RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

fogaodavovo.delivery

Objeto investigado	fogaodavovo.delivery — cardápio digital de marmitas e churrasco com entrega (gTLD .delivery)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	29/07/2026 (RDAP, DNS, HTTP/TLS, geolocalização, páginas institucionais e código do checkout)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do front-end e do checkout
Achado central	O checkout preenche automaticamente o pedido com um CPF ALEATÓRIO gerado no navegador quando o cliente não informa o seu, e consulta um endpoint próprio que devolve o NOME do titular de qualquer CPF digitado; o CNPJ do operador é publicado mascarado ("XX.947.XXX/0001-XX")
Classificação	**RISCO ALTO**
Emissão do laudo	30/07/2026 às 00:31

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **fogaodavovo.delivery**, 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 CPF ou 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 um cardápio digital em PHP intitulado "Fogão da Vovó — Churrasco com Entrega Rápida", com marmitas, costela, picanha e combos de R$ 11,00 a R$ 49,90, pagamento **apenas por Pix** e checkout próprio em `/carrinho.php`. O domínio foi **registrado em 08/04/2026**, cerca de três meses e meio antes da coleta, com titular não publicado.

O achado mais grave está no código do checkout. Ao carregar a página, um campo oculto chamado `cpf` é preenchido pela função `gerarCPFAleatorio()`, que sorteia nove dígitos e calcula os dois dígitos verificadores pelo algoritmo do módulo 11 — isto é, produz um **CPF aleatório aritmeticamente válido**. Se o visitante escolhe não informar o CPF, ou digita um número inválido, o pedido e a cobrança Pix seguem com **o CPF sorteado**, que pertence a uma pessoa real qualquer, sem relação com a compra. Quando o visitante *digita* um CPF válido, o site chama `validar_cpf.php?cpf=` e exibe na tela o **nome do titular** daquele CPF; o mesmo fluxo guarda `cpf_data_nascimento` e `cpf_sexo` no navegador e os envia ao servidor junto do pedido. Ou seja, a operação **tem acesso a uma base de dados pessoais** capaz de devolver nome, data de nascimento e sexo a partir do CPF.

A identificação do responsável é **deliberadamente ilegível**. O rodapé de todas as páginas e a página "Contato Institucional" declaram que o site "é operado por **RESTAURANTE DA VOVO LTDA**" e informam "CNPJ: **XX.947.XXX/0001-XX**" — um número **mascarado**, impossível de conferir em qualquer base pública. As páginas legais (termos de uso, privacidade, entrega, cancelamento e reembolso) existem, mas todas trazem `meta robots noindex`, e a página institucional está datada de **13/03/2026** — **26 dias antes** do registro do próprio domínio, sinal de conteúdo reaproveitado de um modelo pronto.

A vitrine acumula sinais de montagem por template não conferido: o bloco "Endereço" e o bloco "Áreas de Entrega" exibem literalmente os marcadores **"cidade - UF"**, nunca preenchidos; o registro SPF do domínio contém uma segunda entrada com o texto literal `ip4:|IP|`, placeholder de template; e o JSON-LD declara nota **4,9 com 1.128 avaliações** para um estabelecimento cujo domínio tem três meses e meio. O mesmo JSON-LD informa endereço na Rua Domingos de Morais, 2187, São Paulo/SP, e telefone **0800 591 0042**. A operação é intensamente instrumentada para tráfego pago — Facebook Pixel, Google Tag e Microsoft Clarity (gravação de sessão) —, e o evento **Purchase** do Pixel é disparado no instante em que o Pix é *gerado*, **antes de qualquer confirmação de pagamento**.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: um site que **fabrica CPF de terceiros** para completar pedidos, **consulta base de dados pessoais** para exibir o nome de quem digita um CPF, publica o **CNPJ mascarado** e recebe apenas por Pix oferece **risco elevado**. Recomenda-se **não comprar, não pagar e não informar CPF** (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 (Identity Digital/.delivery — registrador Dynadot)	`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 /carrinho.php (sem envio de dados)	`carrinho.html · headers_carrinho.txt`
Página institucional	curl HTTPS de /contato-institucional.php	`contato_institucional.html`
Scripts do cardápio	Download dos JS públicos	`delivry.js · all.js`
Endpoints	GET sem parâmetros (existência e resposta)	`probe_endpoints.txt`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização	ipinfo.io (IP da vitrine e IP autorizado no SPF)	`ipinfo.json · ipinfo_spf_origin.json`

