RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

joaodiskgaspedidos.shop

Objeto investigado	joaodiskgaspedidos.shop — loja de entrega de gás de cozinha e água mineral (gTLD .shop)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	28/07/2026 (RDAP, DNS, HTTP/TLS, geolocalização, bundle JS, validação de CNPJ)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do app · verificação de dígitos do CNPJ
Achado central	CNPJ declarado no rodapé é inexistente (malformado, 15 dígitos), o checkout é servido por um subdomínio gratuito com erro ortográfico e o site é espelhado em um segundo domínio recém-registrado
Classificação	**RISCO ALTO**
Emissão do laudo	28/07/2026 às 04:06

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **joaodiskgaspedidos.shop**, realizada em **28/07/2026** 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 compra. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

O domínio **está no ar** e entrega uma loja em português intitulada "João Disk Gás | Entrega de Gás e Água em até 30 min", que oferece botijões P13/P20/P45 e galões de água mineral com **pagamento por Pix**, "frete grátis" e cupom "JOAO10". É uma aplicação React/Vite **gerada na plataforma Lovable** — o IP resolve para `lovable-app-cd-1-4.p.l5e.io` — com back-end **Supabase**. O domínio foi **registrado em 02/07/2026**, cerca de quatro semanas antes da coleta.

O achado mais direto é documental: o rodapé do site declara **"João Disk Gás Ltda. — CNPJ: 67.667.9700/0001-01"**. Esse número **não é um CNPJ válido**: tem **15 dígitos** (o CNPJ tem 14) e nenhum truncamento de 14 dígitos produz dígitos verificadores compatíveis pelo algoritmo do módulo 11. Ou seja, a inscrição empresarial exibida **não existe** e nunca poderia existir. Ainda assim, o FAQ do próprio site afirma ao cliente que "o PIX é processado em ambiente bancário e vai para a conta da João Disk Gás (**CNPJ ativo**)" — uma afirmação desmentida pelo número que o site publica.

A estrutura reforça o diagnóstico. As metatags canônicas do site apontam para um **segundo domínio**, `joaodiskgaseaguaentregas.shop`, registrado em **23/06/2026** no mesmo registrador e com os mesmos servidores de nome — o mesmo site espelhado em endereços recém-criados. O checkout não roda no domínio da loja: é delegado a `chekoutsegurotransactions.lovable.app`, um **subdomínio gratuito** da plataforma Lovable cujo nome, além de genérico ("checkout seguro"), traz um **erro ortográfico** ("chekout"). A tabela de configuração de pagamento no Supabase expõe chaves como `manual_pix_key`, `manual_pix_name` e `blackcat_enabled`, indicando que a cobrança pode ser feita por **chave Pix avulsa cadastrada manualmente** — sem vínculo verificável com qualquer pessoa jurídica.

Por fim, os elementos de persuasão são fabricados: contador regressivo do cupom, aviso de que "restam N unidades no seu bairro hoje", avaliações com foto e uma lista de bairros atendidos que é **genérica e fixa no código** ("Centro", "Vila Nova", "Jardim das Flores", "Bairro Alto", "Parque Industrial") — nomes que existem em quase toda cidade brasileira, incompatíveis com uma operação real de entrega, que depende de área de cobertura definida.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: uma loja que recebe por Pix, coleta CPF e endereço, publica um **CNPJ inexistente**, afirma no FAQ que o CNPJ está ativo e delega o pagamento a um subdomínio gratuito com o nome escrito errado oferece **risco elevado**. Recomenda-se **não comprar, não pagar e não fornecer dados** (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 (GMO Registry/.shop — registrador Name.com)	`rdap_raw.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	`app_index.js`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · PTR reverso	`ipinfo.json`
Identidade declarada	Validação do CNPJ pelo algoritmo do módulo 11	`app_index.js`
Domínio espelho	RDAP (joaodiskgaseaguaentregas.shop)	`app_index.js`

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

Domínio	joaodiskgaspedidos.shop (gTLD .shop — GMO Registry)
Registro	**02/07/2026** · expira 02/07/2027 (validade de 1 ano)
Idade na coleta	**~4 semanas** — domínio muito recente
Titular	**Não publicado** (RDAP do registro expõe apenas o registrador)
Registrador	Name.com, Inc. (IANA 625)
Servidores de nome	ns1hwy · ns2fln · ns3fqs · ns4jnz.name.com
DNS — A	185.158.133.1 · sem AAAA · **sem MX** · sem TXT
Hospedagem	AS13335 Cloudflare (anycast) — PTR `lovable-app-cd-1-4.p.l5e.io`, infraestrutura da plataforma **Lovable**
Servidor web	Server: cloudflare · cabeçalho `x-deployment-id` · `/~flock.js`
Certificado TLS	CN=joaodiskgaspedidos.shop · emissor Google Trust Services WE1 (DV) · válido 02/07/2026–30/09/2026
Back-end	Supabase — `baqdqzainczqiuadqbpw.supabase.co` (funções save-cart, check-cart, admin)
Checkout	**chekoutsegurotransactions.lovable.app** — subdomínio gratuito de plataforma, com erro ortográfico
Domínio espelho	canonical/og:url apontam para **joaodiskgaseaguaentregas.shop** (registrado 23/06/2026, mesmo registrador e mesmos NS)
Rastreamento	cdn.utmify.com.br (rastreamento de campanhas pagas) · Google Tag Manager

