

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

serenadiva.shop

Objeto investigado	serenadiva.shop - loja Shopify de moda feminina (vestidos, conjuntos, blusas, calças)
Natureza	Verificação de identificação do fornecedor e das condições de venda
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	Loja sem CNPJ que se declara “intermediadora de negócios físicos e digitais” com “estoque terceirizado” internacional, aponta como site oficial um .com.br registrado por pessoa física e usa promoções permanentes de “Compre 1 Leve 2”
Classificação	**RISCO MÉDIO**
Emissão do laudo	18/11/2026 as 00:54

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **serenadiva.shop**, 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, construída na Shopify e protegida por desafio anti-robô (foi lida com navegador headless), vende moda feminina entre R$ 90 e R$ 170, com promoções “Compre 1 Leve 2” e “Kit com 3”, parcelamento em 12x e Pix. O checkout é da Yampi; há pixels de TikTok, Facebook, Google Ads e UTMify, típicos de venda impulsionada por anúncios.

Nenhuma página exibe CNPJ. A política de reembolso diz que a Serena Diva “opera como intermediadora de negócios físicos e digitais” e “atua com o modelo de estoque terceirizado” para trazer “tendências internacionais” — linguagem comum em lojas de dropshipping com envio do exterior, que alonga prazos e dificulta trocas.

A mesma política chama de “site oficial” o domínio **serenadiva.com.br**, registrado três dias antes do .shop por uma pessoa física. O único endereço informado (Av. Professor Oscar Pereira, 6158, Porto Alegre/RS) não vem acompanhado de razão social que permita conferência.

CLASSIFICAÇÃO DE RISCO	RISCO MÉDIO

Leitura: não há indício de captura indevida de dados, mas o fornecedor não é identificado e o modelo declarado (intermediação com estoque terceirizado no exterior) transfere ao comprador o risco de atraso, produto diferente do anunciado e dificuldade de devolução (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	serenadiva.shop

Registro	12/05/2026 · expira 12/05/2027 · **189 dias** antes da coleta
Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)
Registrador	GoDaddy.com LLC · abuse@godaddy.com
Servidores de nome	ns07.domaincontrol.com · ns08.domaincontrol.com
DNS - A	23.227.38.32 · MX: smtp.secureserver.net, mailstore1.secureserver.net
Hospedagem	AS13335 Cloudflare, Inc. · Ottawa/CA · PTR/hostname `myshopify.com` · cabeçalho `server: cloudflare`
Certificado TLS	Let's Encrypt (YE1) · emitido em 07/11/2026 · válido até 05/02/2027
Loja Shopify	`fpyawp-za.myshopify.com` · moeda BRL · checkout Yampi
“Site oficial” citado	`serenadiva.com.br` · registrado em 09/05/2026 por **pessoa física** (CPF mascarado ***.121.277-**)
CNPJ	**Nenhum** exibido na home, no SAC ou na política de reembolso

Leitura: domínio de 189 dias com titular oculto (GoDaddy), DNS GoDaddy, e-mail GoDaddy/Secureserver e site servido pela Shopify. Nada técnico vincula a loja a uma empresa.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Loja Shopify com tema personalizado, checkout Yampi (`api.yampi.io`, `api.dooki.com.br`), avaliações Areviews e pixels de rastreamento. Páginas de política (SAC e reembolso) foram baixadas.

Aspecto	Constatação
Pagamento	Cartão em até 12x e Pix, via checkout Yampi
Fornecedor	Sem CNPJ; “intermediadora” com “estoque terceirizado” internacional
Contato	contato@serenadiva.shop · seg. a sex., 10h-18h · sem telefone
Promoções	“Compre 1 Leve 2”, “Kit com 3”, descontos de até 50%

Leitura: sem razão social, o comprador não tem contra quem reclamar formalmente; o checkout de terceiros não supre essa ausência.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Nenhum CNPJ ou razão social em todo o site	`corpo_home_chrome.html` · `corpo_policies_*.html`	ALTA
2	Modelo declarado de intermediação com estoque terceirizado no exterior	`corpo_policies_refund_policy.html`	MEDIA
3	“Site oficial” .com.br registrado por pessoa física	`rdap_serenadiva.com.br.json`	MEDIA
4	Promoções permanentes “Compre 1 Leve 2” impulsionadas por pixels de anúncio	`corpo_home_chrome.html`	BAIXA

Síntese: quatro indicadores, um de severidade alta (fornecedor não identificado).

6. Conclusão Técnica e Recomendações

A serenadiva.shop é uma loja Shopify funcional, mas sem fornecedor identificado e com modelo declarado de intermediação com estoque terceirizado no exterior. Classificação técnica: **RISCO MÉDIO**.

Recomendações ao consumidor / solicitante

- Antes de comprar, peça por e-mail a razão social e o CNPJ do vendedor e o prazo real de entrega.
- 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 (1079963 bytes)	36cf0d18f400e963b1d3605b793a6563625acc2c799b3e7da0977ee651f35692
corpo_home.html (8715 bytes)	601dd75fce08c8928cef73c039e022a3c46465bda3c0b8568ab9e3bf95cd77fc
corpo_policies_contact_information.html (305229 bytes)	f11821fda0050016daaebb4333f9362420afb39d520e5a3a72a96aa66a5c81a4
corpo_policies_refund_policy.html (306980 bytes)	f7ebb166edbc621d9c1e4200d8870a4945af583add84a7cd9d2e97764c95a8cd
dns_records.txt (439 bytes)	cd1b161e1c146f4ffc72d5b0edbd662ec8318086e3213c861c9157528fcc788d
geoip.json (301 bytes)	304ec09a3057cc350f6451a92a83a2e15840cd1405f8b92b69213e5de11fc678
headers_home.txt (1787 bytes)	d199eaa9a6d866e32d8cc5468919632eab8ec0ef779353f27128f4442728a89f
rdap_raw.json (4291 bytes)	cdc6e97e89250d3904ca78a58a9b994d3f8d1feb11e37224750a8deb968ad6b8
rdap_serenadiva.com.br.json (4057 bytes)	f52c330bddf27cce49d31f2ed3ee9633b92d364a6c10d4bb887c2a9123e66d35
tls_cert.txt (300 bytes)	ffc9bceff2d6e1d0a1316b03e3666cdf4097726e2888781c5c31817f663d9d58

- Fim do relatório -