RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

helpon.shop

Objeto investigado	helpon.shop — endereço citado em reclamação pública como loja online de onde um produto não foi recebido (gTLD .shop)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	02/08/2026 (RDAP, DNS, HTTP/TLS, geolocalização)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS
Achado central	O conteúdo do site não pôde ser verificado: a Cloudflare responde a clientes não interativos com desafio (HTTP 403, cf-mitigated: challenge). A análise limita-se, portanto, aos dados registrais e de infraestrutura
Classificação	RISCO MÉDIO — com alcance de verificação reduzido
Emissão do laudo	02/08/2026 às 01:38

1. Sumário Executivo

Este laudo documenta a análise técnica do endereço **helpon.shop**, realizada em **02/08/2026** por técnicas de OSINT e coleta passiva. Toda evidência foi preservada com hash SHA-256 (Anexo A).

É necessário declarar de saída uma **limitação de alcance**. O endereço responde, mas não entrega conteúdo a clientes não interativos: a requisição HTTPS retorna **HTTP 403** com o cabeçalho `cf-mitigated: challenge` e a página de espera "Just a moment..." da Cloudflare. Trata-se de proteção antiautomação legítima e amplamente usada por sites regulares — não é, por si, indicador de irregularidade. A consequência metodológica, porém, é que **não foi possível examinar o catálogo, os preços, os meios de pagamento, as páginas legais nem eventual CNPJ declarado**. Este laudo, portanto, não afirma nada sobre o conteúdo do site.

O que a camada registral e de infraestrutura permite verificar compõe um perfil de **baixa transparência**. O domínio foi registrado em **26/09/2025** por **um ano**, com vencimento em 26/09/2026 e última alteração em 05/01/2026. O titular **não é publicado** no RDAP, que expõe apenas o registrador (HOSTINGER operations, UAB). O DNS é servido pela Cloudflare, que também atua como proxy — de modo que o endereço IP observado (172.67.157.60) pertence à CDN e a **origem real permanece oculta**.

O achado mais relevante entre os dados disponíveis é a **ausência de registro MX**. Um endereço de comércio eletrônico sem MX não pode receber mensagens no próprio domínio — não há *contato@helpon.shop* em funcionamento —, o que restringe estruturalmente o canal de atendimento pós-venda. Também não há registro TXT: nenhuma política SPF e nenhuma verificação de plataforma publicada.

A reclamação pública que motivou a análise (Reclame AQUI, 19/02/2026) relata não recebimento de produto e falha no atendimento de uma loja online. Trata-se de **relato de consumidor**, não de prova, e nesta coleta não foi possível confrontá-lo com o conteúdo do site.

CLASSIFICAÇÃO DE RISCO **RISCO MÉDIO**

Leitura: a verificação ficou restrita à camada registral, e o que ela mostra é um endereço de **um ano de validade, titular não publicado, origem oculta e sem correio eletrônico configurado**. Isso não demonstra irregularidade — demonstra **baixa transparência**, que é o que o consumidor consegue avaliar antes de comprar.

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 código do front-end foram obtidos por requisição HTTPS de visitante comum, sem qualquer interação intrusiva, sem envio de dados pessoais e sem tentativa de compra ou de pagamento. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do endereço	RDAP do registro .shop	`rdap_raw.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS (visitante comum) — **bloqueado por desafio**	`headers_home.txt` · `headers_retry.txt`
Certificado TLS	openssl s_client + x509	`tls_cert.txt`
Hospedagem / origem	ipinfo.io + PTR reverso	`geoip.json`

Integridade	SHA-256 de cada arquivo coletado	`hash_manifest.txt`

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

Domínio	helpon.shop (gTLD .shop — GMO Registry)
Registro	**26/09/2025** · expira 26/09/2026 (validade de 1 ano)
Última alteração	05/01/2026
Idade na coleta	~10 meses
Registrador	HOSTINGER operations, UAB
Titular	**Não publicado** (o RDAP expõe apenas o registrador)
Status	client transfer prohibited
Nameservers	paislee.ns.cloudflare.com · lee.ns.cloudflare.com
Endereço IP	172.67.157.60 (AS13335 Cloudflare, Inc.) — origem real oculta pela CDN
Registro MX	**Nenhum** — o domínio não recebe e-mail
Registro TXT	Nenhum (sem SPF, sem verificação de plataforma)
Certificado TLS	Google Trust Services (WE1) · 19/07/2026 → 17/10/2026
Resposta HTTP	**403** · `cf-mitigated: challenge` · "Just a moment..."
Conteúdo do site	**Não verificável** nesta coleta passiva

Leitura técnica. Registro de um ano, titular não publicado e origem atrás de CDN são, isoladamente, escolhas comuns e legítimas. O que pesa no conjunto é a **combinação** delas com a ausência de MX em um endereço de comércio: o consumidor não dispõe, antes da compra, de nenhum dado que identifique o fornecedor nem de um canal de e-mail no próprio domínio para registrar reclamação.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Não há análise de aplicação neste laudo. A camada de conteúdo respondeu com desafio da Cloudflare (**HTTP 403**, `cf-mitigated: challenge`) tanto na coleta inicial quanto na repetição com cabeçalhos completos de navegador — comportamento coerente com proteção antiautomação. Como a metodologia deste trabalho é estritamente passiva e não contorna proteções, o exame do conteúdo **não foi realizado**.

