RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

dudabeautyshop.com

Objeto investigado	dudabeautyshop.com - loja de cosméticos e "beauty tech" que se apresenta sob a marca "Luna Beauty" (gTLD .com)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	02/09/2026 (RDAP, DNS, HTTP/TLS, geolocalização, bundle JS)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do bundle
Achado central	Loja que vende ao consumidor brasileiro **sem qualquer identificação de fornecedor** - sem CNPJ, razão social, endereço, telefone ou e-mail -, com **marca exibida ("Luna Beauty") diferente do domínio** e páginas legais que não entregam conteúdo
Classificação	**RISCO ALTO**
Emissão do laudo	02/09/2026 as 22:14

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **dudabeautyshop.com**, realizada em **02/09/2026** 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 envio de dados pessoais e sem qualquer compra ou pagamento. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

O domínio **está no ar** e entrega uma loja de cosméticos intitulada **"Luna Beauty | Skincare de Luxo: Pele, Cabelo e Tecnologia"**, descrita como "skincare de luxo com curadoria coreana [...] séruns, PDRN, peptídeos e dispositivos LED com frete grátis para todo o Brasil". O catálogo, extraído do próprio código da aplicação, inclui itens como "ampola coreana colágeno peptídeos", "máscara LED regenmask", "kit pele de vidro coreana" e "gokoco massageador LED".

O primeiro achado é a **divergência entre o domínio e a marca**. O consumidor compra em `dudabeautyshop.com`, mas toda a comunicação do site - título, descrição, metadados sociais e identidade visual - é de **"Luna Beauty"**. Não há, na página, qualquer explicação para essa diferença: nenhum aviso de mudança de marca, de grupo empresarial ou de nome fantasia. Do ponto de vista do consumidor, o endereço onde o dinheiro é enviado e o nome de quem recebe **não coincidem**.

O achado central, porém, é mais grave: a **ausência completa de identificação do fornecedor**. A legislação brasileira de comércio eletrônico exige que o site informe de forma ostensiva o **CNPJ, a razão social e o endereço físico** do fornecedor, além de canal de atendimento. Na coleta, **nenhum desses dados foi encontrado**: não há CNPJ, razão social, endereço, telefone nem sequer um e-mail de contato em qualquer ponto do conteúdo servido. As rotas de `/politica-privacidade`, `/politica-reembolso` e `/contato` existem no roteador da aplicação, mas **respondem sempre o mesmo esqueleto de página, sem conteúdo** - são links que não levam a documento algum. O domínio também **não tem MX próprio**: o registro de e-mail aponta para um endpoint de recebimento da Amazon, não para uma caixa institucional divulgada ao cliente.

A infraestrutura é a de uma operação **montada rapidamente e desenhada para tráfego pago**. O domínio foi registrado em **20/06/2026** na NameCheap, com **titular oculto**, e opera atrás da Cloudflare, que mascara o endereço real da hospedagem. A aplicação é um SPA React gerado na plataforma **Lovable** (referência a `lovable.dev` no bundle) com back-end **Supabase**, e carrega simultaneamente **pixel do TikTok**, **pixel do Facebook** e o rastreador de campanhas **utmify** - conjunto típico de loja alimentada por anúncios em redes sociais. O bundle ainda expõe rotas administrativas `/admin/zedy-stores`, `/admin/atendimento` e `/admin/blog-seo`, sugerindo que a loja é **uma instância entre várias** de uma mesma plataforma multi-loja.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: uma loja que vende ao consumidor brasileiro **sem informar CNPJ, razão social, endereço, telefone ou e-mail**, cuja marca não corresponde ao domínio, cujas páginas legais não entregam conteúdo e cujo titular está oculto, oferece **risco elevado**. Recomenda-se **não comprar sem antes obter a identificação do fornecedor** (Seções 5 e 6).

