

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

lojavezana.com

Objeto investigado	lojavezana.com - loja de moda feminina “Vezana”
Natureza	Verificação de identificação do vendedor, idade do domínio e meios de pagamento
Data da coleta	28/11/2026 (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 de 22 dias, sem CNPJ, que identifica apenas uma pessoa física como responsável e só aceita **Pix** — o cartão está desativado na configuração do próprio site
Classificação	**RISCO MÉDIO**
Emissão do laudo	28/11/2026 as 01:05

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **lojavezana.com**, realizada em **28/11/2026** 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 Vezana vende vestidos, alfaiataria e bolsas com campanha “BLACK VEZANA” e descontos de 19% a 37% (ex.: vestido de linho de R$ 300,00 por R$ 189,00, ou R$ 173,88 no Pix). O domínio foi registrado em 06/11/2026, 22 dias antes da coleta, e a loja roda na Vercel.

O rodapé não traz CNPJ: indica como “responsável pela loja” uma pessoa física, com nome e CPF, e um “endereço da operação” em Itapeva/MG, com “atendimento exclusivamente on-line”. O telefone tem DDD 17, do noroeste de São Paulo.

A configuração de pagamento exposta pelo próprio site (`/api/payment-gateway/config`) mostra Pix por um intermediário identificado como “beehive” e o cartão como indisponível. O código também registra presença e sessão de cada visitante (`/api/track/presence`, `/api/track/session`).

CLASSIFICAÇÃO DE RISCO	RISCO MÉDIO

Leitura: venda por pessoa física, sem empresa constituída, num domínio de três semanas e só com Pix — combinação que deixa o comprador sem meio de contestação e sem um CNPJ para responsabilizar.

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	lojavezana.com
Registro	06/11/2026 · expira 06/11/2027 · **22 dias** antes da coleta
Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)

Registrador	Cloudflare, Inc. · registrar-abuse@cloudflare.com
Servidores de nome	melnicoff.ns.cloudflare.com · ullis.ns.cloudflare.com
DNS - A	216.150.1.65 · 216.150.16.65 · MX: receive-sae1.forge.rmta.net
Hospedagem	AS16509 Amazon.com, Inc. · Miami/US · cabeçalho `server: Vercel`
Certificado TLS	Let's Encrypt (YR1) · emitido em 06/11/2026 · válido até 04/02/2027
Responsável declarado	Pessoa física, com nome e CPF no rodapé (CPF `490.***.***-80`, dígitos verificadores válidos); nenhum CNPJ
Endereço e telefone	Itapeva/MG (CEP 37655-000) · telefone (17) 98184-5824, DDD do noroeste paulista
Pagamento	`/api/payment-gateway/config`: Pix pelo intermediário “beehive”; cartão `"unavailable"`

Leitura: domínio de 22 dias com titular oculto, registrado na Cloudflare e hospedado na Vercel.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Aplicação Next.js própria na Vercel, com catálogo, carrinho, rastreio de pedido e API de pagamento.

Aspecto	Constatação
Vendedor	Pessoa física; sem CNPJ
Pagamento	Só Pix; cartão indisponível
Descontos	19% a 37%, mais desconto no Pix
Contato	E-mail do domínio e celular de DDD 17

Leitura: a loja não demonstra uma empresa por trás da venda; o risco recai sobre o pagamento por Pix.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Nenhum CNPJ; vendedor identificado só como pessoa física	`corpo_contato.html`	ALTA
2	Domínio de 22 dias	`rdap_raw.json`	MEDIA
3	Pagamento só por Pix (cartão desativado)	`api_payment-gateway_config.json`	MEDIA
4	Endereço em MG e telefone com DDD de SP	`corpo_home.html`	BAIXA
5	Titular do domínio oculto	`rdap_raw.json`	BAIXA

Síntese: cinco indicadores, um de severidade alta.

6. Conclusão Técnica e Recomendações

A lojavezana.com é uma loja recém-criada, sem CNPJ, operada em nome de uma pessoa física e que só aceita Pix. Classificação técnica: **RISCO MÉDIO** — não há prova de fraude, mas faltam a identificação empresarial e os meios de pagamento que protegeriam o comprador.

Recomendações ao consumidor / solicitante

- Antes de pagar, peça nota fiscal e um CNPJ; sem eles, a compra fica sem garantia formal.
- 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 (registrar-abuse@cloudflare.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 28/11/2026; 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
api_payment-gateway_config.json (92 bytes)	d7b811ed3f1cf7fc759ee95de5437944c178c4193a3838eca2b402371de2c844
bundle_js.txt (395858 bytes)	aa63345a15a988858365a8abfe4827be39b704edd32725b3cf4bef13f31474c6
corpo_contato.html (50935 bytes)	f840f87f7833f96eed42631f808983dc891d03a062c951dcaa5bf50452fa318a
corpo_home.html (217034 bytes)	df179930893f5c870b430ac81b806b5fa2578589043708c9b24c1017f6f52fbb
corpo_produto.html (359122 bytes)	4dcc8d2a063be616e75e8ea3ca54acb17aea87451a35eb8a65cfe0da38e5e725
dns_records.txt (454 bytes)	1de8988d0f04416d6f3ce19182381ad0c3cdb6a77f7e674644aba01b718ea38a
geoip.json (272 bytes)	907a6f8f54df09bbe1e7e8d2ac0392f2c50e1cf00e22baaeedaa06e94e53222e
headers_home.txt (667 bytes)	ae44e35328f40a94a28996ef1e731c3a6d0a3c0ae46122d19b0a411a651f6d59
rdap_raw.json (2628 bytes)	d05afeb1aedeadbae4b40419d152986988c74df4219ef00a0620ec0a4f484ce8
tls_cert.txt (299 bytes)	70b1ac3f6703647436b6ee6b1949746d824e9477b23b7204890bb254519557f6

- Fim do relatório -