RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, forense e de risco de fraude do domínio

marmitexgrill.delivery

Objeto investigado	marmitexgrill.delivery
Natureza	Verificação de legitimidade / suspeita de fraude (e-commerce de delivery)
Data da coleta	19/05/2026 — 05:15 a 05:20 UTC (02:15–02:20 BRT)
Métodos	OSINT passivo · RDAP · DNS · análise de cabeçalhos HTTP · TLS · revisão de código-fonte
Emissão do laudo	19/05/2026 às 09:21

1. Sumário Executivo

Este relatório documenta a investigação técnica do sítio eletrônico **https://marmitexgrill.delivery**, apresentado ao público como uma marmitaria com serviço de entrega ("Marmitex Grill"). A coleta de evidências foi realizada em 19/05/2026 por meio de técnicas de OSINT (inteligência de fontes abertas) e análise forense passiva, sem qualquer interação intrusiva com a infraestrutura-alvo.

A análise identificou um **conjunto consistente e convergente de indicadores de fraude**. O domínio é recente (registrado há aproximadamente cinco meses), está hospedado em provedor situado na **Moldávia** — incompatível com um restaurante local brasileiro — compartilha infraestrutura com outro domínio de padrão idêntico, e a página apresenta táticas clássicas de engenharia social (contador regressivo zerado, falsa escassez de estoque, avaliações fabricadas e geolocalização simulada). O código-fonte revela que o pagamento ocorre **exclusivamente via PIX direto**, sem qualquer intermediação por gateway de pagamento legítimo, ao mesmo tempo em que são coletados dados pessoais do consumidor.

CLASSIFICAÇÃO DE RISCO	ALTO RISCO DE FRAUDE

Esta classificação resulta da convergência dos 12 indicadores técnicos detalhados na Seção 9. Recomenda-se enfaticamente que consumidores **não efetuem pagamentos** e **não forneçam dados pessoais** ao endereço investigado.

2. Metodologia e Cadeia de Custódia

A investigação seguiu o princípio da **preservação probatória**: todas as respostas de rede foram salvas em arquivo no momento da coleta e tiveram seu valor de resumo criptográfico (hash SHA-256) calculado, permitindo a verificação de integridade a qualquer tempo. Nenhuma técnica intrusiva, de exploração de vulnerabilidade ou de engenharia reversa de servidor foi empregada — apenas requisições equivalentes às de um visitante comum e consultas a bases públicas (RDAP, DNS).

Etapa	Técnica / ferramenta	Evidência preservada
Registro do domínio	RDAP (Registration Data Access Protocol) — registro .delivery	`rdap_raw.json`
Infraestrutura DNS	Consultas dig (A, NS, MX, TXT, SOA)	(transcrito na Seção 4)
Cabeçalhos HTTP	curl — requisição HTTPS/HTTP	`headers_https.txt`
Conteúdo da página	Captura do HTML servido	`corpo_https.html`
Certificado TLS	openssl s_client / x509	`ssl_cert.txt`
Lógica de aplicação	Revisão do JavaScript do site	`js_delivry.js, js_all.js`
Identidade visual	Captura de ativo gráfico	`logomarmitexgrill.webp`

Todos os artefatos estão na subpasta **evidencias/** e seus hashes constam do Anexo A (Manifesto de Integridade). O fuso horário de referência é UTC; conversões para o horário de Brasília (BRT, UTC–3) são indicadas quando aplicável.

3. Identificação do Domínio (RDAP)

Os dados a seguir foram obtidos junto ao operador do registro do TLD **.delivery** (Identity Digital) pelo protocolo RDAP. Os dados do titular ("registrant") encontram-se **redigidos** por política de privacidade do registro, prática comum mas que, neste caso, impede a identificação do responsável.

Domínio	marmitexgrill.delivery
Status EPP	clientTransferProhibited (transferência bloqueada pelo registrador)
Data de registro	19/12/2025 16:47:49 UTC
Última alteração	24/12/2025 16:48:40 UTC
Data de expiração	19/12/2026 16:47:49 UTC
Idade do domínio	~5 meses na data da coleta — **domínio recente**
Registrador (Registrar)	Dynadot Inc.
Contato de abuso	abuse@dynadot.com · +1.650.262.0100
Titular / Registrant	Redigido (privacidade do registro / proteção de dados)
DNSSEC	Não assinado (delegationSigned: false)
Servidores de nome	dante.ns.cloudflare.com · jocelyn.ns.cloudflare.com

Leitura técnica. O período de registro foi contratado por apenas 1 (um) ano — o mínimo possível — e o domínio possui pouca idade. Domínios de curta duração e recém-criados são fortemente associados a campanhas fraudulentas descartáveis, projetadas para operar por poucas semanas até serem denunciadas e substituídas. A ausência de dados do titular, embora legal, soma-se à falta de transparência do site.

4. Infraestrutura de DNS

A zona DNS é gerenciada pela Cloudflare (servidores de nome), porém o registro de endereço (A) aponta diretamente para um IP de terceiros — ou seja, o site **não utiliza o proxy/CDN da Cloudflare**, expondo o endereço real do servidor de origem.