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

Domínio	fogaodavovo.delivery (gTLD .delivery — Identity Digital)
Registro	**08/04/2026** 17:45:35 UTC · expira 08/04/2027 (validade de 1 ano)
Idade na coleta	**~3 meses e meio**
Titular	**Não publicado** (o RDAP expõe apenas o registrador)
Registrador	Dynadot Inc
Servidores de nome	hugh.ns.cloudflare.com · marlowe.ns.cloudflare.com
DNS	A 104.21.28.201 · 172.67.147.136 · AAAA 2606:4700:30xx:: · MX 10 mail.fogaodavovo.delivery
SPF	"v=spf1 a mx ip4:65.21.203.173 include:relay.mailbaby.net …" + segundo TXT com o placeholder literal `ip4:|IP|`
Origem do e-mail	65.21.203.173 → `host.marketei.com.br` · AS24940 Hetzner, Helsinque/Finlândia
Hospedagem da vitrine	AS13335 Cloudflare (anycast, PoP GRU) · origem nginx (respostas 404/502 do nginx em caminhos inexistentes)
Certificado TLS	CN=fogaodavovo.delivery · Let's Encrypt YE2 (DV) · válido 06/06/2026–04/09/2026
Identidade declarada	"RESTAURANTE DA VOVO LTDA" · **CNPJ XX.947.XXX/0001-XX (mascarado)**
Contato declarado	0800 591 0042 · atendimento@fogaodavovo.delivery · Rua Domingos de Morais, 2187 — São Paulo/SP (JSON-LD)
Rastreamento	Facebook Pixel 1687977611855394 · Google Tag GT-5TW4CPQ8 · Microsoft Clarity jujqqs7wd2 (gravação de sessão)

Leitura técnica. A infraestrutura é de **baixa rastreabilidade**: titular não publicado, vitrine atrás de CDN e e-mail saindo de um servidor compartilhado hospedado na Finlândia. O registro SPF deixado com o marcador `|IP|` e as páginas com os marcadores "cidade - UF" mostram que a operação foi montada a partir de um **modelo pronto, publicado sem revisão**. 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 Hetzner nem aos provedores de e-mail citados, meros provedores de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O cardápio é um aplicativo PHP com jQuery (`delivry.js`), e o checkout roda em `/carrinho.php`, em quatro etapas, com envio ao endpoint próprio `pagamento/gerar_pix.php`. O quadro abaixo reúne o que foi lido no código público, sem qualquer envio de dados.

Item verificado	Constatação
CNPJ do operador	`"RESTAURANTE DA VOVO LTDA — CNPJ: XX.947.XXX/0001-XX" (mascarado, não verificável)`
CPF no pedido	`gerarCPFAleatorio()` preenche o campo oculto "cpf" com CPF sorteado e DV válido ao carregar a página
Consulta de CPF	`fetch("validar_cpf.php?cpf=" + digits)` → devolve e exibe o NOME do titular; guarda `cpf_data_nascimento` e `cpf_sexo`
Envio do pedido	`POST pagamento/gerar_pix.php` com nome, cpf, data_nascimento, sexo, whatsapp, e-mail, endereço completo, itens e tracking
Meios de pagamento	Apenas **Pix** ("Formas de Pagamento: Pix")
Placeholders não preenchidos	Blocos "Endereço" e "Áreas de Entrega" exibem literalmente "cidade - UF"
Prova social	JSON-LD declara `aggregateRating` 4.9 com 1.128 avaliações em domínio de 3 meses e meio
Evento Purchase	`fbq("track","Purchase")` disparado ao gerar o Pix, antes de qualquer confirmação de pagamento
Páginas legais	`/termos-de-uso.php` · `/politica-de-privacidade.php` · `/politica-de-entrega.php` · `/contato-institucional.php` · `/politica-de-cancelamento-e-reembolso.php` — todas com noindex
Data da página institucional	13/03/2026 — **26 dias antes** do registro do domínio (08/04/2026)

