

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

mauro-ferramentas.pages.dev

Objeto investigado	mauro-ferramentas.pages.dev - loja “Mauro Ferramentas” (escadas e equipamentos)
Natureza	Verificação de endereço, vínculo com a empresa declarada e preços
Data da coleta	28/11/2026 (RDAP, DNS, HTTP/TLS, geolocalização, bases públicas, análise do código da página)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do HTML e dos scripts
Achado central	Loja em subdomínio gratuito que exibe o CNPJ de uma **loja de informática da Bahia** e vende escada telescópica de 5,10 m por R$ 158,67
Classificação	**RISCO ALTO**
Emissão do laudo	28/11/2026 as 01:07

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **mauro-ferramentas.pages.dev**, realizada em **28/11/2026** por técnicas de OSINT (inteligência de fontes abertas) e análise passiva — requisições equivalentes às de um visitante comum e consultas a bases públicas, sem cadastro, sem compra e sem envio de dados pessoais. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

A loja funciona em `mauro-ferramentas.pages.dev`, subdomínio gratuito do Cloudflare Pages — não há domínio próprio registrado. Vende escadas de alumínio, lavadora de alta pressão, extratora e balde mop, com 5% de desconto no Pix e parcelamento em 12x.

A página “Sobre a empresa” informa a razão social MAURO JOSE DE OLIVEIRA e o CNPJ 17.810.608/0001-84. A Receita confirma o CNPJ, mas como “MAURO NOTEBOOK”, microempresa de Irecê/BA aberta em 2013 no comércio de equipamentos de informática — outro ramo, e sem endereço, telefone ou e-mail no site que permitam ligar a empresa à loja.

Os preços são muito inferiores aos do varejo: a escada telescópica de 5,10 m sai por R$ 158,67 e a de 3,80 m por R$ 130,90, enquanto escadas telescópicas de 5 m aparecem por cerca de R$ 1.000 em grandes varejistas. O checkout próprio pede nome, CPF e endereço e usa o intermediário de pagamentos Pagou.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: identidade emprestada de uma empresa de outro ramo, subdomínio descartável e preço de atração — o vínculo empresa–site não é demonstrado e o preço sustenta a hipótese de loja falsa.

2. Metodologia e Cadeia de Custódia

Empregaram-se exclusivamente **técnicas passivas**. As respostas de rede e de bases públicas foram salvas no momento da coleta e tiveram hash SHA-256 calculado. O DNS foi consultado via resolvedor público 1.1.1.1; o conteúdo, os cabeçalhos e o bundle JavaScript foram obtidos por requisição HTTPS de visitante comum. Nenhum formulário foi preenchido e nenhum dado pessoal foi enviado. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (rdap.org / registro do gTLD / Registro.br)	`rdap_raw.json · rdap_*.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME) via 1.1.1.1	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS (visitante comum) e navegador headless; home, páginas legais e scripts	`corpo_*.html · headers_home.txt · bundle*.txt`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · PTR reverso	`geoip.json`
CNPJ declarado	Validação por módulo 11 · base pública BrasilAPI/Receita	`cnpj_publico_*.json`
Consolidação	Extração de fatos e hashes SHA-256	`hash_manifest.txt`

3. Identificação Técnica (Domínio, DNS, Hospedagem e TLS)

Endereço	**mauro-ferramentas.pages.dev** — subdomínio gratuito da plataforma `pages.dev`; não há domínio próprio registrado em nome da loja

Domínio da plataforma	pages.dev · registrado em 02/09/2020 · pertence à plataforma, não ao site
DNS - A	172.66.47.189 · 172.66.44.67 · sem MX
Hospedagem	AS13335 Cloudflare, Inc. · San Francisco/US · cabeçalho `server: cloudflare`
Certificado TLS	Let's Encrypt (YE1) · emitido em 20/11/2026 · válido até 18/02/2027
CNPJ exibido	17.810.608/0001-84 · nome fantasia “MAURO NOTEBOOK” · Irecê/BA · desde 2013 · comércio de **equipamentos de informática**, não de ferramentas
Checkout	Página própria `/c/TEL-260` que pede CPF/CNPJ e carrega `js.pagou.ai/payments/v3.js`
Publicidade	Google Ads `AW-18586573829` e Google Tag Manager

Leitura: endereço gratuito do Cloudflare Pages; o registro de `pages.dev` pertence à Cloudflare, não à loja.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Site estático no Cloudflare Pages com checkout próprio (`/c/<referência>`), frete simulado (Jadlog, PAC, Sedex) e rastreamento de campanhas Google Ads.

