RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

diskgasdomaxx.online

Objeto investigado	diskgasdomaxx.online — loja de entrega de botijão de gás e água mineral (gTLD .online)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	29/07/2026 (RDAP, DNS, HTTP/TLS, geolocalização, código do checkout, consulta de CNPJ)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do checkout · base pública da Receita Federal · comparação de hashes
Achado central	O checkout pede número, validade, CVV e a SENHA do cartão, sempre exibe "recusado" por temporizador fixo e é BYTE A BYTE IDÊNTICO ao de gaseaguadojota.online, no mesmo servidor — o CNPJ exibido pertence a uma empresa BAIXADA em 2014, de outro ramo
Classificação	**RISCO ALTO**
Emissão do laudo	30/07/2026 às 00:31

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **diskgasdomaxx.online**, 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, 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 intitulada "Entrega de Gás e Água", que anuncia botijões de 13 kg, 20 kg e 45 kg, garrafões de 20 litros, carvão e gelo, com entrega prometida em **40 minutos** e preços entre R$ 79,90 e R$ 105,40 no botijão de 13 kg. A vitrine exibe repetidamente as marcas **Liquigás, Ultragaz, Copagaz, Supergasbras e Fogás**. O domínio foi **registrado em 25/06/2026**, cerca de cinco semanas antes da coleta, com titular não publicado.

O achado central está no arquivo `/checkout.html`. Ao escolher pagamento com cartão, a função `processarCartao()` coleta **número, nome do titular, validade e CVV** e envia tudo a um `api.php` do próprio site sob o rótulo `etapa: "cartao"`. A tela exibe então uma animação de "Validando Cartão" por 3 segundos e pede a **SENHA do aplicativo do banco**, com o aviso literal: *"ATENÇÃO: Você deve informar a senha que usa no seu app. Ela contém 4 a 6 dígitos, e é a mesma que utiliza para acessar a fatura."* Um cronômetro de 2 minutos pressiona o usuário; 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 exibe **"Cartão recusado"** — resultado **fixo**, produzido por um `setTimeout` no próprio navegador, sem qualquer consulta de autorização — e oferece "Pagar com PIX". Em nenhum ponto há adquirente, gateway, tokenização, 3-D Secure ou antifraude: **o cartão nunca é cobrado**, e a única função do fluxo é capturar dados. **Nenhum estabelecimento legítimo pede a senha do cartão em página web** — ela só é digitada em maquininha ou no aplicativo do banco.

A identidade da loja é **trocável por painel**. O HTML estático publica o CNPJ marcador `00.000.000/0001-00`, e o nome, o CNPJ, o WhatsApp e a logomarca são injetados em tempo de execução por **/admin/cfg.php** — endpoint **público, sem autenticação**, que devolveu: `{"nome":"Disk Gás do Max","cnpj":"20.664.210/0001-91","entrega":"40 minutos", "logo":"/admin/uploads/img_1782358333_logo.webp"}`. A consulta à base pública da Receita Federal mostra que esse CNPJ pertence a **"ELIANA FERREIRA DOS SANTOS 04328933507"**, empresário individual com situação cadastral **BAIXADA desde 19/08/2014** por "extinção por encerramento/liquidação voluntária", aberto em 18/07/2014 em **Itaquaquecetuba/SP**, CNAE de **cabeleireiros, manicure e pedicure** e capital social de R$ 1.000. É uma empresa **extinta há cerca de doze anos e de ramo inteiramente diverso**.