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 (Verisign / .com - registrador NameCheap)	`rdap_raw.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME) via 1.1.1.1	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS (visitante comum)	`corpo_home.html` · `headers_home.txt`
Rotas legais	curl HTTPS de /politica-privacidade, /politica-reembolso e /contato	`legal_politica-privacidade.html` · `legal_politica-reembolso.html` · `legal_contato.html`
Aplicação (front-end)	Download do bundle JS e mapeamento de rotas e integrações	`bundle_js.txt`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · PTR reverso	`geoip.json`

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

Domínio	dudabeautyshop.com (gTLD .com - Verisign)
Registro	**20/06/2026** · expira 20/06/2027 (validade de 1 ano)
Idade na coleta	Cerca de **2 meses e meio**
Titular	**Oculto** (o RDAP expõe apenas o registrador)
Registrador	NameCheap, Inc. (IANA 1068) · abuse@namecheap.com
Status	clientTransferProhibited
Servidores de nome	alice.ns.cloudflare.com · amit.ns.cloudflare.com
DNS - A	172.67.132.68 · 104.21.4.165 (+ AAAA) - faixas Cloudflare
DNS - MX	`inbound-smtp.sa-east-1.amazonaws.com` - **endpoint de recebimento**, não caixa institucional divulgada
Hospedagem	AS13335 Cloudflare, Inc. - **origem real oculta** pelo proxy
Aplicação	SPA React/Vite gerada na plataforma **Lovable** · back-end **Supabase**
Rastreadores	**Pixel do TikTok** · **Pixel do Facebook** · **utmify** (rastreio de campanhas)
Certificado TLS	CN=dudabeautyshop.com · emissor Google Trust Services WE1 (DV) · válido 18/08/2026-16/11/2026
Identificação do fornecedor	**Inexistente** - sem CNPJ, razão social, endereço, telefone ou e-mail

Leitura técnica. Titular oculto, validade de 1 ano, proxy da Cloudflare diante da origem e publicação em plataforma geradora de sites compõem um perfil de **baixa rastreabilidade do responsável** e de **baixo custo de descarte**: encerrar a operação e reabrir sob outro domínio exige pouco mais que um novo registro. O certificado DV gratuito comprova apenas o controle do domínio, **não a identidade de qualquer entidade**. Não se imputa conduta à NameCheap, à Cloudflare, à Lovable, ao Supabase ou à Amazon, meros provedores de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site é uma **loja virtual de cosméticos** implementada como aplicação React de página única (SPA), gerada na plataforma Lovable, com dados servidos por um projeto Supabase. Como toda a navegação ocorre no navegador, **qualquer endereço do site devolve o mesmo esqueleto HTML** - o que explica por que as rotas legais não entregam documento próprio ao visitante nem aos mecanismos de busca. O catálogo e o fluxo de compra (`/checkout`, `/obrigado`) foram identificados no bundle JavaScript.

Exigência legal ao e-commerce	Situação verificada em dudabeautyshop.com
CNPJ do fornecedor em local de destaque	**Ausente** - nenhum CNPJ em qualquer ponto do conteúdo
Razão social / nome empresarial	**Ausente** - apenas a marca "Luna Beauty"
Endereço físico do fornecedor	**Ausente**
Canal de atendimento (telefone / e-mail)	**Ausente** - rota `/contato` sem conteúdo
Política de privacidade acessível	Rota existe, mas **devolve página vazia**
Política de troca / reembolso acessível	Rota existe, mas **devolve página vazia**
Correspondência entre marca e domínio	**Divergente** - "Luna Beauty" × `dudabeautyshop.com`

