interweb

Gerado a 29/10/2026 05:15

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Tornar o Ambiente de Trabalho Remoto de um VPS Windows mais seguro

VPS e Servidores

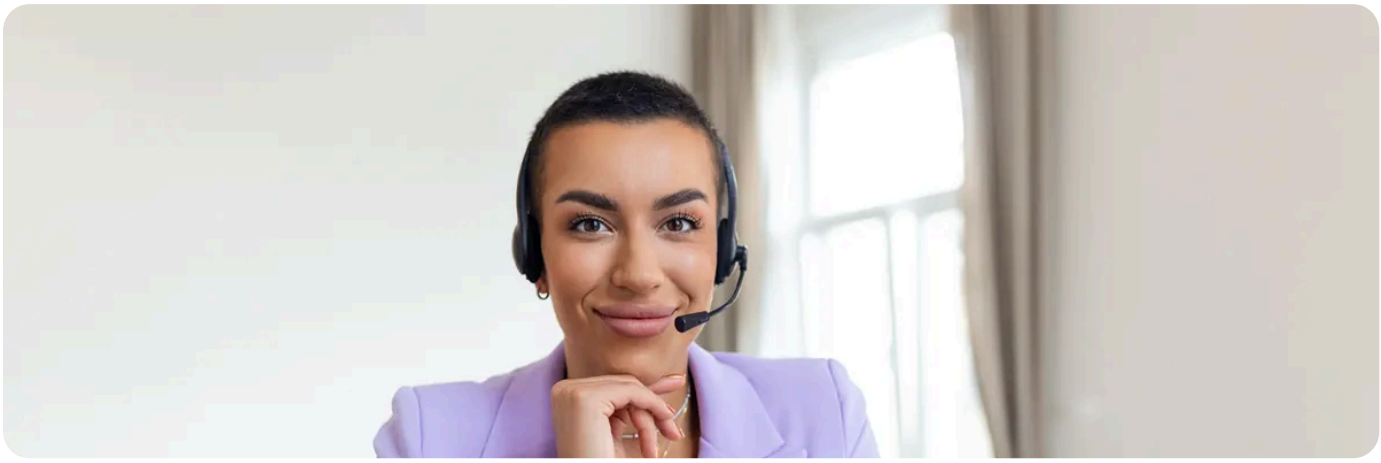
CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-MZ-KB-1412	v2026.10.28	Moçambique · Português

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/1412

Tornar o Ambiente de Trabalho Remoto de um VPS Windows mais seguro

VPS e Servidores · Criado em **10 de outubro de 2026** · Atualizado em **28 de outubro de 2026** · 4 min de leitura



Um Windows Server com a porta 3389 aberta à internet é testado por programas automáticos **todos os dias**, a adivinhar senhas. O ambiente de trabalho remoto (RDP) é a porta de entrada mais atacada num servidor Windows. As defesas que mais contam, por ordem: uma **senha longa e única**, o **bloqueio de contas** depois de tentativas falhadas, **limitar quem pode ligar-se** (por endereço IP na firewall) e manter o **Windows actualizado**. Este artigo parte de já estar ligado ao servidor (**ligar a um VPS Windows**). Num VPS não gerido, a segurança do Windows é sua.

Passo a passo

1. **Mude a senha do Administrador** para uma frase longa que não use noutro lado. É o que mais pesa: uma senha fraca é a forma mais comum de um servidor Windows ser comprometido.

2. **Crie um utilizador próprio para si,** membro dos administradores, e use-o no dia-a-dia. Depois pode desactivar o "Administrator" (as tentativas automáticas apontam quase sempre para esse nome). Teste o novo utilizador numa segunda sessão antes de desactivar o antigo.

3. **Active o bloqueio de contas.** Em *Local Security Policy* (`secpol.msc`), *Account Policies*, *Account Lockout Policy*: defina quantas tentativas falhadas bloqueiam a conta e por quanto tempo. Escolha valores que o impeçam de se bloquear a si no primeiro engano.

4. **Exija autenticação ao nível da rede (NLA).** Em *Propriedades do Sistema*, separador *Remote*, deixe marcada a opção que só permite ligações de computadores com autenticação ao nível da rede. Obriga a autenticar antes de abrir a sessão.

5. **Limite quem pode ligar-se.** No *Windows Defender Firewall with Advanced Security*, abra a regra de entrada do ambiente de trabalho remoto, separador *Scope*, e em *Remote IP address* ponha só o seu endereço (ou os do escritório). Descobre o seu em **o seu endereço IP público**.

6 **Limite quem tem direito a ligar-se** com o grupo *Remote Desktop Users*: só as contas que lá estão (e os administradores) entram por RDP.

7 **Mantenha o Windows Update ligado** e reinicie quando pedir. Falhas do RDP vão sendo descobertas e corrigidas, e um servidor sem actualizações fica com as conhecidas em aberto.

Ver quem tentou entrar

O *Event Viewer*, em *Windows Logs*, *Security*, regista as tentativas: o evento **4625** é um início de sessão falhado, o **4624** um bem-sucedido (o tipo 10 é remoto). Muitas falhas por minuto vindas de endereços desconhecidos são o ruído de fundo da internet; um 4624 de um endereço que não reconhece é o alarme.

Medida	Quanto ajuda
Senha longa e única	Muito. É a que mais pesa.
Bloqueio de contas	Muito. Trava a adivinhação.
Limitar a firewall ao seu IP	Muito, se o seu IP for estável. Quase fecha a porta ao resto do mundo.
Autenticação ao nível da rede	Bastante. Evita abrir sessões a quem ainda não provou quem é.
Mudar a porta 3389	Pouco. Reduz o ruído das varreduras, mas não é protecção: quem procura a encontra.
Windows Update	Muito, a longo prazo. Fecha as falhas conhecidas.

! **Limitar por IP trancará fora quem muda de endereço.**
Se o seu IP muda (dados móveis, ligações domésticas), a regra deixa de o reconhecer e fica sem entrada. Tenha sempre a consola do painel como recurso, que não passa pela rede: **perdi o acesso ao servidor**. E teste a regra numa segunda sessão antes de fechar a primeira.

! **Mudar a porta do RDP**
exige editar o registo do Windows (chave `PortNumber` em `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp`), abrir a nova porta na firewall e reiniciar. Um erro aí pode deixá-lo sem acesso. Dá pouco ganho; invista antes nas medidas acima.

Um túnel ou VPN à frente do RDP é o mais forte:
A porta 3389 deixa de ficar visível na internet. É mais trabalho a montar e a manter, e é seu. Veja também **manter o VPS seguro** e, se o servidor publica um site, **publicar um site com o IIS**.

PRECISA DE AJUDA?

Trancou-se fora do servidor Windows depois de mexer nestas regras? Diga-nos o nome do serviço e damos-lhe a consola.

Abrir um pedido de suporte →

VEJA TAMBÉM

- **Ligar a um VPS Windows por Ambiente de Trabalho Remoto** →
- **Publicar um site no Windows Server com o IIS** →
- **Como saber o seu endereço IP público** →
- **Manter o seu VPS seguro** →

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-1412 · v2026.10.28 · Gerado a 29/10/2026 05:15