Por fim, o caso **não é isolado**. O arquivo `/checkout.html` deste domínio é **byte a byte idêntico** ao do domínio **gaseaguadojota.online**, investigado e publicado por este Observatório em 28/07/2026: ambos têm o hash SHA-256 `e97fce8fb1ae82ff85a41422f218fa22c5bbdd3fe78d4ca898784fbaa43ff1ca`. Os dois domínios resolvem para **o mesmo IP (162.241.203.210)**, usam **os mesmos servidores de nome** (ns1170/ns1171.hostgator.com.br) e **o mesmo registro SPF**. Trata-se do **mesmo kit, no mesmo servidor, com identidades diferentes** — e, no caso do gaseaguadojota.online, o certificado TLS servido era de um terceiro domínio, recargacelularfacil.online.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: **não digite dados de cartão nem senha** neste site. O fluxo de cartão não cobra nada — ele apenas coleta número, CVV e senha e sempre exibe "recusado". A loja é uma fachada reconfigurável, sobre um CNPJ extinto de terceiro, replicada em pelo menos dois domínios no mesmo servidor (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`
Checkout	curl HTTPS de /checkout.html (sem envio de dados)	`checkout.html`
Configuração pública	GET /admin/cfg.php	`cfg_publico.json`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · PTR reverso	`ipinfo.json · ptr.txt`
Identidade declarada	Base pública da Receita Federal (CNPJ)	`cnpj_publico.json`
Correlação de rede	Comparação SHA-256 com o checkout de gaseaguadojota.online	`checkout.html`

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

Domínio	diskgasdomaxx.online (gTLD .online — Radix)
Registro	**25/06/2026** 03:00:37 UTC · expira 25/06/2027 (validade de 1 ano)
Idade na coleta	**~5 semanas** — domínio muito recente
Titular	**Não publicado** (o RDAP expõe apenas o registrador)
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 0 mail.diskgasdomaxx.online · SPF include:websitewelcome.com
Hospedagem	AS31898 (Oracle/Unified Layer) — PTR `162-241-203-210.unifiedlayer.com`, hospedagem compartilhada HostGator Brasil
Servidor web	Apache · last-modified 25/06/2026 (mesma data do registro do domínio)
Certificado TLS	CN=diskgasdomaxx.online · Let's Encrypt YR1 (DV) · válido 25/06/2026–23/09/2026
Identidade injetada	`/admin/cfg.php` (público) → "Disk Gás do Max" · CNPJ 20.664.210/0001-91
CNPJ na Receita Federal	**ELIANA FERREIRA DOS SANTOS 04328933507 — BAIXADA em 19/08/2014** · cabeleireiros/manicure · Itaquaquecetuba/SP
Marcas exibidas	Liquigás · Ultragaz · Copagaz · Supergasbras · Fogás (sem qualquer declaração de autorização ou revenda)
Domínio irmão	**gaseaguadojota.online** — mesmo IP, mesmos NS, mesmo SPF e **checkout com hash SHA-256 idêntico**

Leitura técnica. Domínio de cinco semanas, validade de um ano, titular não publicado e servidor compartilhado compõem um perfil de **baixa rastreabilidade**, incompatível com uma revenda de GLP — atividade regulada pela **ANP**, que exige autorização,

instalações físicas licenciadas e pessoa jurídica identificada. O `last-modified` do HTML coincide com a data de registro do domínio: o site foi publicado no mesmo dia. O certificado DV gratuito comprova apenas o controle do domínio, **não a identidade de qualquer empresa**. A coincidência de IP, de servidores de nome e do hash do checkout com gaseaguadojota.online indica que os endereços são **instâncias do mesmo kit operado pela mesma origem**. Não se imputa conduta ao registrador, à HostGator, à Oracle nem às distribuidoras de gás cujas marcas aparecem na vitrine.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

A loja é um site estático em Apache com identidade carregada em tempo de execução. O checkout (`/checkout.html`, 94.003 bytes) foi lido integralmente, sem preencher nenhum campo. O quadro abaixo reproduz o fluxo tal como escrito no código.

Etapa do checkout	O que o código faz
1 — Dados do pedido	`Coleta nome, telefone, CPF, CEP, rua, número, bairro, cidade e complemento (CEP completado via ViaCEP)`
2 — Cartão	`processarCartao(): envia numero, nome, validade e cvv a api.php com etapa:"cartao"`
3 — "Validando Cartão"	`Popup com animação por 3 segundos (setTimeout), sem qualquer consulta de autorização`
4 — Senha do banco	`"ATENÇÃO: Você deve informar a senha que usa no seu app. Ela contém 4 a 6 dígitos, e é a mesma que utiliza para acessar a fatura." — cronômetro de 02:00`
5 — Envio da senha	`processarCartaoEtapa2(): envia etapa:"cartao_com_senha" com todos os dados do cartão mais a senha`
6 — "Cartão recusado"	`setEstado("recusado") disparado por setTimeout de 4 s — resultado fixo, no navegador`
7 — Migração para Pix	`Botão "Pagar com PIX"; o total ganha 5% de desconto no Pix`
8 — Pix e comprovante	`api.php devolve pix, qr_code e transacao_id; polling api.php?action=status a cada 5 s; modal pede o upload do comprovante`
Identidade da loja	`/admin/cfg.php injeta nome, CNPJ, WhatsApp e logo em tempo de execução (HTML publica 00.000.000/0001-00)`