Registro	Valor	Observação
A	`80.96.108.136`	Servidor de origem exposto (sem proxy CDN)
AAAA	— (ausente)	Sem IPv6
NS	`dante.ns.cloudflare.com / jocelyn.ns.cloudflare.com`	DNS gerenciado pela Cloudflare
MX	— (ausente)	Domínio não recebe e-mail — sem canal de contato por e-mail
TXT / SPF	— (ausente)	Sem políticas de e-mail; nenhuma verificação de propriedade
SOA	`dante.ns.cloudflare.com (serial 2404652507)`	—
www	`CNAME → apex (marmitexgrill.delivery)`	—

Leitura técnica. A inexistência de registros MX e TXT/SPF confirma que o domínio não opera e-mail corporativo — uma empresa de alimentação legítima normalmente dispõe de e-mail próprio. O uso da Cloudflare apenas como DNS autoritativo, sem proxy, é típico de instalações montadas rapidamente.

5. Hospedagem e Geolocalização do Servidor

Endereço IP	80.96.108.136
Sistema autônomo	AS200019 — ALEXHOST SRL
Provedor de hospedagem	AlexHost SRL
País do servidor	**Moldávia** (Chi■in■u)
Servidor web	nginx
DNS reverso (PTR) do IP	bigusburguer.delivery

Achado relevante — reaproveitamento de infraestrutura. O DNS reverso do endereço IP que hospeda o site retorna o nome **bigusburguer.delivery** — um domínio distinto, mas que segue exatamente o mesmo padrão (nome de lanchonete/marmitaria + TLD ".delivery"). Isso indica que o mesmo IP foi, ou ainda é, utilizado por outro site do mesmo tipo, sugerindo uma **operação em série / cluster de sites de delivery falsos** sobre a mesma infraestrutura.

Incompatibilidade geográfica. O site se apresenta como um restaurante de entrega local, com preços em reais (R$), texto em português brasileiro e promessa de "entrega grátis para sua região". No entanto, o servidor está fisicamente na **Moldávia (Leste Europeu)**, hospedado na AlexHost — provedor reconhecidamente utilizado para abrigar conteúdo de baixa reputação. Não há justificativa operacional para que uma marmitaria brasileira hospede seu site de pedidos em um provedor offshore desse perfil.

6. Certificado TLS / HTTPS

Titular (Subject)	CN = marmitexgrill.delivery
Emissor (Issuer)	Let's Encrypt — autoridade "R12" (C=US)
Tipo de validação	DV — Domain Validation (validação apenas de domínio)
Válido de	04/04/2026 12:44:50 UTC
Válido até	03/07/2026 12:44:49 UTC
Número de série	0567E7BC4BAF020B8BF25D58680886A4FA07
Fingerprint SHA-256	A8:E9:3C:D7:F3:86:12:07:42:3D:87:4D:B1:5B:58:94: 4A:82:17:70:9B:09:59:27:ED:26:6F:3A:C6:FB:2A:E1

Leitura técnica. O certificado é válido e a conexão HTTPS é legítima do ponto de vista criptográfico — porém é um certificado **gratuito do tipo DV**, que apenas comprova o controle sobre o domínio e **não atesta a identidade da empresa**. O "cadeado" do navegador, portanto, não é garantia de idoneidade do estabelecimento. Observou-se ainda que o site responde igualmente em HTTP (porta 80) sem redirecionamento para HTTPS, apesar de enviar o cabeçalho HSTS.

7. Análise do Conteúdo da Página

A página inicial (título HTML: *"Faça seu pedido!"*) reproduz a aparência de um aplicativo de delivery. A última modificação do conteúdo, segundo o cabeçalho HTTP, é de **23/04/2026**. Foram identificados os seguintes elementos de **engenharia social** e de fabricação de credibilidade:

Elemento observado	Descrição e leitura forense
Contador regressivo	"A promoção vai acabar em: 00 Horas 00 Minutos 00 Segundos" — temporizador exibido permanentemente zerado, criando falsa urgência.
Falsa escassez	"Apenas 8 unidade(s) com esse preço especial" repetido em vários itens — pressão psicológica de estoque limitado.
Descontos agressivos	Preços do tipo "de R$ 69,90 por R$ 54,90", "Frete Grátis" em todos os itens — atratividade artificial.
Avaliações fabricadas	"4.9/5 (1360 avaliações)" com depoimentos genéricos (Carlos M, Ana Paula S, Rodrigo L., etc.) sem origem verificável.
Geolocalização falsa	"1,6 km de você" e "Entrega grátis para sua região" — proximidade simulada para qualquer visitante.
Texto de modelo não preenchido	Rodapé exibe literalmente "Endereço: cidade - UF" e "Áreas de Entrega: cidade - UF" — placeholders de template jamais personalizados.
CNPJ não verificável	Rodapé informa "CNPJ: 37.XXX.829/0002-54" — número parcialmente mascarado, impossível de validar na Receita Federal.
Imagens externas	Foto de produto carregada a partir da CDN do Facebook (scontent.fgyn22-1.fna.fbcdn.net) — imagem provavelmente extraída de outra página.

