RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

grupopharmalab.store

Objeto investigado	grupopharmalab.store — página que anuncia aluguel de caçambas de entulho em São Paulo (gTLD .store)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	29/07/2026 (RDAP, DNS, HTTP/TLS, geolocalização, bundle JS, consulta de CNPJ)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do bundle · base pública da Receita Federal
Achado central	O domínio, cujo nome remete ao setor farmacêutico, entrega um site de caçambas cujo canonical aponta para ambalocacao.com — domínio que está sob "client hold" (suspenso) e não resolve; o pagamento é combinado exclusivamente por WhatsApp, antes da entrega
Classificação	**RISCO ALTO**
Emissão do laudo	30/07/2026 às 00:31

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **grupopharmalab.store**, realizada em **29/07/2026** por técnicas de OSINT (inteligência de fontes abertas) e análise passiva — requisições equivalentes às de um visitante comum e consultas a bases públicas, sem qualquer interação intrusiva, sem envio de dados pessoais e sem tentativa de contratação ou de pagamento. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

O domínio **está no ar** e entrega uma aplicação React/Vite intitulada "Aluguel de Caçamba SP | Disk Caçambas - São Paulo e Região", que oferece caçambas de 3 m³ a 10 m³ por **R$ 180,00 a R$ 500,00** e concentra todo o atendimento em um único canal: o WhatsApp. O nome do domínio, porém, **não tem relação alguma com a atividade anunciada** — "grupopharmalab" remete ao setor farmacêutico, não a locação de caçambas ou a resíduos de construção.

O achado central é estrutural. As metatags `canonical` e `og:url` da página não apontam para o próprio endereço, mas para **https://ambalocacao.com/** — o domínio para o qual o site foi originalmente publicado. A consulta RDAP mostra que **ambalocacao.com** foi registrado em **06/03/2026** e hoje está com os estados `client hold`, `client delete prohibited`, `client renew prohibited`, `client transfer prohibited` e `client update prohibited`, delegado a `NS1.SUSPENDED-DOMAIN.COM` — ou seja, **suspenso pelo registrador**. O domínio não resolve (consulta DNS sem resposta e conexão HTTP recusada). O **grupopharmalab.store** foi registrado em **11/06/2026**, três meses depois do primeiro, e serve exatamente a mesma aplicação: é o **endereço substituto de um site que saiu do ar por suspensão**.

A identidade empresarial exibida é de **uma empresa real**. O bundle JavaScript declara três vezes "Disk Caçambas - Soluções Ambientais, CNPJ: 19.142.610/0001-58" (rodapé, Política de Privacidade e Termos de Uso). A consulta à base pública da Receita Federal confirma que esse CNPJ pertence a **DAL COL ENGENHARIA E GESTAO AMBIENTAL LTDA**, nome fantasia "DISK CACAMBA - SOLUCOES AMBIENTAL", situação cadastral **ATIVA** desde 25/10/2013, sediada em **Itararé/SP**, com CNAE principal de transporte rodoviário de carga e CNAEs secundários de coleta e disposição de resíduos não perigosos. O site, entretanto, anuncia atendimento em "todo o estado de São Paulo" com telefone de DDD **11** (capital), enquanto a empresa titular do CNPJ está a cerca de **320 km** da capital. **Não há, nas fontes abertas consultadas, qualquer elemento que demonstre vínculo entre esse domínio e essa empresa** — e o quadro é compatível com **apropriação de identidade empresarial**. Não se imputa conduta ilícita à empresa cujo CNPJ é exibido, que pode ser vítima.

Os elementos de confiança são fabricados. A "verificação de área de cobertura" apenas consulta a API pública `viacep.com.br` e responde **"Área de cobertura confirmada!"** para **qualquer CEP brasileiro válido** — não existe checagem real de atendimento. Os três depoimentos exibidos usam **fotos de banco de imagens** (images.unsplash.com). E o fluxo de contratação descrito pelo próprio site é "01 Solicite via WhatsApp → **02 Confirme e Pague** → 03 Entrega → 04 Retirada": não há carrinho, checkout, gateway, nota fiscal nem qualquer página de pagamento — o dinheiro é combinado em conversa privada e **pago antes da entrega**.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: um site cujo endereço não tem relação com o serviço vendido, que substitui um domínio suspenso pelo registrador, exibe o CNPJ de uma empresa real e distante sem vínculo demonstrável, confirma cobertura para qualquer CEP do país e recebe **pagamento antecipado por WhatsApp** oferece **risco elevado**. Recomenda-se **não pagar antecipadamente e confirmar o fornecedor por canais independentes** (Seções 5 e 6).