Aspecto	Constatação
Tipo de serviço	Entrega de botijão de gás (13/20/45 kg), água mineral 20 L, carvão e gelo, prometida em 40 minutos
Tecnologia	HTML estático + JavaScript em Apache (HostGator) · back-end `api.php` próprio
Fluxo de cartão	**Captura de credenciais** — número, validade, CVV e **senha do app do banco**, sem adquirente
Resultado do pagamento	**"Recusado" fixo** — decidido por temporizador no navegador, não pelo emissor
Dados coletados	Nome, telefone, **CPF**, endereço completo, dados completos do cartão e **senha**
Identidade declarada	**CNPJ de terceiro, BAIXADO em 2014**, de ramo diverso (salão de beleza) e outro município
Identidade trocável	**Sim** — nome, CNPJ, WhatsApp e logo vêm de /admin/cfg.php, endpoint público
Uso de marcas	Liquigás, Ultragaz, Copagaz, Supergasbras e Fogás exibidas sem declaração de autorização
Rede	**Mesmo checkout (hash idêntico), mesmo IP e mesmos NS de gaseaguadojota.online**
Conformidade setorial	Nenhuma referência a autorização da ANP, instalação física ou responsável técnico

Leitura técnica. O fluxo de cartão deste site não é um pagamento com defeito — é um **formulário de coleta**. Não há requisição a adquirente, não há tokenização, não há 3-D Secure e o resultado "recusado" está escrito no código, com prazo de quatro segundos. O pedido de **senha do aplicativo do banco** não tem qualquer uso legítimo em comércio eletrônico: junto do número, da validade e do CVV, é o conjunto necessário para transações fraudulentas e, em vários bancos, para acesso à conta. A "recusa" serve para levar a vítima ao Pix, de modo que a operação lucre com o pedido *e* fique com os dados do cartão. A identidade trocável por

`/admin/cfg.php` mostra que o mesmo site pode virar qualquer loja em segundos, e a coincidência do hash do checkout com gaseaguadojota.online comprova a **replicação industrial do kit**. Não se imputa conduta à pessoa cujo CNPJ é exibido (que pode ser vítima de apropriação de identidade), às distribuidoras de gás cujas marcas aparecem, nem aos provedores de infraestrutura (Hostinger, HostGator, Oracle).

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	O checkout pede a SENHA do aplicativo do banco, além de número, validade e CVV, e envia tudo a um api.php próprio	`checkout.html`	ALTA
2	"Cartão recusado" é resultado fixo, gerado por setTimeout no navegador — o cartão nunca é submetido a autorização	`checkout.html`	ALTA
3	Nenhuma integração com adquirente, gateway, tokenização, 3-D Secure ou antifraude em todo o fluxo	`checkout.html`	ALTA
4	CNPJ exibido pertence a empresa BAIXADA em 2014, de outro ramo (cabeleireiros) e outro município	`cfg_publico.json` · `cnpj_publico.json`	ALTA
5	Checkout byte a byte idêntico (mesmo SHA-256) ao de gaseaguadojota.online, no mesmo IP e mesmos NS	`checkout.html` · `dns_records.txt`	ALTA
6	Identidade da loja (nome, CNPJ, WhatsApp, logo) trocável por /admin/cfg.php, endpoint público sem autenticação	`cfg_publico.json` · `corpo.html`	MÉDIA
7	HTML estático publica o CNPJ marcador 00.000.000/0001-00	`corpo.html`	MÉDIA
8	Marcas de distribuidoras (Liquigás, Ultragaz, Copagaz, Supergasbras, Fogás) exibidas sem declaração de autorização	`corpo.html`	MÉDIA
9	Domínio de ~5 semanas, titular não publicado, publicado no mesmo dia do registro	`rdap_raw.json` · `headers_https.txt`	MÉDIA
10	Venda de GLP sem qualquer referência a autorização da ANP ou instalação física	`corpo.html`	MÉDIA
11	Coleta de CPF e endereço completo antes de qualquer confirmação de pedido	`checkout.html`	BAIXA