Leitura técnica. Registro de quatro semanas, validade de um ano, titular não publicado e ausência de e-mail próprio (sem MX) compõem um perfil de **baixa rastreabilidade**, incompatível com uma revenda de gás estabelecida — atividade que, no Brasil, é regulada pela ANP e exige instalações físicas licenciadas. A hospedagem em uma **plataforma de geração de aplicações por IA** (Lovable) e a presença do rastreador **Utmify**, típico de campanhas pagas de tráfego, indicam uma operação montada para captar cliques rapidamente. O certificado DV gratuito comprova apenas o controle do domínio, **não a identidade de qualquer empresa**. Não se imputa conduta ao registrador, à Cloudflare, à Lovable nem à Supabase, meros provedores de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

A loja é uma SPA React/Vite com carrinho, cupom e checkout externo. O quadro abaixo reúne as declarações e os mecanismos extraídos do bundle JavaScript público (`app_index.js`).

Item verificado	Constatação
CNPJ no rodapé	`"João Disk Gás Ltda. — CNPJ: 67.667.9700/0001-01"`
Validação do número	`15 dígitos (CNPJ tem 14); nenhum truncamento de 14 gera DV válido pelo módulo 11 → INEXISTENTE`
Afirmação no FAQ	`"O PIX é processado em ambiente bancário e vai para a conta da João Disk Gás (CNPJ ativo)"`
Checkout	`https://chekoutsegurotransactions.lovable.app (subdomínio gratuito; "chekout" grafado errado)`
Config. de pagamento (Supabase)	`payment_settings: pix_enabled, card_enabled, manual_pix_enabled, manual_pix_key, manual_pix_name ("JOAO DISK GAS"), manual_pix_city, blackcat_enabled`
Domínio espelho (canonical)	`https://joaodiskgaseaguaentregas.shop/ · /checkout · /obrigado`
Bairros atendidos (fixos no código)	`"Centro", "Vila Nova", "Jardim das Flores", "Bairro Alto", "Parque Industrial"`
Gatilhos de urgência	`"Restam N unidades no seu bairro hoje" · contador regressivo do cupom JOAO10 · avaliações com foto`

Aspecto	Constatação
Tipo de serviço	Entrega de botijão de gás (P13/P20/P45) e água mineral, com promessa de 30 minutos
Tecnologia	SPA React/Vite gerada na plataforma **Lovable** · back-end **Supabase** · Cloudflare
Meio de pagamento	Pix e cartão, processados fora do domínio da loja, em subdomínio gratuito de plataforma
Chave Pix	**Pode ser avulsa** — a configuração prevê `manual_pix_key` cadastrada manualmente, sem vínculo verificável com pessoa jurídica
Dados coletados	CPF, nome, e-mail, CEP, número e bairro (endereço completado via ViaCEP)
Identidade declarada	**CNPJ inexistente** — 67.667.9700/0001-01 é malformado e não valida
Coerência das afirmações	**Contraditória** — o FAQ garante "CNPJ ativo" enquanto o rodapé publica um número impossível
Área de cobertura	**Genérica** — lista de bairros fixa no código, com nomes comuns a qualquer cidade
Prova social	Avaliações com foto e alertas de escassez gerados pelo próprio front-end
Rede	Espelhado em **joaodiskgaseaguaentregas.shop** (registrado 9 dias antes, mesmo registrador e NS)