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 código do front-end foram obtidos por requisição HTTPS de visitante comum, sem qualquer interação intrusiva, sem envio de dados pessoais e sem tentativa de compra ou de pagamento. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (Radix/.store — registrador NameCheap)	`rdap_raw.json`
Domínio canônico	RDAP (ambalocacao.com — Realtime Register)	`rdap_ambalocacao.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS (visitante)	`corpo.html · headers_https.txt`
Aplicação (front-end)	Download do bundle JS	`bundle_index.js`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io	`ipinfo.json`
Identidade declarada	Base pública da Receita Federal (CNPJ)	`cnpj_publico.json`

3. Identificação Técnica (Domínio, DNS, Hospedagem e TLS)

Domínio	grupopharmalab.store (gTLD .store — Radix)
Registro	**11/06/2026** 16:59:37 UTC · expira 11/06/2027 (validade de 1 ano)
Idade na coleta	**~7 semanas** — domínio recente
Titular	**Não publicado** (o RDAP expõe apenas o registrador)
Registrador	NameCheap, Inc. (IANA 1068) — Phoenix/AZ, EUA
Servidores de nome	ali.ns.cloudflare.com · rustam.ns.cloudflare.com
DNS	A 104.21.94.166 · 172.67.138.22 · AAAA 2606:4700:30xx:: · **sem MX** · sem TXT
Hospedagem	AS13335 Cloudflare (anycast, PoP GRU) — origem não exposta
Certificado TLS	CN=grupopharmalab.store · Google Trust Services WE1 (DV) · válido 26/07/2026–24/10/2026
Domínio canônico declarado	**ambalocacao.com** — registrado 06/03/2026 (Realtime Register B.V.)
Estado do canônico	**client hold** + delete/renew/transfer/update prohibited · NS `NS1/NS2.SUSPENDED-DOMAIN.COM` · **não resolve**
Identidade exibida	"Disk Caçambas - Soluções Ambientais" · CNPJ 19.142.610/0001-58
CNPJ na Receita Federal	**DAL COL ENGENHARIA E GESTAO AMBIENTAL LTDA** — ATIVA desde 25/10/2013, **Itararé/SP**, micro empresa
Canal de atendimento	WhatsApp — exibe (11) 94665-9960, mas o clique abre `wa.me/message/AJ3YNFFR2NRAM1` (link curto)
Rastreamento	**Nenhum** — sem pixel, GTM, analytics ou rastreador de campanha

Leitura técnica. Há uma dissociação completa entre **nome do endereço** ("grupopharmalab", setor farmacêutico), **serviço anunciado** (locação de caçambas), **domínio canônico** (ambalocacao.com, suspenso) e **identidade empresarial** (empresa ativa de Itararé/SP). Um site legítimo não declara como endereço canônico um domínio que o registrador colocou em `client hold`: esse

estado retira o domínio do DNS e é aplicado, tipicamente, após denúncia de abuso ou dados de titularidade inválidos. O certificado DV gratuito comprova apenas o controle do domínio, **não a identidade de qualquer empresa**. A ausência de MX indica que não existe e-mail próprio no domínio — todo contato passa por WhatsApp. Não se imputa conduta ao registrador, à Cloudflare nem à empresa cujo CNPJ é exibido no site.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site é uma **SPA React/Vite** de página única, servida atrás da Cloudflare. O bundle público (`bundle_index.js`, 640 KB) foi gerado em **modo de desenvolvimento** e publicado assim: preserva chamadas `jsxDEV`, atributos `data-loc` e os caminhos absolutos da máquina do desenvolvedor (`/home/ubuntu/disk-cacambas-novo/client/src/pages/Home.tsx`), o que permitiu ler integralmente a lógica da página. O quadro abaixo reúne as declarações e os mecanismos extraídos dele.

Item verificado	Constatação
Título / SEO	`"Aluguel de Caçamba SP | Disk Caçambas - São Paulo e Região"`
canonical e og:url	`https://ambalocacao.com/` — domínio suspenso (client hold), não resolve
CNPJ declarado (3 ocorrências)	`"Disk Caçambas - Soluções Ambientais, CNPJ: 19.142.610/0001-58"`
CNPJ na base pública	DAL COL ENGENHARIA E GESTAO AMBIENTAL LTDA · ATIVA · Itararé/SP · CNAE 4930-2/02 (transporte de carga) + coleta/disposição de resíduos
Distância declarada vs. sede	Site anuncia "todo o estado de São Paulo" e telefone DDD 11; sede do CNPJ em Itararé/SP (~320 km da capital)
Verificação de cobertura	Consulta viacep.com.br e responde "Área de cobertura confirmada!" para qualquer CEP válido do Brasil
Fluxo de contratação	"01 Solicite via WhatsApp · 02 Confirme e Pague · 03 Entrega Rápida · 04 Retirada Agendada"
Meios de pagamento	"Pix, Cartão ou Boleto Bancário" — **combinados no WhatsApp**; não há carrinho, checkout nem gateway no site
Preços anunciados	3 m³ R$ 180 · 4 m³ R$ 260 · 5 m³ R$ 340 · 7 m³ R$ 430 · 10 m³ R$ 500
Depoimentos	3 avaliações com fotos de banco de imagens (images.unsplash.com)
Build publicado	Bundle de desenvolvimento em produção (jsxDEV, data-loc, /home/ubuntu/disk-cacambas-novo/)

