RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

soyebeauty.com

Objeto investigado	soyebeauty.com — loja virtual de cosméticos coreanos "Soye Korean Beauty" (gTLD .com)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	15/06/2026 (RDAP, DNS, HTTP/TLS, geolocalização, catálogo, imagens)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise de conteúdo, catálogo e metadados
Achado central	E-commerce sem identificação de operador (sem CNPJ/endereço), catálogo e imagens clonados de loja-irmã/marketplaces
Classificação	**RISCO ALTO**
Emissão do laudo	15/06/2026 às 02:14

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **soyebeauty.com**, realizada em **15/06/2026** por técnicas de OSINT (inteligência de fontes abertas) e análise passiva — requisições equivalentes às de um visitante comum e consultas a bases públicas, sem qualquer interação intrusiva ou exploração de vulnerabilidade. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (cadeia de custódia).

O domínio **está no ar** e entrega uma **loja virtual de cosméticos coreanos (K-beauty)** em português (marca exibida "Soye Korean Beauty"), construída sobre a plataforma **Shopify** (`ka2pc0-ub.myshopify.com`) e servida atrás da **Cloudflare**. A loja anuncia produtos de marcas reais de skincare coreano (COSRX, Anua, Beauty of Joseon, Medicube, Laneige, entre outras), com preços em **reais (BRL)**, pagamento por **cartão** no checkout hospedado da Shopify e público-alvo declaradamente brasileiro (idioma pt-BR, moeda BRL).

O conjunto de sinais é o de uma **loja "fantasma"/dropshipping replicada em escala, sem lastro verificável**: domínio **recém-registrado** (14/01/2026) na Hostinger, e — no próprio site — **nenhuma identificação do operador** (sem CNPJ, razão social, endereço físico, e-mail ou telefone; a página de "Contato" é apenas um formulário genérico), **ausência das políticas de troca/devolução e de entrega** exigidas do comércio eletrônico brasileiro, e fortes indícios de **conteúdo clonado**: o catálogo carrega a marca de uma **loja-irmã** ("Yuna Korean Beauty", em 220 dos 248 produtos) e as imagens reaproveitam arquivos de **marketplaces** (Amazon, Mercado Livre) e de outras lojas. O tema da loja preserva ainda **textos em espanhol** não traduzidos ("Añadir al carrito", "Envío gratis", "Tu carrito expira en…") e um **contador regressivo de carrinho** (urgência/escassez artificial).

Ponto juridicamente relevante: o comércio eletrônico no Brasil é obrigado a exibir, em local de destaque, **CNPJ/CPF, razão social e endereço físico do fornecedor** (Decreto 7.962/2013 e art. 33 do CDC) e a assegurar o **direito de arrependimento** em 7 dias. A loja **não apresenta qualquer dessas informações obrigatórias** nem política de devolução, configurando, no mínimo, **irregularidade** e impossibilidade de responsabilizar quem a opera.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: uma loja que recebe pagamentos e dados pessoais **sem identificar quem a opera, sem políticas de troca/devolução e exibindo catálogo e fotos copiados de terceiros** oferece ao consumidor **risco elevado** de não entrega do produto, entrega divergente ou ausência de suporte pós-venda, sem responsável localizável. Recomenda-se **não comprar e não fornecer dados de cartão** antes de confirmar a idoneidade (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 HTTPS e os cabeçalhos foram obtidos por requisição equivalente à de um navegador comum; o catálogo público (`products.json`) e os assets de imagem foram baixados e analisados com `exiftool`. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (Verisign / .com — registrador Hostinger)	`rdap_raw.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns.txt`
Conteúdo / cabeçalhos	curl HTTPS (visitante comum)	`corpo.html · headers.txt`
Certificado TLS	openssl s_client / x509	`tls.txt`

Geolocalização do IP	ipinfo.io · ip-api.com · PTR	`geoip.txt`
Catálogo / preços	Endpoint público products.json (Shopify)	`products.json`
Página de contato	Download /pages/contact	`pagina_contato.html`
Imagens / metadados	Download de assets · exiftool -a -G1 -s	`imagens/ · metadata_exiftool.txt`
Integridade	sha256sum de todos os artefatos	`hash_manifest.txt`

