o endereço completo.
- ✓ **No seu programa:** confirme a segurança da ligação de cada servidor (SSL/TLS, ou STARTTLS na 587) e que o servidor de saída pede autenticação. No Thunderbird está em **Definições da conta**, em **Definições do servidor** e **Servidor de saída (SMTP)**.
- ✓ **O S/MIME e o OpenPGP vivem no programa, não no servidor:** no Outlook em **Centro de Fidedignidade > Segurança do E-mail**; no Thunderbird em **Definições da conta > Encriptação ponto a ponto**. A chave privada fica no seu dispositivo.
- ✓ **No webmail,** uma mensagem encriptada costuma aparecer como um anexo chamado smime.p7m ou como um bloco de texto ilegível: abra-a no programa que tem a chave. As mensagens só assinadas leem-se normalmente.

VEJA TAMBÉM

Portas SMTP 465, 587 e 25: SSL, STARTTLS e qual usar



Como acessar o seu webmail



Como reconhecer um e-mail ou mensagem de phishing, e o que fazer se clicou



A sua conta de e-mail foi pirateada: o que fazer na primeira hora



Guardar uma cópia própria do seu e-mail: como fazer cópia de segurança de uma caixa



A aplicação Gmail ou a aplicação Outlook para a caixa do seu domínio: telemóvel e computador





MozOut 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@mozout.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.mozout.co.mz
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado



Versão online deste
documento

RLX-MZ-KB-2079 · v2026.10.20 · Gerado a 21/10/2026 17:53