Aspecto	Constatação
Tipo de serviço	Locação de caçambas estacionárias (3 a 10 m³) com "descarte regularizado"
Tecnologia	SPA React/Vite atrás da Cloudflare · imagens em Amazon CloudFront · sem back-end próprio detectado
Meio de pagamento	**Antecipado, fora do site** — Pix/cartão/boleto acertados em conversa de WhatsApp
Rastreabilidade do recebedor	**Nenhuma** — não há chave Pix, gateway, CNPJ de cobrança nem nota fiscal expostos
Dados coletados no site	Apenas o CEP (consulta ViaCEP); os demais dados são pedidos no WhatsApp
Identidade declarada	**CNPJ de empresa real e distante**, sem vínculo demonstrado com o domínio
Área de cobertura	**Fabricada** — qualquer CEP do país é "confirmado"
Prova social	Depoimentos com fotos de banco de imagens; "© 2021–2026" em domínio de 7 semanas
Rede	Substitui **ambalocacao.com** (mesma aplicação), suspenso pelo registrador
Conformidade setorial	Nenhuma referência a licença municipal de caçamba, CTR/MTR ou destinação licenciada de resíduos

Leitura técnica. O risco aqui não está em uma função maliciosa no código — o site é uma página de captação simples, sem checkout e sem coleta de cartão. O risco está na **estrutura econômica**: o consumidor é levado a **pagar antes de receber**, em

conversa privada de WhatsApp, a um beneficiário que o site não identifica, sob a identidade de uma empresa que fica a 320 km da região anunciada e cujo vínculo com o domínio não se demonstra. A "confirmação de cobertura" que aprova qualquer CEP do Brasil mostra que a promessa de atendimento local não corresponde a nenhuma operação logística verificável — é apenas um recurso de conversão. Somado ao fato de que o endereço canônico declarado **já foi suspenso pelo registrador** e que o domínio atual nada tem a ver com o ramo, o conjunto descreve um endereço **descartável e rotativo**, montado para receber pagamento antecipado. Não se imputa conduta aos provedores de infraestrutura (NameCheap, Cloudflare, Amazon) nem à empresa cujo CNPJ é exibido.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Site declara como endereço canônico ambalocacao.com, domínio sob "client hold" (suspenso pelo registrador) e que não resolve	`corpo.html` · `rdap_ambalocacao.json`	ALTA
2	Pagamento antecipado combinado exclusivamente por WhatsApp, sem checkout, gateway, chave Pix ou nota fiscal identificáveis	`bundle_index.js`	ALTA
3	Exibe o CNPJ e o nome fantasia de empresa real e ativa sediada a ~320 km da área anunciada, sem vínculo demonstrado	`bundle_index.js` · `cnpj_publico.json`	ALTA
4	"Verificação de área de cobertura" aprova qualquer CEP válido do Brasil — cobertura fabricada	`bundle_index.js`	ALTA
5	Nome do domínio ("grupopharmalab") sem qualquer relação com o serviço vendido — endereço reaproveitado	`rdap_raw.json` · `corpo.html`	MÉDIA
6	Domínio com ~7 semanas, titular não publicado, sem MX, atrás de Cloudflare	`rdap_raw.json` · `dns_records.txt`	MÉDIA
7	Depoimentos com fotos de banco de imagens e "© 2021–2026" em domínio recém-registrado	`bundle_index.js`	MÉDIA
8	Bundle de desenvolvimento publicado em produção, com caminhos internos da máquina do desenvolvedor	`bundle_index.js`	BAIXA
9	Nenhuma referência a licença municipal de caçamba ou a destinação licenciada de resíduos, apesar de prometer "descarte regularizado"	`bundle_index.js`	BAIXA

