

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

torracaferramentas.com

Objeto investigado	torracaferramentas.com - loja online de ferramentas, hidráulica, acessórios e luminárias
Natureza	Verificação de legitimidade da loja, da empresa declarada e do fluxo de pagamento
Data da coleta	17/11/2026 (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 de 41 dias com CNPJ de empresário individual cujo sobrenome coincide com a marca, mas cuja atividade registrada é tapeçaria e cortinas; a meta-descrição do site fala em “cosméticos e produtos de beleza” (resto de modelo) e o Pix sai ~26% mais barato que o cartão
Classificação	**RISCO MÉDIO**
Emissão do laudo	18/11/2026 as 00:54

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **torracaferramentas.com**, realizada em **17/11/2026** 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, em Next.js na Vercel, vende motobombas, bombas d'água, torneiras, pincéis, colas e luminárias, com preços à vista no Pix cerca de **26% menores** que o total parcelado no cartão (ex.: motobomba R$ 748,50 no Pix contra R$ 1.014,22 em 12x). O cartão é processado via Stripe; o Pix, por rota própria (`/api/checkout/pix`).

O rodapé traz endereço em Belo Horizonte, e-mail no próprio domínio e o CNPJ 61.026.455/0001-70, que pertence a uma empresária individual de sobrenome Torraca — coincidência coerente com a marca. A atividade registrada, porém, é comércio de tapeçaria, cortinas e persianas, e não de ferramentas.

A meta-descrição da página inicial diz “Compre cosméticos e produtos de beleza na Torraca Ferramentas” — texto que não corresponde ao catálogo e indica reaproveitamento de um modelo de loja usado para outro segmento.

CLASSIFICAÇÃO DE RISCO	RISCO MÉDIO

Leitura: há vínculo nominal plausível entre a marca e o CNPJ, mas a atividade registrada diverge, o domínio é novo e o modelo de loja foi reaproveitado de outro nicho. Os sinais pedem cautela, sem configurar os indicadores fortes de clone (Seções 4 e 5).

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)

Domínio	torracaferramentas.com
Registro	07/10/2026 · expira 07/10/2027 · **41 dias** antes da coleta

Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)
Registrador	Sav.com, LLC · abuse-contact@sav.com
Servidores de nome	gordon.ns.cloudflare.com · tia.ns.cloudflare.com
DNS - A	216.150.1.1 · 216.150.16.1 · MX: mx1.titan.email, mx2.titan.email
Hospedagem	AS16509 Amazon.com, Inc. · Walnut/US · cabeçalho `server: Vercel`
Certificado TLS	Let's Encrypt (YR2) · emitido em 08/10/2026 · válido até 06/01/2027
CNPJ exibido	61.026.455/0001-70 · empresário individual “LETHYCIA INES DOS SANTOS TORRACA” · aberto em 27/05/2025 · Belo Horizonte/MG (bairro e CEP conferem com o site) · CNAE principal **comércio varejista de tapeçaria, cortinas e persianas** · capital R$ 10 mil
torracaferramentas.com.br	Não registrado (Registro.br)

Leitura: domínio de 41 dias com titular oculto (registrador Sav.com), DNS na Cloudflare, aplicação na Vercel e e-mail Titan no próprio domínio.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Aplicação Next.js (Turbopack) na Vercel, com Supabase, Stripe para cartão e rotas de checkout, frete, funil e `/api/payout/config`. A página de checkout foi baixada como visitante; nenhum pedido foi gerado.

Aspecto	Constatação
Pagamento	Pix (rota própria `/api/checkout/pix`) e cartão via Stripe, em até 12x
Diferença Pix x cartão	~26% (ex.: R$ 748,50 no Pix contra R$ 1.014,22 no cartão)
Identidade	CNPJ 61.026.455/0001-70 · R. Conceição do Pará, 475, Santa Inês, Belo Horizonte/MG · (31) 99019-1681 · atendimento@torracaferramentas.com
Resto de modelo	Meta-descrição “Compre cosméticos e produtos de beleza na Torraca Ferramentas”

Leitura: diferença de preço tão grande entre Pix e cartão desloca o comprador para o meio sem contestação; o cartão via Stripe é a opção que preserva o direito de contestar.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Domínio de 41 dias, titular oculto	`rdap_raw.json`	MEDIA
2	CNAE do CNPJ (tapeçaria/cortinas) diverge do ramo anunciado (ferramentas)	`cnpj_publico_61026455000170.json`	MEDIA
3	Meta-descrição de “cosméticos” — modelo de loja reaproveitado	`corpo_home.html`	MEDIA
4	Pix ~26% mais barato que o cartão	`corpo_home.html`	MEDIA
5	Nenhuma avaliação de produto (“Sem avaliações” em toda a vitrine)	`corpo_home.html`	BAIXA

Síntese: cinco indicadores, nenhum de severidade alta. Não há captura indevida de dados nem identidade alheia demonstrada, mas há inconsistências que um comprador deve pesar.

6. Conclusão Técnica e Recomendações

A torracaferramentas.com exibe um CNPJ cujo titular tem o mesmo sobrenome da marca, mas com atividade registrada diferente, num domínio de 41 dias montado sobre um modelo reaproveitado de loja de cosméticos, e com forte incentivo ao Pix. Classificação técnica: **RISCO MÉDIO**.

Recomendações ao consumidor / solicitante

- Se comprar, prefira o cartão (Stripe), que permite contestação, e confirme por telefone a existência do endereço físico declarado.
- 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 (abuse-contact@sav.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.

Ressalva: este laudo expressa **juízo técnico de risco** com base em evidências públicas coletadas passivamente em 17/11/2026; 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_checkout.txt (53316 bytes)	b96553a530be870bf1b90e26e97bd1abd895504be09afe99a494bc42a538761d
bundle_next_all.txt (1130623 bytes)	19a061fd2009cbb2d7b23dacd2182467530f5ae476c1c77999f3c649d5f7458b
cnpj_publico_61026455000170.json (1358 bytes)	6b11f56905e28a8d6692142d4d5147c30f4ba6391ae77b20c3b8d886f0822538
corpo_checkout.html (379052 bytes)	0aff171dc05710a9341dee857b3d1da73259550dfc30e02253f06eeb0f08016b
corpo_home.html (844921 bytes)	d2869d70cb86660119168263 03d50581ae2405de503ceea083259a3bc1a9394c
corpo_suporte.html (340630 bytes)	6b64d0b34518bcd1690529f9f8bf8d2f80fefabd4adb904eb482d61445d35fc9
dns_records.txt (496 bytes)	4007fb448f63deef610a5957263fd4f2d94449a07f63422b4716bd2910e2ebed
geoip.json (279 bytes)	1762ea88913db39428181fdc55e16b3f22c45a78fe3ce9decd87e7f2f387646a
headers_home.txt (1751 bytes)	6746dcde39dbc88e4836afc13d3035597122ef4193ede4c11e962005d20a69f4
rdap_raw.json (2671 bytes)	2be3e3f0069ac34867335071bc02fcafb90ea7e151217877f5563730316856f7
rdap_torracaferramentas.com.br.json (654 bytes)	350797f53ef9763d8c7698cb6690a675154cad97e98d040e31fafa5c5dfbc90a
tls_cert.txt (307 bytes)	7c20d115e083964dac1a019e7b4cc4d735e68f7687361503aff34b5630101979

- Fim do relatório -