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

Domínio	soyebeauty.com (gTLD .com — Verisign)
Registro	**14/01/2026** · expira 14/01/2027 (validade de 1 ano)
Idade na coleta	**~5 meses** — domínio recente
Titular	**Oculto** (RDAP expõe apenas o registrador)
Registrador	HOSTINGER operations, UAB (IANA 1636)
Status	clientTransferProhibited
Servidores de nome	ns1 / ns2.dns-parking.com (Hostinger)
DNS — A	23.227.38.65 (Shopify, via Cloudflare anycast) · sem AAAA
DNS — MX / TXT	mx1/mx2.hostinger.com · SPF include:_spf.mail.hostinger.com
www	CNAME → shops.myshopify.com (loja Shopify)
Plataforma	Shopify — loja ka2pc0-ub.myshopify.com (cabeçalho `powered-by: Shopify`)
Hospedagem (borda)	AS13335 Cloudflare, Inc. — proxy/CDN à frente da infraestrutura Shopify
Geolocalização do IP	Anycast Cloudflare/Shopify (PTR myshopify.com) — não revela localização física
Servidor web	Server: cloudflare · HTTP/2 200 · content-language pt-BR · servido ao Brasil (country;desc="BR")
Certificado TLS	CN=soyebeauty.com · emissor Let's Encrypt E7 (DV) · válido 19/04/2026–18/07/2026
Série / Fingerprint	05CCD88E0E8FDF82…CB09 · SHA-256 F5:6D:A9:44:DE:5E:F0:9F:9E:02:BD:4C:DF:1C:3F:6F…

Leitura técnica. Registro recente, validade de 1 ano e titular oculto compõem um perfil de **baixa rastreabilidade do responsável**. O domínio foi registrado na **Hostinger** e aponta para uma **loja Shopify** (www → shops.myshopify.com) servida atrás da **Cloudflare**, que oculta o IP de origem. O certificado DV gratuito (Let's Encrypt) comprova apenas o controle do domínio, **não a identidade de qualquer empresa**. Shopify, Cloudflare e Hostinger são **provedores de infraestrutura** neutros, usados também por inúmeras lojas legítimas; não se lhes imputa qualquer conduta — o objeto da análise é exclusivamente o site investigado.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site entrega uma **loja virtual de cosméticos coreanos** em pt-BR sobre **Shopify**, com catálogo de **248 produtos** de skincare/maquiagem de marcas reais (COSRX, Anua, Beauty of Joseon, Medicube, Laneige, Banila Co, Skin1004 etc.) e preços de **R$ 49,90** a valores anômalos (um "produto" digital em espanhol — *"Guía Secreta…"* — listado a R$ 31.774,05, resíduo do template de origem). O checkout é o **hospedado da própria Shopify**; o rodapé anuncia apenas **bandeiras de cartão** (Visa, Mastercard, Amex, Elo, Diners, Discover, JCB) — **não há PIX nem boleto**. O catálogo (`products.json`) revela que **220 dos 248 produtos** trazem o fabricante/marca **"Yuna Korean Beauty"** (e outros "Lumi Korean Beauty"), denotando um **catálogo importado de loja-irmã** dentro de uma mesma rede de lojas Shopify.

Aspecto	Constatação
Tipo de serviço	Loja virtual (e-commerce) de cosméticos coreanos — "Soye Korean Beauty"
Plataforma	Shopify (ka2pc0-ub.myshopify.com) atrás de Cloudflare · tema com app de bundles "Kaching" e carteiras Apple/Google Pay
Meio de pagamento	Checkout hospedado da Shopify — apenas cartões (Visa, Mastercard, Amex, Elo, Diners, Discover, JCB); sem PIX/boleto
Intermediário (gateway)	Processamento de pagamentos da Shopify (não nomeado no front-end)
Dados coletados	No cadastro/checkout: nome, e-mail, telefone, endereço de entrega e dados de cartão (via checkout Shopify)
Identificação do operador	**Ausente** — sem CNPJ, razão social, endereço físico, e-mail ou telefone em qualquer página; "Contato" é só um formulário
Políticas legais	**Incompletas** — só "política de privacidade"; **sem** política de troca/devolução, reembolso ou envio (404)
Catálogo / imagens	Catálogo marcado como "Yuna Korean Beauty" (220/248) — loja-irmã; imagens com nomes de Amazon (61F9V2PYkaL) e Mercado Livre (D_NQ_NP_2X_…) e de terceiros ("KOUMITWO")
Sinais de template	Textos em espanhol não traduzidos ("Añadir al carrito", "Envío gratis", "Tu carrito expira en…"); produtos duplicados com sufixo "-copia"
Urgência / escassez	Contador regressivo de carrinho ("expira em 5 min", esvazia ao zerar) e selos "VENDIDO"

