
# RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

**gaseaguadojota.online**

| | |
|---|---|
| **Objeto investigado** | gaseaguadojota.online — loja de entrega de gás de cozinha e água mineral (gTLD .online) |
| **Natureza** | Verificação de legitimidade e de risco ao consumidor |
| **Data da coleta** | 28/07/2026 (RDAP, DNS, HTTP/TLS, geolocalização, JavaScript da loja e do checkout, base pública de CNPJ) |
| **Métodos** | OSINT passivo · RDAP · DNS · HTTP/TLS · análise do checkout · consulta à base pública de CNPJ |
| **Achado central** | O checkout captura número, validade, CVV e a SENHA do cartão, envia tudo ao servidor e sempre exibe "recusado" — não há nenhuma integração com adquirente no fluxo de cartão |
| **Classificação** | **RISCO ALTO** |
| **Emissão do laudo** | 28/07/2026 às 04:09 |

## 1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **gaseaguadojota.online**, 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, de cartão ou de senha, 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 de entrega de **botijão de gás e água mineral**, exibindo as marcas **Liquigás, Ultragaz, Copagaz e Supergasbras** e prometendo entrega em 40 minutos. É uma página estática servida por **Apache** em hospedagem compartilhada da **HostGator Brasil**. O domínio foi **registrado em 04/07/2026**, cerca de três semanas antes da coleta.

O achado central está no **checkout** (`/checkout.html`), cujo código é público e foi lido integralmente. Ao escolher pagamento com cartão, a função `processarCartao()` coleta **número do cartão** (validado localmente pelo algoritmo de Luhn), **nome do titular**, **validade** e **CVV**, e envia tudo para `api.php` com o rótulo `etapa: 'cartao'`. A tela exibe então uma animação de "validando" por 3 segundos e, em seguida, **pede a senha do cartão** — "Digite entre 4 e 6 dígitos" — com um cronômetro regressivo criando pressão. Confirmada a senha, a função `processarCartaoEtapa2()` reenvia ao servidor **os dados do cartão somados à senha**, sob o rótulo `etapa: 'cartao_com_senha'`. Quatro segundos depois, a tela **sempre** exibe "recusado" e oferece "tentar outro cartão" ou migrar para o Pix.

Não existe, em nenhum ponto desse fluxo, **qualquer integração com adquirente, gateway ou antifraude**: não há tokenização, não há redirecionamento a instituição de pagamento e a resposta de recusa é um `setTimeout` fixo no próprio navegador. O cartão **nunca é cobrado**. A única função do fluxo de cartão é **capturar dados**. Nenhum estabelecimento legítimo solicita a senha do cartão em página web — a senha é digitada apenas em terminal (maquininha) ou no aplicativo do banco.

A identidade da loja confirma o quadro. O HTML estático exibe "Distribuidora Max Gás" com o CNPJ marcador **00.000.000/0001-00**, mas o nome, o CNPJ, o WhatsApp e a logomarca são **injetados em tempo de execução** a partir de `/admin/cfg.php`, que devolveu **"Disk Gás do Jota"** e o CNPJ **21.465.107/0001-85**. A consulta à base pública da Receita Federal mostra que esse CNPJ pertence a **"21.465.107 RENATO CESAR VONO"**, situação cadastral **BAIXADA**, aberta em 2014 em **Salvador/BA**, com CNAE de **comércio varejista de artigos de óptica** e capital social de R$ 1 — ou seja, uma empresa **inativa**, de **outro ramo** e **outro estado**. Trata-se de um **kit white-label**: o operador troca marca, CNPJ e contato pelo painel, sem tocar no site.

