

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

autopecasnovelo.netlify.app

Objeto investigado	autopecasnovelo.netlify.app - site da “Novelo Auto Peças”, peças usadas de leilão, Piracicaba/SP
Natureza	Verificação de identificação do fornecedor e de coerência das declarações
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	Site em **subdomínio gratuito do Netlify**, sem CNPJ, que se diz “desmonte credenciado” com “procedência certificada” e “laudo de origem” e encaminha toda busca de peça para o WhatsApp; o código traz instruções esquecidas de configuração do Google Ads
Classificação	**RISCO ALTO**
Emissão do laudo	18/11/2026 as 00:54

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **autopecasnovelo.netlify.app**, 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 “Novelo Auto Peças” oferece peças usadas originais “provenientes de veículos de leilão”, com “garantia, nota fiscal e laudo de origem”, envio para todo o Brasil e o selo textual “Empresa credenciada”. O endereço declarado é Av. Manoel Conceição, 1083, Vila Rezende, Piracicaba/SP.

O site não tem domínio próprio: roda em `autopecasnovelo.netlify.app`, subdomínio gratuito e descartável da plataforma Netlify. Não há CNPJ nem número de credenciamento. O buscador de peças não consulta estoque: monta uma mensagem e abre o WhatsApp (19) 99759-5132.

O HTML conserva um comentário de modelo — “troque ADS_SEND_TO pelo send_to da sua conversão” —, indício de página montada a partir de template para campanhas pagas de Google Ads.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: alegações de credenciamento sem número verificável, ausência de CNPJ, endereço sem domínio próprio e venda exclusiva por WhatsApp formam o padrão do golpe do falso desmanche (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)

Endereço	**autopecasnovelo.netlify.app** — subdomínio gratuito da plataforma `netlify.app`; não há domínio próprio registrado em nome da loja
Domínio da plataforma	netlify.app · registrado em 08/05/2018 · pertence à Netlify, não ao site
DNS - A	54.232.119.62 · sem MX

Hospedagem	AS16509 Amazon.com, Inc. · São Paulo/BR · PTR/hostname `ec2-54-232-119-62.sa-east-1.compute.amazonaws.com` · cabeçalho `server: Netlify`
Certificado TLS	DigiCert Inc (DigiCert Global G2 TLS RSA SHA256 2020 CA1) · emitido em 16/02/2026 · válido até 19/03/2027
CNPJ	**Nenhum** exibido, apesar de “Empresa credenciada” e “Desmonte credenciado”

Leitura: os dados de RDAP referem-se a `netlify.app`, domínio da própria plataforma (2018); o site não possui registro próprio. Servido pela Netlify em São Paulo (AWS).

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Página estática no Netlify, sem backend próprio, com formulário que apenas monta mensagem para o WhatsApp e marcação de conversão do Google Ads.

Aspecto	Constatação
Venda	Apenas WhatsApp (19) 99759-5132; sem preços nem checkout
Alegações	“Empresa credenciada”, “procedência certificada”, “laudo de origem”, garantia e nota fiscal
Identidade	Sem CNPJ; Av. Manoel Conceição, 1083, Piracicaba/SP
Resto de modelo	Comentário “troque ADS_SEND_TO pelo send_to da sua conversão”

Leitura: o site serve como página de captura de anúncio; toda a transação ocorre fora dele, sem registro.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Subdomínio gratuito Netlify, sem domínio próprio	`dados.json · tls_cert.txt`	ALTA
2	Sem CNPJ apesar de alegar credenciamento	`corpo_home.html`	ALTA
3	Venda exclusivamente por WhatsApp	`corpo_home.html`	ALTA
4	Comentário de template de Google Ads esquecido no HTML	`corpo_home.html`	MEDIA

Síntese: quatro indicadores, três de severidade alta.

6. Conclusão Técnica e Recomendações

O autopecasnovelo.netlify.app é uma página de anúncio em subdomínio gratuito, sem CNPJ e sem credenciamento verificável, que leva a venda de peças ao WhatsApp. Classificação técnica: **RISCO ALTO**.

Recomendações ao consumidor / solicitante

- Peça usada deve ser comprada de desmonte credenciado no Detran do estado, com nota fiscal e etiqueta de rastreabilidade; confira o credenciamento no site do Detran antes de pagar.
- Não pague antecipadamente por Pix a desmanche contatado só por WhatsApp.
- 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@name.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.
- Denunciar o subdomínio à Netlify (formulário de abuso da plataforma).

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.html (47499 bytes)	3da355ef293088063465ef5bd199bb0d6d47ea8c2e08941ad3d1e5c501723393
dns_records.txt (300 bytes)	57ba38b54c658f411fc1d8f6bb85c53fc2f7452cca431c51069260827ca48e52
geoip.json (335 bytes)	df5b98edc54c1ec6b02e86d7df5fafcdd3986298e0aadc1e978fb0429f4b4f9a
headers_home.txt (586 bytes)	4621ff8e3ece3d53cfaf05f4caf069b5995aa2f3e1881cb9f41d270f66da4d31
rdap_raw.json (6714 bytes)	5b6f1a82f827b2c6c620f9fa05eae4c36d76dfd28b1e22e12af993f3744d9224
tls_cert.txt (396 bytes)	33ee7eb1f5ad2672d809467de1d194d778be7c6c9b325499af7911250723aeba

- Fim do relatório -