Aspecto	Constatação
Tipo de serviço	Delivery de marmitas e churrasco (R$ 11,00 a R$ 49,90), com agendamento e "order bumps" de bebidas
Tecnologia	PHP + jQuery atrás da Cloudflare · nginx na origem · endpoints próprios de Pix e de consulta de CPF
Meio de pagamento	**Pix** gerado por endpoint próprio (`pagamento/gerar_pix.php`) — nenhum adquirente ou gateway identificado
Dados coletados	Nome, **CPF**, data de nascimento, sexo, WhatsApp, e-mail, CEP, rua, número, complemento, bairro, cidade, estado e observações
Tratamento do CPF	**Fabricação e consulta** — CPF aleatório quando não informado; consulta de titularidade quando informado
Identidade declarada	**CNPJ mascarado** — impossível verificar quem opera
Área de entrega	**Indefinida** — marcadores "cidade - UF" não preenchidos
Prova social	Nota 4,9 e 1.128 avaliações declaradas no JSON-LD, sem origem verificável
Aquisição de tráfego	Facebook Pixel, Google Tag e Microsoft Clarity — perfil de campanha paga com gravação de sessão
Infraestrutura de e-mail	Servidor compartilhado na Finlândia (Hetzner) autorizado no SPF

Leitura técnica. Dois mecanismos merecem destaque. O primeiro é o **CPF aleatório**: ao gerar cobranças com um CPF sorteado, a operação preenche o campo de pagador exigido pelos intermediários de Pix com o número de **uma pessoa que nada tem a ver**

com o pedido, o que dificulta o rastreio e pode gerar registros indevidos em nome de terceiros. O segundo é o **validar_cpf.php**: devolver nome, data de nascimento e sexo a partir de um CPF exige acesso a uma base de dados pessoais que não é pública no Brasil; exibir o nome do visitante logo após ele digitar o CPF é, além de um provável tratamento irregular de dados sob a LGPD, um poderoso recurso de **construção de confiança**. Some-se a isso o CNPJ mascarado, a área de entrega nunca preenchida, a nota 4,9 declarada por conta própria e o pagamento exclusivo por Pix sem gateway: o consumidor paga antes, para um recebedor que não pode identificar, a uma empresa que não pode conferir. Não se imputa conduta aos provedores de infraestrutura nem a intermediários de pagamento.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Checkout preenche o pedido com CPF aleatório gerado no navegador quando o cliente não informa o seu	`carrinho.html`	ALTA
2	Endpoint validar_cpf.php devolve o nome do titular de qualquer CPF digitado; o fluxo guarda data de nascimento e sexo	`carrinho.html · probe_endpoints.txt`	ALTA
3	CNPJ do operador publicado mascarado ("XX.947.XXX/0001-XX"), impossível de verificar	`corpo.html · contato_institucional.html`	ALTA
4	Pagamento exclusivo por Pix gerado por endpoint próprio, sem adquirente, gateway ou nota fiscal	`delivry.js · carrinho.html`	ALTA
5	Evento Purchase enviado ao Facebook no momento em que o Pix é gerado, antes de qualquer pagamento	`carrinho.html`	MÉDIA
6	JSON-LD declara nota 4,9 com 1.128 avaliações em domínio de três meses e meio	`corpo.html`	MÉDIA
7	Blocos "Endereço" e "Áreas de Entrega" exibem os marcadores "cidade - UF" não preenchidos	`corpo.html`	MÉDIA
8	Registro SPF com placeholder literal "ip4:|IP|" — template publicado sem revisão	`dns_records.txt`	MÉDIA
9	Página institucional datada 26 dias antes do registro do domínio — conteúdo de modelo reaproveitado	`contato_institucional.html · rdap_raw.json`	MÉDIA
10	Titular do domínio não publicado e páginas legais marcadas com noindex	`rdap_raw.json · contato_institucional.html`	BAIXA
11	Gravação de sessão (Microsoft Clarity) em páginas que coletam CPF e endereço	`corpo.html · carrinho.html`	BAIXA

