RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

saboariacaseira.netlify.app

Objeto investigado	saboariacaseira.netlify.app — página de vendas de um infoproduto sobre fabricação artesanal de sabonetes, publicada em subdomínio gratuito da Netlify
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	02/08/2026 (DNS, HTTP/TLS, geolocalização, leitura da página)
Métodos	OSINT passivo · DNS · HTTP/TLS · análise do conteúdo público
Achado central	A página exibe o selo "DESCONTO SOMENTE HOJE - 16/06/2026" com a data fixa no HTML: na coleta, 47 dias depois, o mesmo aviso de urgência continuava sendo apresentado como se fosse do dia
Classificação	**RISCO MÉDIO**
Emissão do laudo	02/08/2026 às 01:38

1. Sumário Executivo

Este laudo documenta a análise técnica do endereço **saboariacaseira.netlify.app**, realizada em **02/08/2026** por técnicas de OSINT e coleta passiva — requisições equivalentes às de um visitante comum, sem compra e sem envio de dados pessoais. Toda evidência foi preservada com hash SHA-256 (Anexo A).

O endereço **não é um domínio próprio**: é um subdomínio gratuito da plataforma Netlify. Isso tem três consequências que o consumidor precisa conhecer. Primeiro, **não existe registro RDAP/WHOIS próprio** — consultar a idade do endereço devolveria a data de registro de *netlify.app*, da plataforma, e não a de quem publicou a página. Segundo, a publicação é **instantânea e gratuita**, sem exigência de vínculo cadastral do publicador. Terceiro, o endereço pode ser abandonado sem qualquer custo. O conteúdo é servido pela infraestrutura da Netlify sobre AWS em São Paulo (PTR `ec2-54-232-119-62.sa-east-1.compute.amazonaws.com`), com certificado curinga da própria plataforma.

A página vende um método de fabricação de sabonetes artesanais com promessa de renda — "+20 Receitas de Sabonetes Infantis para Lucrar o Ano Inteiro", com encomendas "de 50 a 300+ unidades" para festas, maternidades e escolas. Os valores praticados vão de **R$ 67,00 riscado para R$ 27,00** no produto principal, com oferta adicional de **R$ 24,90 por R$ 17,80**. O pagamento é processado **fora do site**, em `pay.cakto.com.br/ix2n4rr` — plataforma de checkout de infoprodutos —, e a página declara "Garantia 7 Dias" e "Pagamento 100% Seguro".

O achado central é uma **urgência artificial demonstrável**. O topo da página exibe o selo "DESCONTO SOMENTE HOJE - **16/06/2026**", com a data **escrita fixamente no HTML**: não há no documento nenhuma função de data (`new Date`, `toLocaleDateString` ou equivalente) que a atualize. Na coleta, feita em 02/08/2026, o aviso de "somente hoje" portanto anunciava uma data **47 dias no passado** — o que demonstra que o desconto não é do dia e que a escassez comunicada não corresponde a fato.

Há ainda uma **divergência entre a garantia e o prazo de acesso**. A página promete "garantia de 7 dias incondicionais" com devolução "na hora", mas o próprio FAQ informa que "o tempo de acesso é de **5 meses**" — acesso temporário, não vitalício, o que precisa estar claro antes da compra. Não há em nenhum ponto CNPJ, razão social, endereço ou telefone; o único canal é o WhatsApp. A página também pré-conecta aos serviços `i.pravatar.cc` (gerador de avatares aleatórios) e `images.unsplash.com` (banco de imagens), além de `fast.wistia.com`, usado para o vídeo de vendas.

CLASSIFICAÇÃO DE RISCO **RISCO MÉDIO**

Leitura: um infoproduto vendido por plataforma de checkout estabelecida, mas apresentado em endereço gratuito e descartável, **sem qualquer identificação do fornecedor** e com gatilho de escassez que a própria página desmente ao trazer a data congelada no código. O risco é de **publicidade enganosa quanto à urgência e ao prazo de acesso**, mais do que de não entrega.