Leitura técnica. O risco aqui não está na plataforma (Shopify é amplamente usada por lojas legítimas), mas no **conjunto de sinais de loja "fantasma"/dropshipping**: ausência total de identificação e de políticas obrigatórias, catálogo e fotos copiados de uma loja-irmã ("Yuna Korean Beauty") e de marketplaces, tema multilíngue não localizado e gatilhos de urgência artificiais. Esse padrão — várias lojas Shopify quase idênticas, trocando apenas o nome (Soye / Yuna / Lumi "Korean Beauty"), criadas em domínios recém-registrados — é típico de **redes de lojas descartáveis**, em que o consumidor paga e frequentemente não recebe o produto, recebe item diferente do anunciado ou fica sem suporte. A vantagem relativa, frente a golpes de PIX direto, é que o pagamento por **cartão no checkout Shopify** admite contestação (chargeback) junto à operadora.
Imagens. Dos 46 arquivos gráficos baixados, o Shopify removeu os metadados EXIF (sem GPS, autor ou câmera); ainda assim, **25 deles compartilham um perfil ICC idêntico** ("c2ci / CC0 / Little CMS"), indicando **reprocessamento em lote por uma mesma ferramenta** — coerente com imagens raspadas de terceiros e re-salvas. Os próprios nomes de arquivo denunciam a origem (Amazon, Mercado Livre, outras lojas). Ver `imagens/metadata_exiftool.txt`.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	E-commerce sem identificação do operador (CNPJ, razão social, endereço, contato)	`corpo.html · pagina_contato.html`	ALTA
2	Ausência das políticas obrigatórias de troca/devolução e envio (Decreto 7.962/2013)	`/policies/* → 404`	ALTA

3	Catálogo clonado de loja-irmã ("Yuna Korean Beauty" em 220/248 produtos)	`products.json`	ALTA
4	Imagens copiadas de marketplaces (Amazon, Mercado Livre) e de terceiros	`imagens/` · `metadata_exiftool.txt`	MÉDIA
5	Domínio recém-registrado (~5 meses), validade de 1 ano, titular oculto	`RDAP — 14/01/2026`	MÉDIA
6	Tema não localizado: textos em espanhol numa loja pt-BR	`corpo.html`	MÉDIA
7	Urgência/escassez artificial: contador de carrinho e selos "VENDIDO"	`corpo.html`	MÉDIA
8	Perfil ICC uniforme em 25/46 imagens (reprocessamento em lote)	`metadata_exiftool.txt`	MÉDIA
9	Produtos duplicados ("-copia") e preço anômalo (R$ 31.774 em guia espanhol)	`products.json`	BAIXA
10	Origem mascarada por Cloudflare (IP real do servidor oculto)	`dns.txt` · `headers.txt`	BAIXA

Síntese: 3 indicadores de severidade ALTA, 5 MÉDIA e 2 BAIXA. **Nenhum fator de legitimidade** (operador identificado, políticas legais completas, conteúdo próprio, histórico) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 15/06/2026, conclui-se que **soyebeauty.com** é uma **loja virtual de cosméticos coreanos em operação**, sobre Shopify e voltada ao público brasileiro (pt-BR, BRL), que recebe pagamentos por cartão e coleta dados pessoais e de entrega, porém **sem identificar quem a opera** (sem CNPJ, razão social, endereço ou contato), **sem as políticas de troca/devolução e envio** exigidas do comércio eletrônico brasileiro, e com **catálogo e imagens copiados** de uma loja-irmã ("Yuna Korean Beauty") e de marketplaces. Somam-se o registro recente, o titular oculto, os resíduos de template em espanhol e os gatilhos de urgência artificiais — perfil compatível com **loja "fantasma"/dropshipping de uma rede de sites descartáveis**. Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não realizar compras** nem fornecer dados de cartão antes de confirmar a idoneidade da loja (CNPJ, razão social e endereço verificáveis — ausentes neste site).
- Desconfiar de anúncios em redes sociais (Instagram, TikTok, Facebook) que prometam cosméticos importados com preços muito abaixo do mercado e ofertas com contagem regressiva.
- Se já houve compra: guardar comprovantes e e-mails, abrir **contestação/chargeback** junto à operadora do cartão, e registrar reclamação em **consumidor.gov.br**, **Procon** e, se necessário, Boletim de Ocorrência.

Recomendações de mitigação / denúncia

- Reportar a loja aos canais de **abuse da Shopify** e da **Cloudflare** (uso da plataforma sem identificação legal do comerciante) e, sendo o caso, ao **Procon** e à **Senacon/consumidor.gov.br**, anexando este laudo.
- Verificar e reportar as **lojas-irmãs** da mesma rede (catálogo marcado como "Yuna / Lumi Korean Beauty"), que tendem a repetir o mesmo padrão em outros domínios recém-registrados.
- 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. A classificação expressa um juízo técnico de risco e não substitui decisão de autoridade policial, administrativa ou judicial. Não se imputa conduta ilícita aos provedores de infraestrutura e de pagamento citados (Shopify, Cloudflare, Hostinger), meros intermediários técnicos.

— Fim do relatório —

Documento gerado por Dono do Site — OSINT & Investigação Digital · Relatório técnico baseado em dados públicos e análise de conteúdo aberto.