Leitura técnica. Revenda de GLP é atividade **regulada pela ANP**, que exige autorização, instalações licenciadas e pessoa jurídica identificada. Aqui não há nenhuma das três: o CNPJ publicado é **impossível**, a área de cobertura é uma lista genérica escrita no código e o pagamento sai do domínio da loja para um **subdomínio gratuito** de plataforma, cujo nome transmite segurança ("checkout seguro transactions") mas está grafado errado — sinal recorrente de montagem apressada. A previsão de **chave Pix manual** significa que o dinheiro pode ir para uma chave avulsa, dissociando quem recebe de quem anuncia. Os gatilhos de urgência e as avaliações são gerados pelo próprio front-end, isto é, **não refletem demanda ou clientes reais**. O conjunto — domínio de quatro semanas, espelho recém-criado, CNPJ inexistente e checkout terceirizado a subdomínio gratuito — descreve uma loja montada para **receber pagamentos sem responsabilidade identificável**. Não se imputa conduta aos provedores de infraestrutura nem a intermediários de pagamento citados.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	CNPJ declarado no rodapé é inexistente: 15 dígitos e sem dígitos verificadores válidos	`app_index.js`	ALTA
2	FAQ afirma ao cliente que o Pix vai para a conta da empresa com "CNPJ ativo", contradizendo o número publicado	`app_index.js`	ALTA
3	Checkout delegado a subdomínio gratuito de plataforma, com o nome grafado errado ("chekoutsegurotransactions")	`app_index.js`	ALTA
4	Configuração de pagamento prevê chave Pix avulsa cadastrada manualmente, sem vínculo com pessoa jurídica	`app_index.js`	ALTA
5	Site espelhado em joaodiskgaseaguaentregas.shop, registrado 9 dias antes no mesmo registrador — rotação de endereços	`corpo.html` · `app_index.js`	MÉDIA
6	Domínio com ~4 semanas, sem MX, titular não publicado, hospedado em plataforma de geração de apps	`rdap_raw.json` · `dns_records.txt`	MÉDIA
7	Área de cobertura genérica fixa no código, incompatível com operação real de entrega	`app_index.js`	MÉDIA
8	Escassez e avaliações fabricadas pelo próprio front-end	`app_index.js`	MÉDIA
9	Venda de GLP sem qualquer referência a autorização da ANP ou a instalação física	`corpo.html` · `app_index.js`	MÉDIA
10	Coleta de CPF para uma entrega de botijão, sem necessidade aparente	`app_index.js`	BAIXA

Síntese: 4 indicadores de severidade ALTA, 5 MÉDIA e 1 BAIXA. **Nenhum fator de legitimidade** (CNPJ válido, endereço físico, autorização da ANP, área de cobertura real, checkout no próprio domínio) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 28/07/2026, conclui-se que **joaodiskgaspedidos.shop** é uma **loja online de alto risco**: criada há cerca de quatro semanas em plataforma de geração de aplicações, espelhada em um segundo domínio igualmente recente, que anuncia entrega de gás e água com pagamento por Pix enquanto publica no rodapé um **CNPJ inexistente** — e afirma ao cliente, no próprio FAQ, que esse CNPJ está ativo. O pagamento é delegado a um **subdomínio gratuito** de plataforma com o nome grafado errado, a configuração admite **chave Pix avulsa**, e a área de cobertura, a escassez e as avaliações são fabricadas no código. Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não comprar, não pagar por Pix e não fornecer CPF, endereço ou dados de cartão** ao site.
- Antes de comprar gás, **confirmar o CNPJ** do revendedor na base pública da Receita Federal e verificar a autorização na **ANP**: revenda de GLP exige instalação física licenciada e pessoa jurídica identificada.
- Desconfiar de entrega de botijão com preço muito abaixo do praticado no bairro, cupom com contagem regressiva e "unidades restantes" — são gatilhos gerados pelo site, não indicadores de estoque.
- Se já houve pagamento: acionar o banco e o mecanismo **MED** do Pix, reunir comprovantes e prints, e registrar Boletim de Ocorrência e reclamação em **consumidor.gov.br**.

Recomendações de mitigação / denúncia

- Denunciar os domínios `joaodiskgaspedidos.shop` e `joaodiskgaseaguaentregas.shop` aos canais de *abuse* do registrador (Name.com), da Cloudflare e da **Lovable** — esta última também responsável pelo subdomínio de checkout `chekoutsegurotransactions.lovable.app` —, anexando

este laudo.

- Comunicar a **ANP** e o **Procon** sobre a oferta de revenda de GLP por pessoa jurídica inexistente.
- 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 compra foi realizada e nenhum dado pessoal foi enviado; o recebedor final do Pix não foi determinado porque isso exigiria simular um pedido, o que não foi feito. 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 (Name.com, Cloudflare, Lovable, Supabase) nem a intermediários de pagamento.

Anexo A — Manifesto de Integridade (SHA-256)

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

Arquivo	SHA-256
`app_index.js`	`0c99cabec53e1fcc15255fc4898007ad1ea3bb39944d83427d422f7866cc2593`
`corpo.html`	`68ecac2c31dee1da1eaa6308dd5971723e49dc8b6d0c25b85fa6c91499cb7d5e`
`dns_records.txt`	`bf3e9b13e929271ffbce8c8006b92f1a3dc2d7afeb25b86c763103ce2a82f2e8`
`headers_https.txt`	`90ced9f527bbe3e3a8a59d11e44b2976282dc00ed5a1327a72936e100fd5ec3a`
`ipinfo.json`	`f3de4534eb304f6b11755d5092960c41b83eb6bcf64b805dc41d0f172d6870b3`
`rdap_raw.json`	`865b853508a0beff231edf33b1c36740657f5d120f23de11d8f3e82de70e70df`
`tls_cert.txt`	`8f29926e0a1e5aec284cd897d2b4a3c2d8e6987ff26a7b84a9f947935735f891`

— Fim do relatório —