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
Natureza do endereço	Identificação de subdomínio de plataforma gratuita	`dados.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_records.txt`

Conteúdo / cabeçalhos	curl HTTPS (visitante comum)	`corpo_home.html · headers_home.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)

Endereço	saboariacaseira.netlify.app (**subdomínio gratuito** da plataforma Netlify)
Registro próprio	**Inexistente** — subdomínios de plataforma não têm RDAP/WHOIS próprio
Idade do endereço	**Não apurável** por fontes registrais
Titular	**Não identificável** — a plataforma não publica quem criou o subdomínio
Custo de criação	Gratuito e instantâneo, sem vínculo cadastral exigido
Endereço IP	54.232.119.62 (AS16509 Amazon) · PTR ec2-54-232-119-62.sa-east-1.compute.amazonaws.com
Localização da borda	São Paulo, Brasil (região AWS sa-east-1)
Servidor	`server: Netlify`
Registro MX	**Nenhum** — não há e-mail no endereço
Certificado TLS	DigiCert Global G2 (certificado da plataforma) · 16/02/2026 → 19/03/2027
Identificação legal	**Ausente** — sem CNPJ, razão social, endereço ou telefone
Canal de atendimento	WhatsApp (`wa.me`), único contato publicado
Checkout	`pay.cakto.com.br/ix2n4rr` (plataforma externa de infoprodutos)

Leitura técnica. Publicar em subdomínio gratuito não é irregular — é comum em testes, projetos pessoais e páginas de campanha. O que importa ao consumidor é a consequência prática: **não há nenhuma camada registral que identifique o responsável**, nem custo algum para abandonar o endereço. Quando isso se soma à ausência total de CNPJ, razão social e endereço na própria página, o comprador fica sem qualquer meio de identificar com quem contratou.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

A página é um documento estático de vendas (44,9 KB), servido pela Netlify, com vídeo hospedado no Wistia e checkout delegado à plataforma Cakto. Não há aplicação própria, área de login, formulário de dados pessoais ou endpoint de pagamento no próprio endereço — o pagamento ocorre **fora** deste site, o que reduz a superfície de risco técnico, mas não altera as questões de conteúdo descritas abaixo.

Item verificado	Constatação
Selo de urgência	`"DESCONTO SOMENTE HOJE - 16/06/2026" com data fixa no HTML`
Data da coleta	`02/08/2026 — 47 dias após a data anunciada como "hoje"`
Atualização por script	`Nenhuma — sem new Date ou toLocaleDateString no documento`
Preço principal	`R$ 67,00 riscado → R$ 27,00`
Oferta adicional	`R$ 24,90 → R$ 17,80, "pagamento único"`
Garantia declarada	`"Garantia de 7 dias incondicionais" com devolução "na hora"`
Prazo de acesso	`"5 meses inteiros" (FAQ) — acesso temporário, não vitalício`
Checkout	`Externo: pay.cakto.com.br/ix2n4rr`
Promessa comercial	`Encomendas "de 50 a 300+ unidades" para festas, maternidades, escolas e empresas`
Serviços pré-conectados	`i.pravatar.cc (avatares aleatórios) · images.unsplash.com (banco de imagens) · fast.wistia.com (vídeo)`

Aspecto	Constatação
Tipo de serviço	Infoproduto (curso digital) sobre fabricação de sabonetes artesanais, com promessa de renda
Tecnologia	Página estática servida pela Netlify · vídeo Wistia · ícones Material Symbols
Hospedagem	Netlify sobre AWS sa-east-1 (São Paulo) — publicação gratuita e instantânea
Correio eletrônico	Ausente — subdomínio de plataforma, sem MX
Identificação do fornecedor	Nenhuma — sem CNPJ, razão social, endereço ou telefone
Canal de atendimento	Apenas WhatsApp
Meio de pagamento	Delegado à plataforma Cakto — **fator de legitimidade**, por haver intermediário identificável
Documentos legais	Nenhuma página de termos ou de privacidade encontrada
Relato público	Reclame AQUI, 30/04/2026: reclamação contra a processadora citando este endereço

Leitura técnica. Não há coleta indevida de dados nem fluxo de pagamento próprio: o checkout é delegado a uma plataforma estabelecida, que mantém identificação do vendedor em seus próprios registros e oferece canal de reembolso — o que é um **fator relevante de legitimidade**. O risco concentra-se no **conteúdo publicitário**: a escassez anunciada é comprovadamente artificial, o prazo de acesso real (5 meses) aparece apenas no FAQ, e o endereço não permite identificar o fornecedor. São exatamente os pontos que o responsável pela página pode corrigir sem alterar o produto.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Selo "DESCONTO SOMENTE HOJE" com data fixa no HTML, 47 dias anterior à coleta, sem qualquer script que a atualize	`corpo_home.html`	ALTA