Aspecto	Constatação
Endereço	Subdomínio gratuito, sem domínio próprio
Empresa exibida	Loja de informática de Irecê/BA
Preço	Escada telescópica 5,10 m por R$ 158,67
Pagamento	Checkout próprio com CPF, Pix e cartão

Leitura: antes de pagar, o comprador não consegue ligar a loja a nenhuma empresa do ramo.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Preço de escada telescópica muito abaixo do varejo	`corpo_produto_escada.html`	ALTA
2	CNPJ de empresa de outro ramo, sem vínculo demonstrado	`cnpj_publico_17810608000184.json`	ALTA
3	Subdomínio gratuito, sem domínio próprio	`dns_records.txt`	MEDIA
4	Sem endereço, telefone ou e-mail da loja	`corpo_empresa.html`	MEDIA
5	Checkout próprio que coleta CPF e endereço	`corpo_checkout_TEL-260.html`	BAIXA

Síntese: cinco indicadores, dois de severidade alta.

6. Conclusão Técnica e Recomendações

A mauro-ferramentas.pages.dev vende ferramentas a preços muito abaixo do mercado em um endereço descartável, usando o CNPJ de uma loja de informática da Bahia. Classificação técnica: **RISCO ALTO**, com indício de apropriação de identidade — a empresa do CNPJ deve ser tratada como possível vítima, não como responsável.

Recomendações ao consumidor / solicitante

- Desconfie de lojas que funcionam em endereços como `*.pages.dev`, `*.vercel.app` ou `*.netlify.app`: são gratuitos e podem ser descartados a qualquer momento.
- Desconfie de preços muito abaixo do mercado combinados com desconto extra para pagamento via Pix.
- Antes de comprar, confira o CNPJ na Receita Federal e se o domínio do site pertence de fato à empresa (consulta RDAP / Registro.br).
- Prefira cartão de crédito, que permite contestação (chargeback); o Pix é instantâneo e de difícil reversão.

Recomendações de mitigação / denúncia

- Reportar o endereço ao Google Safe Browsing e ao canal de abuso do registrador (registrar-abuse@cloudflare.com).
- Vítimas que pagaram via Pix: acionar o banco imediatamente pedindo o MED (Mecanismo Especial de Devolução), registrar boletim de ocorrência e reclamação em consumidor.gov.br / Procon, anexando este laudo.
- Comunicar a empresa do CNPJ 17.810.608/0001-84 sobre o uso de seus dados.

Ressalva: este laudo expressa **juízo técnico de risco** com base em evidências públicas coletadas passivamente em 28/11/2026; não é decisão judicial e não imputa crime a nenhuma pessoa física ou jurídica. Registradores, provedores de hospedagem/CDN, plataformas de loja e intermediários de pagamento são citados apenas como fatos técnicos, sem imputação de conduta. O titular do site pode usar estes achados para corrigir as inconsistências apontadas. Os fatos podem mudar após a coleta.

Anexo A - Manifesto de Integridade (SHA-256)

Hashes SHA-256 das evidências preservadas no momento da coleta (cadeia de custódia).

Arquivo	SHA-256
bundle_js.txt (31027 bytes)	2efa73f66220fae95e1b8a950e9f1aca1802de7980b4c0cd7fde0c6bf6479bd4
cnpj_publico_17810608000184.json (1606 bytes)	0fe8c4fef8462589680828ff10d4712ef33d4b8c6760c4cd2afb93e79070fd3e
corpo_checkout_TEL-260.html (47217 bytes)	984e01ee2aba06fd41ea2e44561253d8cf9320ce0d6b16353cf919c53c7b2736
corpo_empresa.html (14243 bytes)	7b2479fcff26f7191e4aa76306617259406ba66c0074d42130726360bb824145
corpo_home.html (26443 bytes)	f4baec4f1883800fb61ec73c3b5214f8e6f02d67d3ed89c5198fd53532485ca7
corpo_produto_escada.html (54543 bytes)	2bb1d05a0ddc9fc00bac50e47d5956a066734805ac0535ee858b5483114e2ad2
dns_records.txt (472 bytes)	107492e4f4cd79ee53bd02cedaa9806b3a3edd311a581dfa0e2007e3b2fc3352
ferramentas.js.txt (5191 bytes)	91ac2a9b435e3c6ac47da10987f2668632098c2c709aa80d32e5f4e263defe8b
geoip.json (288 bytes)	dfeb76eed337951a9c38b3e6f396dd7c96ca859123aa0c9ba1d79edcb921e1d8
headers_home.txt (723 bytes)	75a5fb198ad9f57524e2202cd7b670c76561be6ed6ae84aabdeeafb2229a8d64
rdap_raw.json (5833 bytes)	87ac08dd118e4fa735970b786b157a6c36598eb59a0bf138c05e2e026c64de51
tls_cert.txt (312 bytes)	487e13e1fe80287907b700e61c055e4803bef982dc8326ea62df28c0e616781c

- Fim do relatório -