Síntese: 4 indicadores de severidade ALTA, 3 MÉDIA e 2 BAIXA. Como **fator de legitimidade** registra-se apenas que o CNPJ exibido existe, está ativo e atua no ramo de resíduos — mas nenhuma evidência liga esse CNPJ ao domínio investigado, e o próprio site aponta como endereço oficial um domínio suspenso.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 29/07/2026, conclui-se que **grupopharmalab.store** é um **endereço substituto de alto risco**: registrado há sete semanas com um nome sem relação alguma com o serviço que anuncia, serve a mesma aplicação de **ambalocacao.com** — domínio colocado em `client hold` pelo registrador e hoje fora do DNS —, exibe o CNPJ de uma empresa real sediada a 320 km da área anunciada sem qualquer vínculo demonstrável, aprova cobertura para qualquer CEP do país e concentra a cobrança em **pagamento antecipado por WhatsApp**, sem checkout, chave Pix, gateway ou nota fiscal identificáveis. Classifica-se o caso como **RISCO ALTO** ao consumidor. Registra-se expressamente que **não se imputa conduta ilícita à empresa cujo CNPJ é exibido**, que pode ser vítima de apropriação de identidade.

Recomendações ao consumidor / solicitante

- **Não pagar antecipadamente** por Pix, cartão ou boleto combinados em conversa de WhatsApp, sem contrato, nota fiscal e identificação do recebedor.

- Antes de contratar caçamba, **confirmar o fornecedor por canais independentes**: consultar o CNPJ na base pública da Receita Federal, ligar para o telefone cadastrado da empresa (não o do anúncio) e verificar na prefeitura se a caçamba terá **licença/autorização de ocupação da via** e destinação licenciada.
- Desconfiar de site cujo **nome de domínio não tem relação com o serviço** e cuja "verificação de cobertura" aprova qualquer endereço.
- Se já houve pagamento: acionar o banco e o mecanismo **MED** do Pix (ou o estorno do cartão), reunir comprovantes e prints da conversa, e registrar Boletim de Ocorrência e reclamação em **consumidor.gov.br**.

Recomendações de mitigação / denúncia

- Denunciar o domínio `grupopharmalab.store` aos canais de *abuse* do registrador (NameCheap) e da **Cloudflare**, anexando este laudo e apontando a reincidência em relação a `ambalocacao.com`, já suspenso.
- Comunicar a empresa titular do CNPJ 19.142.610/0001-58 para que avalie medidas quanto ao **uso do seu nome fantasia e da sua inscrição** por terceiro não identificado.
- Reportar ao **Procon** a oferta de serviço com identificação empresarial não comprovada e pagamento antecipado fora de ambiente de pagamento.
- Preservar este relatório e as evidências (pasta `evidencias/`, com hashes SHA-256) para eventual uso administrativo ou judicial.

*Ressalva metodológica: este laudo baseia-se em fontes abertas e reflete o estado do domínio na data indicada. Nenhuma contratação foi feita, nenhum contato por WhatsApp foi iniciado e nenhum dado pessoal foi enviado; o beneficiário do pagamento não foi determinado porque isso exigiria simular uma contratação, o que não foi feito. O vínculo entre o domínio e a empresa cujo CNPJ é exibido **não foi demonstrado nem descartado** — descreve-se o fato, sem imputar conduta a essa empresa. A classificação expressa um juízo técnico de risco e não substitui decisão de autoridade policial, administrativa ou judicial. Não se imputa conduta ilícita aos provedores de infraestrutura (NameCheap, Realtime Register, Cloudflare, Amazon).*

Anexo A — Manifesto de Integridade (SHA-256)

Hashes SHA-256 das evidências preservadas no momento da coleta (cadeia de custódia).

Arquivo	SHA-256
`bundle_index.js`	`3ad8fa59c6bb7619361efc6d97aec5aedf6834fc704295d04f1620efeec0443d`
`cnpj_publico.json`	`ac1efd8ecbcbe180829a9f652e1f759163c0209c653f3b1700d495b300cca056`
`corpo.html`	`18080b46a3d2cfb8da05ad15ea105a72d9e9c4a870813756d53e0c79c2423a13`
`dns_records.txt`	`8cb5c214934ee3c36d22c9d228c20f88067fcb60cfd9c54bbba9e7252a455a99`
`headers_https.txt`	`c5661dac30a877959462e590b594429815910a9e3d76dd8ed58e21bcef09da5a`
`ipinfo.json`	`e35c28593e4468916b34fa1b56607e111d445773f4122a9beb5e9e1d655edbae`
`rdap_ambalocacao.json`	`fd8d67d01e1f535bf6d264a7add71187c38c3f86fe5665148c4199c3dc5d08c1`
`rdap_raw.json`	`27518d8b273835a7b912d16790d42e8fac7e136a51088c7985a35f76f93f4eb7`
`tls_cert.txt`	`f5b308fcf9ef9ccce68fd143017decbb0785e491019ca1f61310c262c77aeb7d`

— Fim do relatório —