

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

desmonteformula1.com

Objeto investigado	desmonteformula1.com - site do “Desmonte Formula 1”, peças usadas na Zona Norte de São Paulo
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	Domínio de **4 dias**, gerado na Lovable, que cita a lei dos desmontes mas não exibe CNPJ nem credenciamento, alega “mais de mil câmbios” e “dez mil m²” e usa imagens copiadas de outra autopeças
Classificação	**RISCO ALTO**
Emissão do laudo	23/11/2026 as 02:19

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **desmonteformula1.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).

O site apresenta o “Desmonte Formula 1”, na Av. Pedro Berruguete, 19 — Jardim Shangrilá, Zona Norte de São Paulo, com “estoque amplo”, “mais de mil câmbios em estoque”, “mais de dez mil metros quadrados” de peças, nota fiscal, garantia de 90 dias e envio para todo o Brasil em até 24 horas após a confirmação.

O domínio foi registrado em **19/11/2026**, quatro dias antes da coleta, e o site é uma aplicação gerada na Lovable (selo “Edit with Lovable” ainda visível). Um bloco “Desmonte Legal!” cita a Lei Federal 12.977/2014 e a Resolução Contran 611/16, mas a página não informa CNPJ nem número de credenciamento.

Parte das imagens é carregada de outros sites — `autopecasalvorada.com.br` (outra autopeças), Wikimedia e `i.ibb.co` —, e todo pedido é feito pelo WhatsApp (11) 98642-0468.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: site de dias, sem CNPJ, com alegações de grande estrutura e imagens de terceiros, e venda só por WhatsApp — o padrão recorrente 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	desmonteformula1.com
Registro	19/11/2026 · expira 19/11/2027 · **4 dias** antes da coleta
Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)

Registrador	GoDaddy.com, LLC · abuse@godaddy.com
Servidores de nome	ns13.domaincontrol.com · ns14.domaincontrol.com
DNS - A	185.158.133.1 · sem MX
Hospedagem	AS13335 Cloudflare, Inc. · San Francisco/US · PTR/hostname `lovable-app-cd-1-4.p.l5e.io` · cabeçalho `server: cloudflare`
Certificado TLS	Google Trust Services (WE1) · emitido em 19/11/2026 · válido até 17/02/2027
CNPJ	**Nenhum** exibido, apesar de citar a Lei 12.977/2014 e a Resolução Contran 611/16

Leitura: domínio de 4 dias com titular oculto (GoDaddy), DNS GoDaddy, sem MX; aplicação hospedada na Lovable atrás da Cloudflare.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Aplicação React gerada na Lovable, com rota `/admin` exposta no rodapé e rota `/api/broadcast`; sem catálogo transacional.

Aspecto	Constatação
Venda	Pedidos pelo WhatsApp (11) 98642-0468; sem preços nem checkout
Alegações	Mil câmbios, 10 mil m², nota fiscal, garantia de 90 dias, envio em 24 h
Identidade	Sem CNPJ; Av. Pedro Berruguete, 19, Zona Norte/SP; contato@desmonteformula1.com (domínio sem MX)
Imagens	Carregadas de autopecasalvorada.com.br, Wikimedia e i.ibb.co

Leitura: o e-mail informado usa um domínio sem servidor de e-mail configurado; o único canal real é o WhatsApp.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Domínio de 4 dias	`rdap_raw.json`	ALTA
2	Sem CNPJ nem credenciamento, apesar de citar a lei dos desmontes	`corpo_home.html`	ALTA
3	Venda exclusivamente por WhatsApp	`corpo_home.html`	ALTA
4	Imagens carregadas do site de outra autopeças	`corpo_home.html`	MEDIA
5	E-mail de contato em domínio sem MX	`dns_records.txt`	BAIXA

Síntese: cinco indicadores, três de severidade alta.

6. Conclusão Técnica e Recomendações

O desmonteformula1.com foi criado há quatro dias, alega grande estrutura sem exibir CNPJ nem credenciamento, usa imagens de terceiros e leva 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@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 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 (652896 bytes)	bda0c7bbe8a2f73745f31539d1629a7ed3250c34f130d1eee01528909d0c93b4
corpo_home.html (44292 bytes)	8d1ccce79126faa5d567cb0df52b4181757d96aa56b7d2e049cbb2a958029747
dns_records.txt (347 bytes)	470c25176fd050f998d161a0170c4b535bd7413b559501cae474cc8af45fce38
geoip.json (333 bytes)	8c316e02ecf7a6652c0547faed6e32afe85bc5de6ecd42dcda1ab4739083ac95
hash_manifest.txt.n (378 bytes)	904d0970fd02e83a5f103c89abe709085e002d6f2bf9ef9b2bcb481d999e8a61
headers_home.txt (824 bytes)	6a4f322651ba19a08eb6ae20079cee778692f0969aca0d06c0662d8b658acade
rdap_raw.json (2713 bytes)	90d766756ff0ea9f918db6a5f60baad9d5a0efd0ec8cc0135e099cc6cfe9adb4
tls_cert.txt (309 bytes)	74266bf417eae00b480c54205edf7ce9a36844a9b84f5aed8fdebbc0cea17e5b

- Fim do relatório -