



RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

sephora-brazil.shop

Objeto investigado	sephora-brazil.shop — loja online que se apresenta como "Sephora Brasil", usando o logotipo da marca Sephora (gTLD .shop)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	30/07/2026 (RDAP, DNS, HTTP/TLS, geolocalização, API pública do site, base pública de CNPJ)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do front-end e das rotas públicas de API
Achado central	Loja que imita a marca Sephora, declara um CNPJ inexistente , exibe oito meios de pagamento mas só aceita Pix
Classificação	RISCO ALTO
Emissão do laudo	30/07/2026 às 01:07

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **sephora-brazil.shop**, realizada em **30/07/2026** 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. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

O domínio **está no ar** e entrega uma **loja online em português** intitulada "Sephora Brasil — A beleza daquilo que nos une", que exibe o **logotipo da marca Sephora** no topo de todas as páginas. Trata-se de uma aplicação **Next.js** servida atrás da CDN **Bunny.net**, com aparência profissional, catálogo navegável, cupons, avaliações e um checkout próprio. A operação oficial da Sephora no Brasil se dá em **sephora.com.br**; o domínio investigado **não pertence a esse conjunto** e nada no site comprova autorização para usar a marca.

Três constatações sustentam a classificação de risco. Primeira: o **CNPJ declarado no rodapé** — 09.354.522/0001-30 — é **matematicamente inválido** (reprova na verificação de dígitos por módulo 11) e é **rejeitado pela base pública da Receita Federal**; ou seja, não identifica nenhuma empresa existente. Segunda: o rodapé anuncia **oito meios de pagamento** (Visa, Mastercard, Amex, Elo, Diners, JCB, Nupay e Pix), mas a própria API pública do site (/api/payment-methods) devolve **apenas Pix** — e o código do checkout força a lista de opções a Pix. O consumidor só pode pagar pelo único meio **irreversível e sem estorno por contestação**. Terceira: o **catálogo não é de produtos Sephora** — são secadores Mondial e Philco, aparadores Philips e Wahl e perfumes de terceiros, com descontos de 33% a 48%, mix típico de loja genérica.

Reforçam o quadro: **titular do domínio oculto**, registro de 1 ano feito em **13/03/2026**, ausência de **MX** (o e-mail contato@sephora-brazil.shop anunciado não tem como receber mensagens), páginas institucionais de **texto genérico** — a página "Sobre" afirma trabalhar com "eletrônicos, moda, casa e decoração, esportes e beleza", incoerente com uma loja de cosméticos — e **contador de urgência** nas "Ofertas do Dia". Existe ainda um antecessor: **sephora-mundo.shop**, registrado em 17/02/2026 e colocado em **clientHold** (suspensão pelo registrador) em 27/03/2026, hoje fora do ar. O domínio investigado foi registrado **14 dias antes** dessa suspensão.

CLASSIFICAÇÃO DE RISCO

RISCO ALTO

Leitura: uma loja que usa a marca de terceiro, declara um **CNPJ que não existe**, não tem e-mail funcional e aceita **somente Pix** enquanto exibe bandeiras de cartão que não pode processar não oferece ao consumidor **nenhum responsável identificável** nem via de reversão do pagamento. Recomenda-se **não comprar, não pagar e não fornecer dados** (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, os bundles JavaScript e as rotas públicas de API foram obtidos por requisição HTTPS de visitante comum. Nenhuma conta foi criada e nenhum pedido foi emitido. Fuso de referência: UTC.

Etapas	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (.shop — registrador Dynadot)	rdap_raw.json
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	dns_records.txt
Conteúdo / cabeçalhos	curl HTTPS (visitante)	corpo.html · headers_https.txt

Páginas institucionais	curl HTTPS (sobre, termos, privacidade, trocas, contato)	pagina_*.html
Aplicação (front-end)	Download dos bundles Next.js	evidencias/js/*.js
Meios de pagamento	Rota pública /api/payment-methods	api_payment_methods.json
Cupons / catálogo	Rotas públicas /api/coupons/public e /api/categories	api_coupons.json
Certificado TLS	openssl s_client / x509	tls_cert.txt
Geolocalização do IP	ipinfo.io · PTR reverso	ipinfo.json · ptr.txt
Identidade declarada	Verificação de DV (módulo 11) + base pública de CNPJ	cnpj_publico.json
Domínio antecessor	RDAP (.shop — sephora-mundo.shop)	rdap_sephora-mundo.json
Captura visual	Chrome headless (home, produto, rodapé)	imagens/*.png