Há ainda um vínculo técnico revelador: o certificado TLS servido pelo domínio tem **CN=recargacelularfacil.online** — outro domínio, registrado em **04/07/2026 às 18:14:04**, **menos de meio segundo antes** de gaseaguadojota.online, no mesmo registrador e com os mesmos servidores de nome da HostGator. Os dois endereços foram **registrados em lote** e residem na mesma hospedagem.

| CLASSIFICAÇÃO DE RISCO | RISCO ALTO |
|---|---|

Leitura: o checkout deste site pede o **número, o CVV e a senha do cartão**, envia tudo a um servidor próprio e nunca cobra nada — é **captura de credenciais**, não um pagamento. Recomenda-se **não comprar, não digitar dados de cartão, jamais informar a senha** e, se já houver informado, **bloquear o cartão imediatamente** (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/.online — registrador Hostinger) | `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 (loja) | Extração do JavaScript embutido na página | `app_inline.js` |
| Configuração da loja | GET público em /admin/cfg.php | `admin_cfg.json` |
| Checkout | GET público em /checkout.html e extração do JS | `checkout.html · checkout_app.js` |
| Certificado TLS | openssl s_client / x509 | `tls_cert.txt` |
| Geolocalização do IP | ipinfo.io · PTR reverso | `ipinfo.json` |
| Identidade declarada | Base pública de CNPJ (Receita Federal, via BrasilAPI) | `cnpj_publico.json` |

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

| | |
|---|---|
| **Domínio** | gaseaguadojota.online (gTLD .online — Radix) |
| **Registro** | **04/07/2026 18:14:04 UTC** · expira 04/07/2027 (validade de 1 ano) |
| **Idade na coleta** | **~3 semanas** — domínio muito recente |
| **Titular** | **Redigido** no RDAP (o registro informa remoção do contato do titular) |
| **Registrador** | HOSTINGER operations, UAB (Vilnius, Lituânia) |
| **Servidores de nome** | ns1170.hostgator.com.br · ns1171.hostgator.com.br |
| **DNS — A** | 162.241.203.210 · sem AAAA · MX mail.gaseaguadojota.online · TXT `v=spf1 a mx include:websitewelcome.com ~all` |
| **Hospedagem** | AS31898 Oracle (Vinhedo/SP) — PTR `162-241-203-210.unifiedlayer.com`, hospedagem compartilhada HostGator |
| **Servidor web** | Server: Apache · página estática de ~290 KB, sem framework |
| **Certificado TLS** | **CN=recargacelularfacil.online** — certificado de **outro domínio** · emissor Let's Encrypt YR2 · válido 07/07/2026–05/10/2026 |
| **Domínio irmão** | **recargacelularfacil.online** — registrado em **04/07/2026 18:14:04 UTC**, menos de meio segundo antes, mesmo registrador e mesmos NS |
| **Painel administrativo** | `/admin/cfg.php` — endpoint público que devolve nome, CNPJ, prazo e logomarca da loja |

**Leitura técnica.** Registro de três semanas, validade de um ano e titular redigido compõem um perfil de **baixa rastreabilidade**. O ponto mais informativo é o **certificado TLS emitido para outro domínio**: em hospedagem compartilhada isso ocorre quando vários sites do mesmo operador dividem o mesmo servidor e certificado. Somado ao registro dos dois domínios **na mesma fração de segundo**, com o mesmo registrador e os mesmos servidores de nome, o vínculo entre `gaseaguadojota.online` e `recargacelularfacil.online` é **tecnicamente demonstrado**: são endereços registrados em lote pelo mesmo operador. A existência de um endpoint público `/admin/cfg.php` que define a identidade exibida revela um **kit reaproveitável**, e não uma loja própria. Não se imputa conduta à Hostinger, à HostGator nem à Oracle, meros provedores de infraestrutura.