2	Nenhuma identificação legal do fornecedor (sem CNPJ, razão social, endereço ou telefone)	`corpo_home.html`	ALTA
3	Endereço em subdomínio gratuito de plataforma: sem registro próprio, sem titular apurável e sem custo de abandono	`dados.json` · `dns_records.txt`	MÉDIA
4	Garantia anunciada no topo sem menção ao prazo de acesso real de 5 meses, informado apenas no FAQ	`corpo_home.html`	MÉDIA
5	Nenhuma página de termos de uso ou política de privacidade	`corpo_home.html`	MÉDIA
6	Atendimento restrito ao WhatsApp, sem e-mail nem telefone fixo publicados	`corpo_home.html`	BAIXA

Síntese: 2 indicadores de severidade ALTA, 3 MÉDIA e 1 BAIXA. Como **fator de legitimidade** registra-se a delegação do pagamento a plataforma de checkout estabelecida (Cakto), que mantém cadastro do vendedor e canal próprio de reembolso — elemento ausente em páginas que cobram por Pix direto.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em **02/08/2026**, **saboariacaseira.netlify.app** é uma página de vendas de infoproduto cujo **pagamento é processado por plataforma estabelecida** — o que a distingue favoravelmente de endereços que cobram por Pix direto a recebedor não identificado. O risco não está no meio de pagamento, e sim no **conteúdo publicitário e na ausência de identificação**: o selo "DESCONTO SOMENTE HOJE" traz a data **16/06/2026 fixa no código**, exibida sem alteração 47 dias depois, de modo que a urgência comunicada não corresponde a fato; o prazo real de acesso (5 meses) aparece só no FAQ, enquanto o topo comunica apenas garantia; e não há CNPJ, razão social, endereço ou telefone em nenhum ponto, em endereço gratuito que não permite apurar titularidade. Classifica-se o caso como **RISCO MÉDIO**. Todos os pontos são corrigíveis pelo próprio responsável — remover ou automatizar a data, informar o prazo de acesso junto ao preço, publicar identificação legal e termos de uso mudariam substancialmente esta classificação.

Recomendações ao consumidor / solicitante

- Desconsiderar o aviso de "desconto somente hoje": a data está fixa no código da página e não corresponde ao dia da visita.
- Confirmar, **antes de pagar**, o prazo real de acesso ao conteúdo — a página anuncia garantia no topo, mas o acesso informado no FAQ é de 5 meses.
- Guardar o comprovante e o e-mail da plataforma de checkout: é por ela que o pedido de reembolso dentro dos 7 dias deve ser feito, com registro rastreável.
- Tratar promessas de renda ("encomendas de 50 a 300+ unidades") como projeção comercial, não como resultado assegurado.

Recomendações de mitigação / denúncia

- Ao responsável pela página: remover a data fixa do selo de urgência ou torná-la dinâmica, e publicar o prazo de acesso de 5 meses junto ao preço, não apenas no FAQ.
- Ao responsável pela página: publicar identificação legal (razão social, CNPJ), termos de uso e política de privacidade, e considerar a migração para domínio próprio, que permite verificação registral.
- Ao consumidor lesado: acionar primeiro o canal de reembolso da plataforma de checkout, que mantém o cadastro do vendedor, antes de recorrer a reclamação administrativa.
- Aos canais de *abuse* da plataforma de hospedagem (Netlify) e da plataforma de checkout: o material aqui preservado pode instruir comunicação, observando que ambas são provedoras sem responsabilidade sobre o conteúdo publicado pelo 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
bundle_js.txt (25471 bytes)	e89b43994dc02b13d2d09589fc4015552c9c5ff27ec0fb305118ebc1fc376768
corpo_home.html (45099 bytes)	bb80f521b7b5ba56b7163c71763f2102036f31d196f0322b1be197a02a3919c0
dns_records.txt (300 bytes)	59c69d5968f35a62be11a8837c957d4b5207452fa56ef15f576d0089d4d7b8ac
geoip.json (335 bytes)	df5b98edc54c1ec6b02e86d7df5fafcdd3986298e0aadc1e978fb0429f4b4f9a
headers_home.txt (475 bytes)	630bd5ed0bae4634cd763989d614c2b9d4f86682710e2ef4221fce82fa05dd3e
rdap_raw.json (0 bytes)	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
tls_cert.txt (396 bytes)	33ee7eb1f5ad2672d809467de1d194d778be7c6c9b325499af7911250723aeba

— Fim do relatório —