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

Domínio	sephora-brazil.shop (gTLD .shop) · handle RDAP DO16827219-GMO
Registro	13/03/2026 · expira 13/03/2027 (validade de 1 ano)
Última alteração	29/07/2026 — um dia antes da coleta
Titular	Oculto (RDAP expõe apenas o registrador)
Registrador	Dynadot Inc. (IANA 472) · status clientTransferProhibited
Servidores de nome	kiki.bunny.net · coco.bunny.net — DNS da Bunny.net (CDN)
DNS — A	151.243.137.143 · sem AAAA · sem MX · TXT google-site-verification
www	registro A para o mesmo IP (sem CNAME)
Hospedagem	AS212238 Datacamp Limited (rede da Bunny.net) · geolocalização São Paulo/BR
Origem real	Não exposta — servidor de origem fica atrás da CDN
Servidor web	Server: nginx/1.31.3 · aplicação Next.js (rotas /_next/, turbopack)
Certificado TLS	CN=sephora-brazil.shop · emissor Let's Encrypt (DV) · válido 28/07/2026–26/10/2026
Emissão do TLS	28/07/2026 — dois dias antes da coleta, coincidindo com a alteração no RDAP
Cabeçalhos	HSTS, CSP com nonce, X-Frame-Options, Referrer-Policy — configuração cuidadosa
Domínio antecessor	sephora-mundo.shop — registrado 17/02/2026 (Hostinger), clientHold desde 27/03/2026, sem registro A

Leitura técnica. Titular oculto e registro de apenas 1 ano compõem um perfil de **baixa rastreabilidade do responsável**. A ausência de MX significa que o e-mail de atendimento divulgado no rodapé **não pode receber mensagens** — não existe canal de contato funcional por e-mail. O uso da CDN mantém a origem oculta, impedindo identificar onde a loja é realmente hospedada. O certificado DV gratuito comprova apenas o controle do domínio, **não a identidade de qualquer empresa** e muito menos vínculo com a marca Sephora. A reconfiguração de TLS e RDAP nos dois dias anteriores à coleta indica **infraestrutura ativa e recentemente movimentada**. Não se imputa conduta ao registrador (Dynadot), à Bunny.net/Datacamp nem à Let's Encrypt, meros provedores de infraestrutura.

4. Identidade Declarada, Meios de Pagamento e Catálogo

O rodapé de todas as páginas declara "© 2026 Sephora Brasil — Todos os direitos reservados. CNPJ 09.354.522/0001-30 · Av. das Nações Unidas, 12901 - Brooklin | São Paulo - SP, 04578-910", telefone (11) 3004-7522 e e-mail contato@sephora-brazil.shop. O CNPJ foi submetido à verificação de dígitos e à base pública:

Verificação	Resultado
CNPJ declarado	09.354.522/0001-30
Dígitos verificadores (módulo 11)	INVÁLIDO — os dois DV não conferem
Base pública (Receita Federal)	Rejeitado: "CNPJ 09.354.522/0001-30 inválido"
Conclusão	O número não identifica nenhuma empresa existente — é um CNPJ fabricado
E-mail declarado	contato@sephora-brazil.shop — domínio sem MX , não recebe mensagens
Marca exibida	Logotipo SEPHORA no cabeçalho de todas as páginas; nome "Sephora Brasil" no título, JSON-LD e rodapé
Operação oficial no Brasil	sephora.com.br — o domínio investigado não integra esse conjunto e não apresenta autorização de uso da marca

Meios de pagamento. O rodapé exibe oito selos sob o título "MEIOS DE PAGAMENTO": Visa, Mastercard, Amex, Elo, Diners Club, JCB, Nupay e Pix. A rota pública `/api/payment-methods` devolve, porém:

Constatação	Detalhe
Resposta da API	<code>{"methods":[{"gateway":"blackcat","displayName":"Pix"}, {"gateway":"unipay","displayName":"Pix"}], "pix":{"gateway":"unipay"}}</code>
Meios efetivamente ofertados	Apenas Pix — nenhum método de cartão
Comportamento do checkout	O front-end substitui a lista de opções pelo item Pix retornado pela API e o seleciona à força
Divergência	8 bandeiras anunciadas × 1 meio aceito — os selos de cartão são decorativos
Consequência ao consumidor	Só resta o meio irreversível : Pix não admite estorno por contestação de cartão
Direcionamento a Pix	Todos os preços exibidos "à vista no Pix"; páginas de produto trazem "Promoção válida no Pix"
Fluxo do pedido	Exige criar conta e cadastrar endereço; o QR só aparece em <code>/checkout/pagamento/<id></code>
Recebedor do Pix	Não determinado — obter o BR Code exigiria criar conta e emitir pedido, fora do escopo passivo