## 4. Plataforma, Fluxo de Pagamento e Dados Coletados

A loja é uma página estática com carrinho em JavaScript; o pagamento ocorre em `/checkout.html`, cujo código também é público. Os trechos abaixo são transcrições literais desse código (`checkout_app.js`), na ordem em que são executados.

| Etapa do checkout (código literal) | O que acontece |
|---|---|
| 1. Coleta dos dados do cartão | `cardDataGlobal={numero:v('cardNum'), nome:v('cardName'), validade:v('cardExp'), cvv:v('cardCvv'), parcelas:'1'}` |
| 2. Envio ao servidor | `fetch('api.php',{method:'POST', body: JSON.stringify({etapa:'cartao', ...cardDataGlobal, ...orderAddrGlobal})})` |
| 3. Tela falsa de validação | `setEstado('validando'); … // comentário do código: "Após 3s vai para senha"` |
| 4. Pedido da senha do cartão | `setEstado('senha'); document.getElementById('senhaApp').focus(); iniciarTimer(); // "Digite entre 4 e 6 dígitos"` |
| 5. Envio do cartão + senha | `fetch('api.php',{method:'POST', body: JSON.stringify({etapa:'cartao_com_senha', ...cardDataGlobal, ...orderAddrGlobal, senha})})` |
| 6. Recusa sempre | `setTimeout(()=>{ … setEstado('recusado'); },4000)` — resultado fixo no navegador, sem consulta a adquirente |
| 7. Saídas oferecidas | `tentarOutroCartao()` — limpa os campos e pede outro cartão · `irParaPix()` — migra o pedido para Pix |
| Integração com adquirente | `Nenhuma — sem tokenização, sem gateway, sem redirecionamento a instituição de pagamento` |

| Aspecto | Constatação |
|---|---|
| Tipo de serviço | Entrega de botijão de gás (13/20/45 kg) e água mineral, com promessa de 40 minutos |
| Tecnologia | Página estática em Apache (HostGator compartilhado) · carrinho e checkout em JavaScript · back-end PHP (`api.php`, `/admin/cfg.php`) |
| Fluxo de cartão | **Captura de número, nome, validade, CVV e SENHA**, enviados ao servidor próprio; recusa sempre exibida, cartão nunca cobrado |
| Fluxo de Pix | confirmarPedido() → api.php retorna pix, qr_code e transacao_id (desconto de 5% para induzir à migração após a "recusa") |
| Dados coletados | Nome, telefone, **CPF**, CEP e endereço completo (ViaCEP), além dos dados do cartão e da senha |
| Marca exibida (HTML) | "Distribuidora Max Gás" · CNPJ marcador `00.000.000/0001-00` |
| Marca exibida (em execução) | "Disk Gás do Jota" · CNPJ 21.465.107/0001-85, injetados por `/admin/cfg.php` |
| Verificação do CNPJ | **21.465.107 RENATO CESAR VONO — situação BAIXADA**, aberta 25/11/2014, Salvador/BA, CNAE **comércio varejista de artigos de óptica**, capital social R$ 1 |
| Marcas de terceiros | Liquigás, Ultragaz, Copagaz e Supergasbras exibidas sem comprovação de revenda autorizada |
| Prova social | "847 avaliações verificadas" e depoimentos nominais fixos no HTML · notificações de "pedido realizado agora mesmo" |
| Domínio irmão | recargacelularfacil.online — mesmo servidor, mesmo certificado, registrado na mesma fração de segundo |

**Leitura técnica.** O fluxo de cartão deste site **não é um pagamento com falha**: é uma **coleta de credenciais desenhada como pagamento**. Um checkout real tokeniza o cartão, envia-o a um adquirente e recebe uma resposta de autorização; aqui, os dados vão em texto para um `api.php` do próprio site, a "validação" é uma animação temporizada e a recusa é um `setTimeout` — o resultado é o mesmo para qualquer cartão. A etapa da **senha** não tem nenhuma justificativa técnica em comércio eletrônico e é o elemento que converte o conjunto em captura de credencial bancária completa: número, validade, CVV e senha permitem uso do cartão em canais que exijam apenas esses elementos. A recusa forçada cumpre duas funções: **colher mais de um cartão** ("tentar outro cartão") e **empurrar a vítima para o Pix**, garantindo o pagamento além dos dados. A identidade da loja, por sua vez, é **intercambiável** e apoia-se no CNPJ **baixado** de um terceiro sem relação com o ramo. Não se imputa conduta à pessoa cujo CNPJ aparece (que pode ser vítima de apropriação de identidade), às distribuidoras de gás cujas marcas são exibidas, nem aos provedores de infraestrutura.

