interweb

Gerado a 15/11/2026 00:31

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Trancar o editor de ficheiros do WordPress e algumas definições do wp-config que valem a pena

Utilizadores, entrada e segurança

CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-1918	v2026.10.15	Angola · Português

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

https://www.meu.interweb.ao/knowledgebase/1918

Trancar o editor de ficheiros do WordPress e algumas definições do wp-config que valem a pena

Utilizadores, entrada e segurança · Criado em **15 de outubro de 2026** · 2 min de leitura



A resposta curta: o WordPress tem, no painel, um **editor de ficheiros** que deixa mudar o código do tema e dos plugins. Uma gralha ali tira o site do ar, e quem entrar no painel sem licença pode meter código malicioso. Uma linha no **wp-config.php** desliga-o. Há mais duas ou três definições do mesmo ficheiro que reforçam o site.

As definições

Linha	O que faz
`define( 'DISALLOW_FILE_EDIT', true );`	**Esconde os editores** de temas e de plugins do painel. Não mexe em mais nada. A mais útil.
`define( 'FORCE_SSL_ADMIN', true );`	Obriga o painel e o início de sessão a usar https. Só se o site já tem certificado.
`define( 'WP_POST_REVISIONS', 10 );`	Guarda só as últimas versões de cada artigo, em vez de todas: ajuda a manter a base de dados magra.
`define( 'DISALLOW_FILE_MODS', true );`	**Cuidado:** bloqueia também instalar e atualizar plugins, temas e o próprio WordPress. Só para sites geridos por outra via.
Chaves de segurança (salts)	Mudá-las desliga toda a gente do painel. Útil depois de uma suspeita de intrusão.

Passo a passo

1. **Faça uma cópia do wp-config.php.** Um erro de escrita neste ficheiro tira o site do ar.

2. **Abra o wp-config.php** (Gestor de Ficheiros do cPanel) e ponha a linha escolhida **antes** da frase «That's all, stop editing».

3. **Grave e abra o painel:** em Aspeto e em Plugins já não deve haver os editores de ficheiros.

4. **Confira as permissões** do wp-config.php: ele guarda a senha da base de dados e não deve ser legível por todos: **Permissões de ficheiros**.

5. **Faça as alterações de código** de outra forma (num tema filho, ou por SFTP), e não pelo painel: **Tema filho**.

Isto reforça, não protege sozinho.
O editor desligado não impede quem já tem uma senha de administrador de instalar um plugin malicioso. A defesa verdadeira é o login bem protegido e os plugins em dia: **Proteger o login do WordPress**.

Se o ficheiro foi estragado, veja **Refazer a ligação do wp-config.php**. Outra porta a considerar: **XML-RPC**.

PRECISA DE AJUDA?

Quer ajuda a rever a segurança do seu WordPress? Abra um pedido com o endereço.

Abrir pedido de suporte →

VEJA TAMBÉM

- **Proteger a entrada do WordPress: três passos por ordem de efeito**
- **Permissões de ficheiros explicadas: o que significam 755, 644 e 777**
- **Tema filho ou edição directa: porque as actualizações apagam as suas alterações**
- **Um plugin abandonado ou um PHP antigo: como descobrir os riscos do seu site**
- **Recriar a ligação do wp-config.php**

interweb

Interweb Angola

RLX Angola, Lda. · Grupo RLX Holdings

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

Versão online deste documento

RLX-AO-KB-1918 · v2026.10.15 · Gerado a 15/11/2026 00:31