Aspecto	Constatação
Tipo de site	Loja virtual de cosméticos e dispositivos de beleza, conteúdo em PT-BR, frete "grátis para todo o Brasil"
Marca exibida	**"Luna Beauty"** - **não corresponde** ao domínio `dudabeautyshop.com`
Identificação do fornecedor	**Inexistente** - sem CNPJ, razão social, endereço, telefone ou e-mail
Páginas legais	Rotas `/politica-privacidade`, `/politica-reembolso` e `/contato` **devolvem página vazia**
Tecnologia	SPA React gerada na plataforma **Lovable**, back-end **Supabase**, atrás da Cloudflare
Rastreadores de anúncios	Pixel do **TikTok**, pixel do **Facebook** e **utmify** - perfil de loja movida a tráfego pago
Indício de multi-loja	Rotas `/admin/zedy-stores`, `/admin/atendimento`, `/admin/blog-seo` no bundle
Titular do domínio	**Oculto** no RDAP; origem mascarada por proxy
E-mail institucional	Sem caixa divulgada; MX aponta para endpoint de recebimento da Amazon
Produtos	Cosméticos "coreanos", séruns, PDRN, peptídeos e dispositivos LED - categoria sujeita a regras sanitárias de importação e registro

Leitura técnica. A tabela acima é o núcleo do caso. Não se trata de um detalhe formal: a identificação do fornecedor é **o que torna possível reclamar, trocar, devolver ou processar**. Sem CNPJ, sem razão social, sem endereço e sem telefone, o consumidor que pagar e não receber - ou receber produto diverso - **não tem contra quem se voltar**: não há a quem enviar notificação, nem parte a indicar em reclamação no consumidor.gov.br ou em ação judicial. A divergência entre a marca "Luna Beauty" e o domínio `dudabeautyshop.com` agrava o quadro, porque nem sequer o nome sob o qual buscar informação é estável. O conjunto de pixels de anúncios (TikTok, Facebook, utmify) indica que o tráfego vem de campanhas pagas em redes sociais - modelo que permite alcançar rapidamente grande público antes de qualquer reputação se formar. Registre-se que **nada nas evidências demonstra que os produtos não sejam entregues**; o que se documenta aqui é a **impossibilidade de identificar e responsabilizar o**

fornecedor, que é o risco.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Ausência total de identificação do fornecedor: sem CNPJ, razão social, endereço, telefone ou e-mail	`corpo_home.html` · `bundle_js.txt`	ALTA
2	Rotas de política de privacidade, reembolso e contato devolvem página vazia, sem documento legal	`legal_politica-privacidade.html` · `legal_politica-reembolso.html` · `legal_contato.html`	ALTA
3	Marca exibida ("Luna Beauty") diverge do domínio, sem qualquer explicação ao consumidor	`corpo_home.html`	ALTA
4	Titular do domínio oculto no RDAP e origem da hospedagem mascarada por proxy	`rdap_raw.json` · `geoip.json`	ALTA
5	Domínio recente (20/06/2026) com validade de 1 ano, publicado em plataforma geradora de sites	`rdap_raw.json` · `bundle_js.txt`	MEDIA
6	Loja movida a tráfego pago: pixels de TikTok e Facebook mais rastreador utmify	`corpo_home.html` · `bundle_js.txt`	MEDIA
7	Indício de operação multi-loja padronizada (rotas /admin/zedy-stores no bundle)	`bundle_js.txt`	MEDIA
8	Sem caixa de e-mail institucional divulgada; MX aponta para endpoint de recebimento genérico	`dns_records.txt`	BAIXA
9	Venda de cosméticos importados e dispositivos, categoria sujeita a exigências sanitárias, sem qualquer dado regulatório	`corpo_home.html`	BAIXA
10	Promessa de "frete grátis para todo o Brasil" sem política de entrega acessível	`corpo_home.html`	BAIXA

Síntese: 4 indicadores de severidade ALTA, 3 MEDIA e 3 BAIXA. **Nenhum fator de legitimidade** (CNPJ, razão social, endereço, canal de atendimento identificável, política de troca acessível) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em **02/09/2026**, conclui-se que **dudabeautyshop.com** apresenta **risco alto ao consumidor**. A loja vende cosméticos e dispositivos de beleza ao público brasileiro sob a marca "Luna Beauty" - que **não corresponde ao próprio domínio** - e **não informa qualquer dado de identificação do fornecedor**: não há CNPJ, razão social, endereço físico, telefone ou e-mail em nenhum ponto do conteúdo servido. As rotas de política de privacidade, de reembolso e de contato existem, mas devolvem página vazia. Some-se o titular oculto no registro, a origem mascarada por proxy, o domínio recente publicado em plataforma geradora de sites e o conjunto de pixels de anúncios que indica captação por tráfego pago em redes sociais. Não se afirma que os produtos deixem de ser entregues; o que as evidências demonstram é que, **se algo der errado, o consumidor não tem como identificar nem responsabilizar quem recebeu seu dinheiro**. Classifica-se o caso como **RISCO ALTO**.