## 5. Indicadores de Risco

| # | Indicador | Evidência | Sev. |
|---|---|---|---|
| 1 | Checkout solicita a **senha do cartão** (4 a 6 dígitos) e a envia ao servidor junto com número, validade e CVV | `checkout_app.js` | ALTA |
| 2 | Dados completos do cartão enviados a api.php sem tokenização, gateway ou adquirente | `checkout_app.js` | ALTA |
| 3 | Recusa exibida por temporizador fixo no navegador — o cartão nunca é cobrado; o fluxo existe para capturar dados | `checkout_app.js` | ALTA |
| 4 | Após a "recusa", o site oferece tentar outro cartão ou migrar para Pix com desconto — colheita adicional e pagamento | `checkout_app.js` | ALTA |
| 5 | CNPJ exibido pertence a empresa com situação BAIXADA, de outro ramo (óptica) e outro estado | `admin_cfg.json` · `cnpj_publico.json` | ALTA |
| 6 | Identidade da loja (nome, CNPJ, contato, logo) é intercambiável via /admin/cfg.php — kit white-label | `app_inline.js` · `admin_cfg.json` | ALTA |
| 7 | Certificado TLS emitido para recargacelularfacil.online, domínio registrado na mesma fração de segundo e no mesmo servidor | `tls_cert.txt` · `rdap_raw.json` | MÉDIA |
| 8 | Domínio com ~3 semanas, titular redigido, validade de 1 ano, em hospedagem compartilhada | `rdap_raw.json` | MÉDIA |
| 9 | Marcas Liquigás, Ultragaz, Copagaz e Supergasbras exibidas sem comprovação de revenda autorizada | `corpo.html` | MÉDIA |
| 10 | "847 avaliações verificadas" e notificações de pedido fixas no código | `corpo.html` · `app_inline.js` | MÉDIA |
| 11 | HTML publicado ainda traz o CNPJ marcador 00.000.000/0001-00 | `corpo.html` | BAIXA |

Síntese: 6 indicadores de severidade ALTA, 4 MÉDIA e 1 BAIXA. **Nenhum fator de legitimidade** (CNPJ ativo e coerente, integração real de pagamento, autorização da ANP, identidade estável) foi constatado. Este é o caso de maior gravidade do lote, por envolver **captura de senha de cartão**.

## 6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 28/07/2026, conclui-se que **gaseaguadojota.online** opera um **checkout de captura de credenciais de cartão** disfarçado de loja de entrega de gás e água. O código público do próprio site coleta número, nome, validade, CVV e, em uma segunda etapa cronometrada, a **senha do cartão**, enviando tudo a um `api.php` local — sem qualquer adquirente, gateway ou tokenização — e sempre exibindo "recusado" por temporizador, para então pedir outro cartão ou migrar o pedido para Pix. A identidade da loja é intercambiável por um painel público e apoia-se em um **CNPJ baixado**, de outro ramo e outro estado, e o domínio compartilha servidor e certificado com `recargacelularfacil.online`, registrado na mesma fração de segundo. Classifica-se o caso como **RISCO ALTO** ao consumidor.

