Fenix WP

RELATÓRIO DE ENTREGA Nº 2026-001

Site limpo e entregue

Padaria Pão Quente (exemplo) · padaria.example.com

PLANO	INÍCIO	ENTREGA	GARANTIA ATÉ
Limpeza Completa	**16/09/2026**	**16/09/2026**	**16/10/2026**

01 Resumo

Site limpo

O site foi reconstruído a partir das fontes oficiais, o spam em japonês e o redirecionamento para o site de apostas foram removidos, e todas as portas de entrada encontradas foram fechadas. A invasão começou por uma versão antiga do plugin de formulários, que já foi atualizada.

02 O que foi encontrado

TIPO	ONDE	AÇÃO
Backdoor	`wp-content/uploads/2024/03/cache.php`	Removido
Backdoor	`wp-content/uploads/2024/05/image.php`	Removido
Backdoor	`wp-includes/class-wp-cache.php` (arquivo falso)	Removido
Arquivo persistente	`wp-content/mu-plugins/wp-cache-helper.php`	Removido
Redirecionamento	`.htaccess`, regra para visitantes vindos do Google	Removido
Administrador fantasma	`wp_users`, usuário wpadmin2	Excluído
Spam de SEO	1.284 posts em japonês em `wp_posts`	Excluídos
Porta de entrada	Plugin de formulários desatualizado	Atualizado

03 Roteiro executado

01 Backup forense — FEITO

Cópia completa dos arquivos e do banco de dados antes de qualquer alteração, guardada fora do servidor.

→ Cópia de 850 MB guardada fora do servidor.

02 Inventário — FEITO

Versões do WordPress e do PHP, plugins e temas com as versões, usuários administradores, crons e outros sites na mesma conta.

03 Core do WordPress — FEITO

Conferência dos checksums oficiais e reinstalação do core limpo, na mesma versão.

→ WordPress 6.6.2 reinstalado; 4 arquivos do core estavam alterados.

04 Plugins e temas — FEITO

Reinstalação a partir das fontes oficiais. Plugins pirateados (nulled), inativos e abandonados são removidos.

→ 14 plugins reinstalados; 2 inativos removidos.

05 Pasta de uploads — FEITO

Remoção de qualquer arquivo executável e bloqueio da execução de PHP em `wp-content/uploads`.

06 Pontos de persistência — FEITO

Revisão de `wp-config.php`, `.htaccess`, `index.php`, `mu-plugins`, drop-ins, `.user.ini`, arquivos fora da pasta pública e crontab do servidor.

07 Banco de dados — FEITO

Limpeza de `wp_options`, de posts e páginas com scripts injetados, do spam de SEO e de usuários desconhecidos.

08 Código sob medida e loja — NÃO SE APLICA

Revisão manual do tema e dos plugins próprios, do checkout (roubo de cartão), dos pedidos e de cada site da rede ou da conta.

09 Blindagem — FEITO

Troca de todas as senhas (WordPress, hospedagem, FTP e banco), novas chaves de segurança, sessões encerradas, editor de arquivos desativado, permissões, atualizações e 2FA.

10 Google e SEO — FEITO

Limpeza do SEO: Search Console (proprietários, sitemaps e ações manuais), remoção das páginas de spam do Google e pedido de revisão do aviso.

→ Pedido de revisão enviado pelo Search Console em 16/09/2026.

11 Validação — FEITO

Teste das páginas principais, dos formulários e do checkout, comparando com o estado anterior.

12 Backup limpo e entrega — FEITO

Backup do site já limpo, relatório em PDF e orientações.

04 O que foi trocado

- Senhas de todos os administradores do WordPress.
- Senha do painel da hospedagem e do FTP.
- Senha do banco de dados, já atualizada no `wp-config.php`.
- Chaves de segurança (salts), com todas as sessões encerradas.

05 O que fica com você

Estas tarefas não dependem de mim e fazem parte das condições da garantia.

- [ ] Trocar as senhas de e-mail e de outros serviços ligados ao site.
- [ ] Passar um antivírus atualizado nos computadores que acessam o painel.
- [ ] Não instalar plugins ou temas pirateados (nulled).
- [ ] Manter WordPress, plugins e temas atualizados.

06 Garantia

A garantia vale até **16/10/2026**. Se o site for invadido de novo nesse período, eu faço uma nova limpeza sem custo, desde que as tarefas do item 05 tenham sido feitas, que ninguém tenha alterado o site fora do combinado e que o servidor não esteja comprometido no nível do sistema.

Suporte prolongado: não contratado. Até o fim da garantia, dá para estender por mais 30 dias por R$ 130.

Qualquer sinal estranho no site durante a garantia, é só me chamar no WhatsApp.