

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

autopecasviaoestedesmonte.com

Objeto investigado	autopecasviaoestedesmonte.com - site da “Auto peças Via Oeste — Desmonte credenciado”
Natureza	Verificação de identificação do fornecedor e de coerência das declarações
Data da coleta	23/11/2026 (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 sem CNPJ que se diz “desmonte credenciado” no Detran de São Paulo, mas exibe o logotipo do Detran de Santa Catarina, alega 60 mil peças e conduz toda a venda ao WhatsApp com “15% de desconto”
Classificação	**RISCO ALTO**
Emissão do laudo	23/11/2026 as 02:19

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **autopecasviaoestedesmonte.com**, realizada em **23/11/2026** 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 página, em WordPress com Elementor, oferece lataria, iluminação, motores e câmbios “com garantia e procedência”, “15% de desconto para novos clientes”, “mais de 60 mil peças” e envio para todo o Brasil. Todos os botões “Solicitar orçamento agora” abrem o WhatsApp (11) 96515-1951.

O texto afirma que a empresa está “devidamente cadastrada no DETRAN/SP/CP” e segue “as normas de uma desmontadora veicular autorizada”, mas não exibe CNPJ, razão social, endereço nem número de credenciamento. O único selo de órgão público é uma imagem chamada `detransc` — o logotipo do Detran de Santa Catarina, incoerente com a alegação de cadastro em São Paulo.

O domínio foi registrado em 06/03/2026 com titular oculto. O rodapé contém um link oculto para um site de “plugins premium WordPress” (`full.services`), comum em temas pirateados.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: alegação de credenciamento sem número verificável, selo de outro estado, ausência total de identificação e venda por WhatsApp compõem o padrão 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)

Domínio	autopecasviaoestedesmonte.com
Registro	06/03/2026 · expira 06/03/2027 · **262 dias** antes da coleta
Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)

Registrador	HOSTINGER operations, UAB · abuse-tracker@hostinger.com
Servidores de nome	ns1.dns-parking.com · ns2.dns-parking.com
DNS - A	46.202.145.123 · sem MX
Hospedagem	AS47583 Hostinger Operations UAB · São Paulo/BR · cabeçalho `server: LiteSpeed`
Certificado TLS	Let's Encrypt (YE1) · emitido em 31/10/2026 · válido até 29/01/2027
CNPJ	**Nenhum** exibido, apesar de “empresa devidamente cadastrada no DETRAN/SP/CP”
Selo exibido	Imagem `detransc-removebg-preview…png` — logotipo do Detran de **Santa Catarina**, enquanto o texto alega cadastro no Detran de São Paulo

Leitura: domínio de 262 dias com titular oculto, registrado e hospedado na Hostinger (São Paulo), servidor LiteSpeed, sem e-mail configurado.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

WordPress 7 com Elementor e botões flutuantes de WhatsApp; sem catálogo transacional nem checkout.

Aspecto	Constatação
Venda	Orçamento pelo WhatsApp (11) 96515-1951; sem preços nem checkout
Alegações	“Desmonte credenciado”, “cadastrada no DETRAN/SP/CP”, 60 mil peças, 15% de desconto
Identidade	Sem CNPJ, sem razão social, sem endereço
Selo	Logotipo do Detran de Santa Catarina

Leitura: sem identificação, o comprador não tem como verificar o credenciamento nem reclamar formalmente.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Nenhum CNPJ, razão social ou endereço	`corpo_home.html`	ALTA
2	Alega credenciamento em SP mas exibe logotipo do Detran-SC	`corpo_home.html`	ALTA
3	Venda exclusivamente por WhatsApp	`corpo_home.html`	ALTA
4	Link oculto para site de plugins piratas	`corpo_home.html`	BAIXA
5	Domínio com titular oculto	`rdap_raw.json`	BAIXA

Síntese: cinco indicadores, três de severidade alta.

6. Conclusão Técnica e Recomendações

O autopecasviaoestedesmonte.com alega ser desmonte credenciado sem exibir nenhum dado verificável, usa o selo de um Detran diferente do alegado e leva toda a venda 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; prefira retirar no local.
- 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-tracker@hostinger.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 23/11/2026; 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
bundle_js.txt (107279 bytes)	f827c4f3c266df69d0c6a72c33fd09bc46fc5ce4ab73d87b7383b20b2c843391
corpo_home.html (109390 bytes)	6385b3ee876e62dedb91659053eeae2e022420d2c691fe1b66531db198de3c69
dns_records.txt (469 bytes)	0d225a653458cebd5f15795d241891b56e1a22240581007a1f0652aa4b02fe66
geoip.json (277 bytes)	419b2b2a22064ead85dc645259425c4db0315cc63fa538276e14d3563496a140
hash_manifest.txt.n (379 bytes)	043141dfc79cb124e544c88849825127e27bbf39d6adc138aeb6592c34782218
headers_home.txt (672 bytes)	7513b049f5fff352a2e8ef6d2f64868dd30ef17c2dfdb470662302a2b1a87806
rdap_raw.json (2718 bytes)	9bc3fa6cfa9a44b8b1527321e70052ddae26b299139e0b78545fe291e67f99d1
tls_cert.txt (314 bytes)	381c50c1fb2b14fee244f00170aa975e6890ece5d49628d155a0189f17de56ce

- Fim do relatório -