Síntese: 5 indicadores de severidade ALTA, 5 MÉDIA e 1 BAIXA. **Nenhum fator de legitimidade** (CNPJ ativo, endereço físico, autorização da ANP, adquirente ou gateway real, identidade estável) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 29/07/2026, conclui-se que **diskgasdomaxx.online** opera um **checkout de captura de credenciais de cartão** disfarçado de loja de entrega de gás e água. O código público do checkout coleta número, validade, CVV e a **senha do aplicativo do banco**, envia tudo a um `api.php` do próprio site e sempre exibe "recusado" por temporizador — sem adquirente, sem tokenização e sem que o cartão seja cobrado —, redirecionando a vítima para o Pix. A identidade da loja é injetada em tempo de execução por um endpoint público e se apoia no CNPJ de uma empresa **baixada em 2014**, de ramo e município diversos. O mesmo checkout, com **hash SHA-256 idêntico**, é servido por **gaseaguadojota.online**, no mesmo IP e com os mesmos servidores de nome. Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Nunca informe a senha do cartão ou do aplicativo do banco em uma página da internet.** Ela só é digitada em maquininha ou no app oficial do banco — nenhum site legítimo a solicita.

- Se os dados já foram digitados: **bloquear o cartão imediatamente** pelo aplicativo, **trocar a senha do app do banco** e comunicar a central oficial do emissor sobre a exposição.
- **Não pagar por Pix** após a "recusa" do cartão — a recusa é falsa e serve apenas para migrar o pagamento para um recebedor não identificável.
- Antes de comprar gás, conferir o **CNPJ na base pública da Receita Federal** e a autorização na **ANP**; revenda de GLP exige instalação física licenciada e pessoa jurídica ativa.
- 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 `diskgasdomaxx.online` e `gaseaguadojota.online` aos canais de *abuse* do registrador (Hostinger) e da hospedagem (**HostGator Brasil**), anexando este laudo e o hash SHA-256 que comprova o checkout idêntico.
- Comunicar o incidente às **bandeiras e emissores de cartão** e ao **CERT.br**, indicando a página que solicita senha de aplicativo bancário.
- Comunicar a **ANP** e o **Procon** sobre a oferta de revenda de GLP por pessoa jurídica baixada, com uso de marcas de distribuidoras sem autorização declarada.
- 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, de cartão ou de senha foi enviado ao site; o fluxo descrito foi lido no código público do checkout. 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 à pessoa cujo CNPJ é exibido pelo site, 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
`cfg_publico.json`	`9a120367d7e5bd72873bc6ba402784191744616e51b2296cb634ca1b9271e4c6`
`checkout.html`	`e97fce8fb1ae82ff85a41422f218fa22c5bbdd3fe78d4ca898784fbaa43ff1ca`
`cnpj_publico.json`	`950ee2eaafbb0aeb3db0e18e93412c5893161fcefa08e0906f74c34380bbbf36`
`corpo.html`	`bdfa173239bb31e4c4a8041aa3a21f5ea9836a3f71e947510d43722a2c5a9a00`
`dns_records.txt`	`9828e67975926bd3eeb9bb34e1f9fbc4fa3ca10f524f8f673483867e15abe825`
`headers_https.txt`	`4d3e2abb603b9f9434d9713146f8b0cbcc1d14785dcfbb5130d3a3cb485da303`
`ipinfo.json`	`d7e4b22983c456aaaa3308784ef309e62046d612619075e5dd295bf37295bc0a`
`ptr.txt`	`c1753ff036246ec177014083552cb77baced3687b97ecab5f079ce5d2abac1dd`
`rdap_raw.json`	`edcd0cb084c54d6c38278c0974217a8ad1097fcf25def0de21e1121c2a9fa761`
`tls_cert.txt`	`8626514c351089b865e9b851251cde96e73708333d80f1455706d000c0e5d852`

— Fim do relatório —