Recomendações ao consumidor / solicitante

- **Não concluir compra** enquanto o site não informar **CNPJ, razão social e endereço** do fornecedor - dados obrigatórios no comércio eletrônico brasileiro.
- Antes de qualquer pagamento, exigir a identificação por escrito e **conferir o CNPJ na consulta pública da Receita Federal**, verificando se a atividade e a situação cadastral são compatíveis com a loja.

- Desconfiar quando a **marca exibida difere do domínio** sem explicação: o nome pelo qual você buscaria reputação não é o mesmo para onde o dinheiro vai.
- Preferir **cartão de crédito** a Pix em lojas desconhecidas: o cartão permite contestação junto à administradora; o Pix, na prática, é irreversível.
- Se já houve pagamento: acionar o banco (e o mecanismo **MED** do Pix, se for o caso), reunir prints do anúncio, do site e do comprovante, e registrar reclamação em **consumidor.gov.br** e Boletim de Ocorrência.

Recomendações de mitigação / denúncia

- Denunciar o domínio aos canais de abuse do registrador (`abuse@namecheap.com`), da Cloudflare e da plataforma de publicação (Lovable), anexando este laudo.
- Reportar os anúncios às plataformas de mídia (**Meta** e **TikTok**), que exigem identificação do anunciante e podem suspender campanhas de lojas sem dados de fornecedor.
- Comunicar ao **Procon** a oferta ao consumidor brasileiro sem os dados de identificação exigidos pela legislação de comércio eletrônico.
- Preservar este relatório e as evidências (pasta `evidencias/`, com hashes SHA-256) para eventual uso administrativo ou judicial.

*Ressalva metodológica: este laudo baseia-se em fontes abertas e reflete o estado do domínio na data indicada (coleta em 02/09/2026). A classificação expressa um **juízo técnico de risco** e não substitui decisão de autoridade policial, administrativa ou judicial. **Não se afirma que produtos deixem de ser entregues** nem se imputa conduta criminosa a quem opera o site: o que se documenta é a ausência verificável dos dados de identificação exigidos e a consequente impossibilidade de responsabilização. Não se imputa conduta ilícita aos provedores de infraestrutura citados (NameCheap, Cloudflare, Lovable, Supabase, Amazon).*

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 (105601 bytes)`	`671f383b4712892393153e807920dc40f94017342cf3a44d4c27fe194c2b5a35`
`corpo_home.html (7186 bytes)`	`1913bfb3ad3a85ad657be37382e14af174b7c27977c319b58bcb41bcbbe0b130`
`dns_records.txt (517 bytes)`	`5662a039ea4f40731a922751ad4d581cbf8d95e4cebe9d3534961cb842c7b40c`
`geoip.json (288 bytes)`	`ec71bc49b5110aaa59231a60f374f57bbad3f93d891c1597c76c4c9ea1411510`
`headers_home.txt (597 bytes)`	`b73280d087cbaff4adff9a8fc337ff5abf12d5faffb73ffc488ea52df2fe8d6c`
`rdap_raw.json (2620 bytes)`	`1eebf4c65dd7b04e5fc0875b872dd72c37d090d967bb2b33e30c9a5cd435eeb3`
`tls_cert.txt (307 bytes)`	`d3d1571ae8177a66be0d192e2dc9bf075d0e9e9b6abdea7abb5d2c2fd3962a50`

- Fim do relatório -