Aspecto	Constatação
Catálogo	Secadores e escovas Mondial/Philco, aparadores Philips OneBlade, Wahl e Kemei, protetores solares e perfumes de terceiros (Dior, Chanel, Creed, Carolina Herrera, Natura, O Boticário)
Coerência com a marca	Incompatível — não são produtos comercializados pela Sephora
Descontos	33% a 48% sobre preço "de" riscado, em todo o catálogo
Urgência artificial	"Ofertas do Dia — Termina em" com contador regressivo permanente
Avaliações	2 a 5 avaliações por produto, todas entre 4,7 e 5,0, com nomes abreviados — padrão uniforme e não verificável
Páginas institucionais	Textos de 3 a 4 frases genéricas; "Sobre" declara atuar em "eletrônicos, moda, casa e decoração, esportes e beleza", incoerente com loja de cosméticos
Identificação legal	Termos e Política de Privacidade não identificam razão social, CNPJ, endereço ou encarregado de dados (LGPD)
Plataforma	Next.js + API própria com identificadores cuid e suporte nativo a múltiplos gateways de Pix (blackcat, unipay) — indício de kit de loja reaproveitável

Leitura técnica. A combinação é autoexplicativa: a loja **invoca a marca Sephora** para dar credibilidade, **declara um CNPJ que não existe** para simular identificação legal, **exibe bandeiras de cartão que não pode processar** para simular um checkout convencional e **só aceita Pix**, o único meio sem via de reversão. Nenhum responsável é identificável: titular do domínio oculto, origem atrás de CDN, CNPJ fabricado, e-mail sem MX. A cronologia do antecessor `sephora-mundo.shop` — suspenso por `clientHold` em 27/03/2026, com o domínio investigado registrado 14 dias antes — é **compatível com rotação de endereços**, mas trata-se de **inferência**: não há evidência técnica coletada que prove operador comum aos dois domínios. Não se imputa conduta à Sephora (titular da marca, possível vítima de apropriação) nem aos provedores de pagamento nomeados pela API.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	CNPJ declarado no rodapé é matematicamente inválido e inexistente na base pública	corpo.html · cnpj_publico.json	ALTA
2	Uso do logotipo e do nome da marca Sephora sem qualquer comprovação de autorização	corpo.html · imagens/home.png	ALTA
3	Exibe 8 bandeiras de pagamento mas a API só oferta Pix — único meio irreversível	api_payment_methods.json · imagens/sobre_rodape.png	ALTA
4	Titular do domínio oculto e origem escondida atrás de CDN — sem responsável localizável	rdap_raw.json · dns_records.txt	ALTA
5	Catálogo incompatível com a marca (eletroportáteis e perfumes de terceiros) com 33–48% de desconto	corpo.html · pagina_produto.html	MÉDIA
6	Antecessor sephora-mundo.shop suspenso (clientHold) 14 dias após o registro deste domínio	rdap_sephora-mundo.json	MÉDIA
7	Termos e Política de Privacidade genéricos, sem razão social, CNPJ ou encarregado LGPD	pagina_termos-de-uso.html · pagina_politica-de-privacidade.html	MÉDIA
8	E-mail de atendimento anunciado em domínio sem MX — não recebe mensagens	dns_records.txt · corpo.html	BAIXA
9	Contador regressivo permanente e avaliações uniformes (2–5 por produto, 4,7–5,0)	corpo.html · pagina_produto.html	BAIXA

Síntese: 4 indicadores de severidade ALTA, 3 MÉDIA e 2 BAIXA. **Nenhum fator de legitimidade** (CNPJ verificável, responsável identificável, autorização de uso da marca, meio de pagamento reversível) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 30/07/2026, conclui-se que **sephora-brazil.shop** é uma **loja online de alto risco**: apresenta-se como "Sephora Brasil" e exibe o logotipo da marca sem qualquer comprovação de autorização; declara no rodapé um **CNPJ matematicamente inválido e inexistente na base da Receita Federal**; anuncia oito meios de pagamento mas **só aceita Pix**, o único irreversível; mantém **titular oculto** e origem atrás de CDN; e oferece um catálogo de eletroportáteis e perfumes de terceiros que não corresponde à marca invocada. Não há, em nenhuma das fontes consultadas, **responsável identificável** pela operação. Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não comprar, não pagar por Pix e não fornecer CPF, endereço ou dados pessoais** ao site.
- Desconfiar de ofertas "Sephora" com 30% a 50% de desconto divulgadas por redes sociais, WhatsApp ou anúncios pagos que conduzam a `sephora-brazil.shop`.
- Conferir o CNPJ de qualquer loja antes de comprar: um número que a base pública recusa é sinal de que a loja **não tem existência legal**.
- Estranhar sites que exibem bandeiras de cartão mas, no checkout, só permitem Pix — a escolha do meio irreversível é deliberada.
- Se já houve pagamento: acionar o banco e o mecanismo **MED** do Pix, reunir comprovantes e registrar reclamação em **consumidor.gov.br** e Boletim de Ocorrência.

