

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

acheieencantei.com

Objeto investigado	acheieencantei.com - loja Shopify de bonecas “bebê reborn” hiper-realistas
Natureza	Verificação de identificação do fornecedor e de legitimidade da loja
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	Domínio de **5 dias** vendendo bonecas de R$ 300 a R$ 1.339 com rodapé inteiramente de modelo — CNPJ 00.000.000/0001-00, “Rua 0”, telefone (11) 99999-9999 e e-mail “suporte@sualoja.com”
Classificação	**RISCO ALTO**
Emissão do laudo	18/11/2026 as 00:54

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **acheieencantei.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, na Shopify e atrás de desafio anti-robô (lida com navegador headless), oferece bonecas “bebê reborn” de silicone sólido entre R$ 299 e R$ 1.339,90, com descontos de até 43%, frete grátis, 6x sem juros e cupom “Primeira15”.

O domínio foi registrado em 12/11/2026, cinco dias antes da coleta. Nenhum dado de identificação é real: o rodapé traz “© 2023 Minhaloja”, endereço “Rua 0, 232”, CEP inválido (010010-010), **CNPJ 00.000.000/0001-00**, telefone (11) 99999-9999 e e-mail suporte@sualoja.com — textos de exemplo do tema que não foram substituídos.

O bloco “Loja Verificada” exibe selos do Reclame Aqui, Google Safe Browsing e SSLShopper que apenas apontam para as páginas genéricas desses serviços.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: uma loja que vende produtos de ticket alto sem nenhum dado verdadeiro de identificação, em domínio de cinco dias, não oferece ao comprador qualquer meio de responsabilizar o vendedor (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	acheieencantei.com
Registro	12/11/2026 · expira 12/11/2027 · **5 dias** antes da coleta
Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)

Registrador	GoDaddy.com, LLC · abuse@godaddy.com
Servidores de nome	ns59.domaincontrol.com · ns60.domaincontrol.com
DNS - A	23.227.38.32 · sem MX
Hospedagem	AS13335 Cloudflare, Inc. · Ottawa/CA · PTR/hostname `myshopify.com` · cabeçalho `server: cloudflare`
Certificado TLS	Let's Encrypt (YE2) · emitido em 12/11/2026 · válido até 10/02/2027
Loja Shopify	`5q86tn-9t.myshopify.com` · moeda BRL
Dados no rodapé	“© 2023 Minhaloja” · “Rua 0, 232, Centro, São Paulo - SP, CEP 010010-010” · **CNPJ 00.000.000/0001-00** · “(11) 99999-9999” · “suporte@sualoja.com” — todos de modelo

Leitura: domínio de 5 dias com titular oculto (GoDaddy), DNS GoDaddy, sem MX, site servido pela Shopify; certificado TLS emitido no dia do registro.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Loja Shopify com tema de nicho reborn, app de tabela de medidas hospedado no Heroku e Google Analytics. As páginas de política padrão da Shopify estão vazias.

Aspecto	Constatação
Pagamento	Parcelamento em até 12x (6x sem juros anunciado); meios não detalhados
Fornecedor	Inexistente: todos os dados do rodapé são de exemplo
Contato	Só WhatsApp (link genérico) e e-mail de modelo
Selos	“Loja Verificada” com links genéricos

Leitura: com CNPJ zerado, endereço fictício e telefone 99999-9999, não há fornecedor identificável.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Domínio de 5 dias, titular oculto	`rdap_raw.json`	ALTA
2	CNPJ 00.000.000/0001-00, endereço “Rua 0” e telefone de exemplo	`corpo_home_chrome.html`	ALTA
3	E-mail “suporte@sualoja.com” e “© 2023 Minhaloja” (modelo não personalizado)	`corpo_home_chrome.html`	ALTA
4	Selos de verificação decorativos	`corpo_home_chrome.html`	MEDIA
5	Produtos de R$ 300 a R$ 1.339 com descontos de até 43%	`corpo_home_chrome.html`	MEDIA

Síntese: cinco indicadores, três de severidade alta. O padrão é típico de loja montada às pressas para campanha de anúncios.

6. Conclusão Técnica e Recomendações

A acheieencantei.com tem cinco dias de existência e nenhum dado verdadeiro de identificação — CNPJ, endereço, telefone e e-mail são textos de exemplo do tema. Classificação técnica: **RISCO ALTO**.

Recomendações ao consumidor / solicitante

- Não compre em loja cujo rodapé exibe CNPJ 00.000.000/0001-00 ou telefone (11) 99999-9999.
- 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@godaddy.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
corpo_home_chrome.html (1029144 bytes)	e0f9bb804f72ffc3e641ad7d1fa0134ed6579bf083097807c8d2d31a326ac89c
corpo_home.html (8718 bytes)	74aa74b0196a5b5a160508b98e3ebe6d24111a316d44d6f32efec020c544b0f7
corpo_policies_contact_information.html (174169 bytes)	7c4a8cfe71e4e2b13ee52967cc2dead03562088ff4cf7fb613029436f81f2ce4
corpo_policies_refund_policy.html (174163 bytes)	c97f12351ece583da18edcfb2ffbd92915fa49678e1bc2aa1430d286a080cec2
dns_records.txt (353 bytes)	8c5496dc6ebcaff873f476735ef5ae47a7727803a8f8eff33bd4d1a93c58abcc
geoip.json (301 bytes)	304ec09a3057cc350f6451a92a83a2e15840cd1405f8b92b69213e5de11fc678
headers_home.txt (1791 bytes)	ad8960d5e380ab47432d48a6646dc5149c9df4ea0262927e11c7448bbfa35fa0
rdap_raw.json (2697 bytes)	d2fd48378449e07029b9371fe79879ebdeade3198012f08c8584f271d90097c9
tls_cert.txt (303 bytes)	2b7b0770f0f24ca98299bf21f62c3c069b6dbba7f1e2552e851574c7f8f79d66

- Fim do relatório -