### Recomendações ao consumidor / solicitante

- **Não comprar, não digitar dados de cartão e jamais informar a senha do cartão** — nenhum site legítimo pede senha de cartão em página web; a senha só é digitada em maquininha ou no aplicativo do banco.
- **Se já digitou os dados do cartão neste site: bloqueie o cartão imediatamente** pelo aplicativo ou pela central do banco, peça a emissão de um novo número, conteste eventuais lançamentos e registre Boletim de Ocorrência.
- Se já digitou a **senha**: além do bloqueio, **troque a senha** do cartão e do aplicativo bancário, ative alertas de transação e verifique se há empréstimos ou compras não reconhecidas.
- Se pagou por Pix: acionar o banco e o mecanismo **MED** do Pix, reunir comprovantes e prints, e registrar reclamação em **consumidor.gov.br**.
- Antes de comprar gás, confirmar o CNPJ do revendedor na base pública da Receita Federal e a autorização na **ANP** — revenda de GLP exige instalação física licenciada.

### Recomendações de mitigação / denúncia

- Denunciar os domínios `gaseaguadojota.online` e `recargacelularfacil.online` aos canais de *abuse* da **Hostinger** (registrador) e da **HostGator Brasil** (hospedagem), destacando a captura de dados e senha de cartão — situação que costuma justificar remoção imediata —, anexando este laudo.
- Comunicar as bandeiras de cartão e o banco emissor sobre a página de captura, e reportar o endereço aos programas de bloqueio de phishing dos navegadores (Google Safe Browsing e Microsoft SmartScreen).
- Comunicar as distribuidoras **Liquigás, Ultragaz, Copagaz e Supergasbras** sobre o uso de suas marcas, e a **ANP** e o **Procon** sobre a oferta de revenda de GLP por empresa baixada.
- 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. Nenhum dado pessoal, de cartão ou de senha foi enviado ao site e nenhuma compra foi realizada; todo o fluxo descrito foi lido no código JavaScript público servido a qualquer visitante, e o recebedor final do Pix não foi determinado por exigir a simulação de um pedido. A classificação expressa um juízo técnico de risco e não substitui decisão de autoridade policial, administrativa ou judicial. Não se imputa conduta ilícita à pessoa cujo CNPJ é exibido pelo site (que pode ser vítima de apropriação de identidade), às distribuidoras de gás cujas marcas aparecem, nem aos provedores de infraestrutura (Hostinger, HostGator, Oracle).*

## Anexo A — Manifesto de Integridade (SHA-256)

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

| Arquivo | SHA-256 |
|---|---|
| `admin_cfg.json` | `5d5a4027dbbfa052a964c8d4514a8d9a50691c573e75ed43c0b7631b25081b42` |
| `app_inline.js` | `d1947f78496f56fde0bdd754df68eb1a3f1b2c175ec443e71a59983ccde8b1eb` |
| `checkout_app.js` | `57d9f59b72ac79af3088908ed5ab5a2a60a3606eac49642f684e8cd3b29bdb44` |
| `checkout.html` | `e97fce8fb1ae82ff85a41422f218fa22c5bbdd3fe78d4ca898784fbaa43ff1ca` |
| `cnpj_publico.json` | `79410a89238fcfe0298c536d05836399304d7205a4a89b842140a5d3c123f6b0` |
| `corpo.html` | `fa69125e8102bbdc9c009251dd8fb219bda568d8b331ef47d5bc24cd362f69f4` |
| `dns_records.txt` | `a01244bf7069ebc3f8685758fec3d06d989fca06e28a0887c33beddffbbe4d5e` |
| `headers_https.txt` | `0733de918b5cad2b669cae9c63bd58cdc7eac4a1bcc7210f4bbab4bf782dd4d9` |
| `ipinfo.json` | `d7e4b22983c456aaaa3308784ef309e62046d612619075e5dd295bf37295bc0a` |
| `rdap_raw.json` | `29c65eac1a7443614ad73fb75901ae4a8ee6e74a5b525fbdf3e3c68c469b0207` |
| `tls_cert.txt` | `c88291523a67f21c9f5c0401d0afcc5fb3bf58344a33a955ec13c8626ecf000c` |

*— Fim do relatório —*