Recomendações de mitigação / denúncia

- Denunciar o domínio aos canais de abuse do registrador (**Dynadot**) e do provedor de CDN/DNS (**Bunny.net**), anexando este laudo — o antecessor sephora-mundo.shop já foi suspenso por via semelhante.
- Comunicar a titular da marca **Sephora** sobre o uso não autorizado do nome e do logotipo, para as providências de propriedade industrial.
- Reportar o caso à **Senacon/Procon** e ao **consumidor.gov.br**, destacando a declaração de CNPJ inexistente e a divergência entre meios de pagamento anunciados e aceitos.
- 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. O recebedor do Pix não foi determinado, por exigir criação de conta e emissão de pedido — fora do escopo passivo. A relação com sephora-mundo.shop é inferência cronológica, não prova de operador comum. Não se imputa conduta ilícita à titular da marca Sephora, aos provedores de infraestrutura (Dynadot, Bunny.net/Datacamp, Let's Encrypt) nem aos provedores de pagamento nomeados pela API do site.

Anexo A — Manifesto de Integridade (SHA-256)

Hashes SHA-256 das evidências preservadas no momento da coleta (cadeia de custódia). Os bundles JavaScript baixados constam da pasta evidencias/js/ e do manifesto completo.

Arquivo	SHA-256
api_coupons.json	053b9290d47f36634661fd271ab357df05ad7e126105d73166b0a17b5079aadf
api_payment_methods.json	a9d0b55c558aff74104b27c6b2eeef4e6b87cfd2d981061f5097a05fc07a92b
cnpj_publico.json	7cb5ca0df59aceae9fa267b1f13def7e6b578e88abafe94396ace838ca2b4d5b
corpo.html	278465df8393defcead017664645c3b7d23af3ecd6209b9c44c40f718ae2cf37
dns_records.txt	447c04216dca89c88309c1d73f05dc694b3dc89e9da5874da822bb3e4374b991
hash_manifest.txt	c4b42b3417b444934f9d038df3d57c136d9bee2cbffc45fbc368e0e78a45f12a
headers_https.txt	28091dee71a579a69577892eb77f39f176d34a161e675b51572168a1253be642
ipinfo.json	27e95d2e40e4531561d933283c8709ceb49030bb2ffae752bf7f67b9409c9bde
pagina_checkout.html	267a86a609aa71d879069606ded426d1ac5b908bf39c80b9d79bc15726aade65
pagina_contato.html	df937916c05895f895bed10b18fbdffb2346d46ff7bafcae7458b9b155de2d353
pagina_politica-de-privacida de.html	ea7eee23303f3924e6f5a73974f236b488b1e1611fbffbf5c48654a8825914c1d
pagina_produto.html	3746e6fd34ea790bcc9a2a88f44e573f929e0fa0d127f4f07ab947cc8c0279ee
pagina_sobre.html	77b4621cd962795e6fabcb253d1acd8300b7e840e507a865569e3dada0eb32da2
pagina_termos-de-uso.html	8b656cc187df5c4416129a86884025994d364db17eaf763068be412611a34b53
pagina_trocas-e-devolucoes.h tml	23fc7d1b154d79d7e12ba62703ad7f16861b72c910b58828bde3c148b24680cb
ptr.txt	9ba39257979de0db7a9d07ebe7cb3221fd27ce4cdd61c3e6c526529b22c6ef33
rdap_raw.json	93340abecb97553dae4b019af09c13f2de860db1a4eb7584d7cee62674e73212
rdap_sephora-mundo.json	84aaa14090b5cac555ec8ed0a043fa564b5583b3b89dd720ebf675a89bc04afd
rede_fingerprint.txt	9171e714ef5780566389fa3a260d9471b6b09c706f589d344fa207b308328c4d
tls_cert.txt	d4d6fd3b08c999ea3531a811f646bb19d5b23e8699315aa45acf88d772b73fe9
imagens/home.png	54a2b6f0c9b71580f8ef60d3a436ffe5eda4400446cd2ececc7ab9d9dfdf42ec7f

imagens/produto.png	c28416922d56c20dc26a9e64ea406ef1f6fcaaf01eeabdf4611e0f0f4c0216c3
imagens/sobre_rodape.png	042c6e0b8f604b76d14f64c4b72c3e8c2f9745aae84291d665bf8c59ed504205

— Fim do relatório —