Item verificado	Constatação
Catálogo e preços	`Não verificável`
Meios de pagamento	`Não verificável`
CNPJ declarado	`Não verificável`
Páginas legais	`Não verificável`
Canal de atendimento	`Não verificável` na página; sem MX no domínio
Edge que respondeu	`GRU (São Paulo) — cf-ray: ...-GRU`

Aspecto	Constatação
Tipo de serviço	Loja online, conforme o relato público que motivou a análise (não confirmado nesta coleta)
Tecnologia	Não determinável — conteúdo protegido por desafio
Hospedagem	Origem oculta pela Cloudflare; nenhum IP de origem exposto
Correio eletrônico	Ausente — sem MX, o domínio não recebe mensagens
Identificação do fornecedor	Não verificável — titular oculto no RDAP e conteúdo inacessível
Prazo do domínio	1 ano, vencendo em 26/09/2026
Relato público	Reclame AQUI, 19/02/2026: não recebimento de produto e falha no atendimento

Leitura técnica. É importante não converter ausência de verificação em afirmação: o desafio da Cloudflare **não é indício de irregularidade**, e milhares de lojas legítimas o utilizam. O que este laudo pode afirmar é apenas o que a camada registral mostrou — e essa camada, sozinha, não permite ao consumidor identificar o fornecedor nem localizar um canal de contato no domínio.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Ausência de registro MX em endereço de comércio eletrônico: não há e-mail de contato no próprio domínio	`dns_records.txt`	MÉDIA
2	Titular do domínio não publicado no RDAP	`rdap_raw.json`	MÉDIA
3	Domínio registrado por apenas 1 ano	`rdap_raw.json`	MÉDIA
4	Origem real oculta atrás da CDN, sem servidor ou localização identificáveis	`geoip.json`	BAIXA
5	Conteúdo não verificável por cliente não interativo, o que impede conferir identificação legal e meios de pagamento	`headers_retry.txt`	BAIXA

Síntese: nenhum indicador de severidade ALTA, 3 MÉDIA e 2 BAIXA. Como **fator de legitimidade** registra-se o certificado TLS válido e a proteção antiautomação ativa — ambos compatíveis com operação regular. O alcance da verificação foi **reduzido**, e a classificação reflete essa limitação.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em **02/08/2026**, não é possível concluir sobre o conteúdo de **helpon.shop**: o site responde a clientes não interativos com desafio da Cloudflare, e a metodologia estritamente passiva deste trabalho não contorna essa proteção. O que a camada registral mostra é um endereço com **um ano de validade, titular não publicado, origem oculta atrás de CDN e sem registro MX** — perfil de baixa transparência para um endereço de comércio, ainda que nenhum desses elementos, isoladamente, seja irregular. Classifica-se o caso como **RISCO MÉDIO com alcance de verificação reduzido**, e recomenda-se ao consumidor tratar a ausência de identificação verificável como o principal ponto de cautela. Uma reavaliação será possível caso o conteúdo se torne acessível a coleta passiva.

Recomendações ao consumidor / solicitante

- Antes de comprar, procurar na própria loja razão social, CNPJ e endereço — a ausência desses dados é o ponto de cautela verificável neste caso.
- Preferir meios de pagamento com mecanismo de contestação (cartão de crédito) a pagamento por Pix antecipado quando o fornecedor não é identificável.
- Guardar comprovante, data, valor e telas do pedido: sem CNPJ publicado, esse é o conjunto documental disponível para reclamação.
- Havendo pagamento por Pix já realizado, procurar o próprio banco quanto aos mecanismos disponíveis, observando os prazos aplicáveis, e registrar o caso no consumidor.gov.br.

Recomendações de mitigação / denúncia

- Ao responsável pelo site: publicar razão social, CNPJ e endereço em página acessível e configurar registro MX, de modo que exista um canal de e-mail no próprio domínio.
- Ao responsável pelo site: avaliar a configuração do desafio antiautomação, que hoje impede qualquer verificação externa de boa-fé sobre a identificação legal da loja.
- Ao consumidor lesado: reunir comprovante e telas do pedido como base documental de reclamação administrativa.
- Aos canais de *abuse* do registrador (Hostinger) e da Cloudflare: o material aqui preservado pode instruir comunicação, observando que ambos são provedores de infraestrutura sem responsabilidade sobre o conteúdo do cliente.

Ressalva metodológica: este laudo baseia-se em fontes abertas e reflete o estado do endereço na data indicada. A coleta foi integralmente passiva — requisições equivalentes às de um visitante comum, sem criação de conta, sem envio de dados pessoais, sem tentativa de compra e sem qualquer interação intrusiva. Não se imputa conduta ilícita a provedores de infraestrutura (registrador, hospedagem, CDN, autoridade certificadora) nem a intermediários de pagamento regulados, que não respondem pelo conteúdo publicado por seus clientes. A classificação de risco é juízo técnico sobre o conjunto de indicadores observados, não decisão judicial nem afirmação sobre a intenção de quem opera o endereço. Sinais aqui descritos como alerta podem decorrer de escolhas de configuração e ser corrigidos pelo próprio responsável pelo site.

Anexo A — Manifesto de Integridade (SHA-256)

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

Arquivo	SHA-256
`corpo_home.html (5849 bytes)`	`345037ef916eb50bf21a975486fb6f236d7d6242f24356443de58b70864dd01a`
`dns_records.txt (357 bytes)`	`f97eeed6207eae13a3e519b5bb97338b8ee39851359dd399daf326a8204977fe`
`geoip.json (288 bytes)`	`48e9a0422ad3b9f747bbb00535a28bfc3629e7021cb9a11a448ff360b63d29b9`
`headers_home.txt (2207 bytes)`	`fac9053ea9e235875a0fc255eb8c99142e37027eb6984c546ba1b9e8e46af70b`
`rdap_raw.json (4213 bytes)`	`433883c0be500cba252c8b23876a425a4ee6c864a300d7b793ce79197fe08b27`
`tls_cert.txt (300 bytes)`	`5a688345cd922b901ec09c9413caebcad0105a2934313cc0838c82f0ff9c3c95`

— Fim do relatório —