Síntese: 4 indicadores de severidade ALTA, 5 MÉDIA e 2 BAIXA. Como **fatores de legitimidade** registram-se a existência de páginas legais completas e de um endereço físico plausível no JSON-LD — nenhum dos dois, porém, é verificável, já que o CNPJ que os sustentaria está mascarado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 29/07/2026, conclui-se que **fogaodavovo.delivery** é um **cardápio digital de alto risco**: registrado há três meses e meio com titular não publicado, publica o CNPJ do operador **mascarado**, nunca preencheu a própria área de entrega, declara para si nota 4,9 com 1.128 avaliações e recebe **apenas por Pix**, gerado por endpoint próprio, sem adquirente identificável. Sobretudo, o checkout **gera um CPF aleatório** para completar pedidos de quem não informa o seu e **consulta uma base de dados pessoais** capaz de devolver nome, data de nascimento e sexo a partir do CPF digitado — dois mecanismos incompatíveis com uma operação regular de delivery. Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não comprar, não pagar por Pix e, em nenhuma hipótese, informar CPF** a este site.

- Se o CPF já foi digitado, considerar que **nome, data de nascimento e sexo** podem ter sido coletados; monitorar tentativas de golpe que usem esses dados ("golpe do falso funcionário", cobranças em seu nome) e exercer os direitos da **LGPD** perante a ANPD.
- Exigir sempre **CNPJ legível e verificável**: um estabelecimento que publica o próprio CNPJ com "X" no lugar dos números não pode ser identificado nem responsabilizado.
- 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 o domínio `fogaodavovo.delivery` aos canais de *abuse* do registrador (Dynadot) e da **Cloudflare**, anexando este laudo.
- Comunicar a **ANPD** (Autoridade Nacional de Proteção de Dados) sobre o endpoint `validar_cpf.php`, que devolve dados pessoais de titulares de CPF, e sobre a geração de cobranças com CPF de terceiros.
- Reportar ao **Procon** a oferta com identificação empresarial mascarada e avaliações declaradas sem origem verificável (arts. 30, 31 e 37 do Código de Defesa do Consumidor).
- 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, nenhum CPF foi consultado e nenhum dado pessoal foi enviado — os endpoints citados foram apenas verificados quanto à existência, com requisições sem parâmetros. 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 (Dynadot, Cloudflare, Hetzner) 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
`all.js`	`5101e851a23398954fbfa2389b67bd72cdb3bdfbefe26abdf98016157a796cbb`
`carrinho.html`	`1887e3f1bc7648897a7cfff79c22c8c3f23021550376a7f2ca59581930a534a4`
`contato_institucional.html`	`013471d19d20a272dc971e7cbbbcbf49d09de916117341c0b6971d79df5784ad`
`corpo.html`	`de898c1405e1007901149ab7ab3b397e9de64e3ccdc70a9bceb64d5188a73858`
`delivry.js`	`4611512bd767fdb2a29484541405ae7b5d585f2c30d77ae7c857a1db07261154`
`dns_records.txt`	`4ebdf4d2c7f8f20fbe17af9a67a2fbb2b2747fbe5b53aad29de2be20400fb96c`
`headers_carrinho.txt`	`624c7c0dfa3db24601a64db33cfa7a9b7576e955bd0f39c6302edd018238f346`
`headers_https.txt`	`6fc563dd440c885090dbc22485ee97450a398bd4bcee0054beaea52752a77cbb`
`ipinfo.json`	`986fc688c704ade41f4d603181d407cfd803e5396b54205dd8861a426332f88d`
`ipinfo_spf_origin.json`	`44ea7ad7778def5e9ae2ed16627b8a14d06a812a9336b6d4d829245bc07dcea6`
`probe_endpoints.txt`	`138ec8f1769ea8b4b37cd571c8d61102719453ed09731652f44b7e7c310c1414`
`rdap_raw.json`	`4713886a047e3e22e8f9a0a227bb245836b3cb215021d330a5c923b5210b632e`
`tls_cert.txt`	`36c339039a72bd8e2e012abf58975a589a928c74d620bbe73fd761075b3c43de`

— Fim do relatório —