Leitura técnica. A presença de placeholders de modelo não preenchidos ("cidade - UF") é prova material de que o site foi produzido em massa a partir de um template genérico de delivery e publicado sem sequer ser configurado para um estabelecimento real. Um CNPJ parcialmente ocultado não permite verificação de existência jurídica da empresa.

8. Análise do Fluxo de Pagamento (código-fonte)

A revisão do arquivo de lógica do site (`js/delivry.js`) revelou os pontos de comunicação ("endpoints") da aplicação, no diretório `/delivery/`:

Endpoint	Função
`enviarPedido.php`	Recebe e registra o pedido com os dados pessoais do consumidor.
`gerarPixCopiaECola.php`	Geração de código PIX "copia e cola" para o pagamento.
`carrinho.php`	Gerenciamento do carrinho de compras.
`validarCupom.php`	Validação de cupons de desconto.
`validarEmail.php / validarCodigoEmail.php`	Captura e validação de e-mail do usuário.
`verificarLojaAberta.php`	Verificação de horário de funcionamento.

8.1. Dados pessoais coletados

A função que envia o pedido transmite ao servidor, em texto, o seguinte conjunto de dados pessoais do consumidor (trecho extraído de `delivry.js`):

8.2. Pagamento exclusivamente via PIX direto

O código contém a função `copiarChavePix()`, que copia uma chave PIX para a área de transferência do visitante. **Não há integração com nenhum gateway de pagamento** (ex.: operadoras de cartão, PSPs regulados). O pagamento é direcionado diretamente a uma chave PIX — modelo que **não oferece rastreabilidade nem mecanismo de estorno/chargeback** ao consumidor, sendo o método preferencial em golpes de falsas lojas. A chave PIX não é exposta de forma estática no HTML inicial: ela é apresentada dinamicamente apenas na etapa final do checkout, o que dificulta a denúncia preventiva.

Leitura técnica. A combinação "coleta de dados pessoais completos do comprador" + "pagamento apenas por PIX direto, sem gateway" + "ausência de pessoa jurídica verificável" é o padrão operacional característico de sites de falso comércio eletrônico. O consumidor paga, fornece seus dados, e não há contrapartida nem meio de reaver o valor.

9. Indicadores de Fraude (IoF)

A tabela consolida os indicadores objetivos identificados. Nenhum isoladamente é conclusivo, mas a sua **convergência** sustenta a classificação de risco atribuída.

#	Indicador	Evidência	Severidade
1	Domínio recém-registrado (~5 meses), contratado por 1 ano	`RDAP — registro em 19/12/2025`	ALTA
2	Servidor hospedado na Moldávia, incompatível com delivery local	`IP 80.96.108.136 / AS200019 AlexHost`	ALTA
3	IP compartilhado com outro domínio de padrão idêntico	`PTR → bigusburguer.delivery`	ALTA
4	Pagamento apenas via PIX direto, sem gateway nem estorno	`Função copiarChavePix() em delivry.js`	ALTA
5	CNPJ parcialmente mascarado e não verificável	`Rodapé: "CNPJ 37.XXX.829/0002-54"`	ALTA
6	Coleta de dados pessoais completos do consumidor	`enviarPedido.php (delivry.js)`	MÉDIA
7	Contador regressivo de promoção permanentemente zerado	`HTML — bloco de promoção`	MÉDIA
8	Falsa escassez de estoque ("apenas 8 unidades")	`HTML — itens do cardápio`	MÉDIA
9	Avaliações fabricadas (1.360 avaliações, 4.9/5)	`HTML — bloco de depoimentos`	MÉDIA
10	Placeholders de template não preenchidos ("cidade - UF")	`HTML — rodapé`	MÉDIA
11	Domínio sem MX/SPF — sem e-mail corporativo	`Consulta DNS`	MÉDIA
12	Pixel de rastreamento de campanha/afiliados (UTMify)	`cdn.utmify.com.br — Pixel 6945fd5c...`	BAIXA

Síntese: 5 indicadores de severidade ALTA, 6 de severidade MÉDIA e 1 de severidade BAIXA. O presença simultânea de hospedagem offshore, domínio descartável, ausência de pessoa jurídica verificável e pagamento exclusivo por PIX direto constitui o perfil clássico de loja virtual fraudulenta.

10. Conclusão Técnica

Com base nas evidências coletadas e preservadas em 19/05/2026, conclui-se que o sítio **marmitexgrill.delivery** apresenta **alto risco de fraude**. O conjunto de achados — domínio recente e de baixa duração, hospedagem em provedor offshore na Moldávia, compartilhamento de infraestrutura com outro domínio de mesmo padrão, conteúdo construído sobre template genérico com campos de modelo não preenchidos, mecanismos de engenharia social (urgência, escassez e avaliações fabricadas), CNPJ não verificável e fluxo de pagamento restrito a PIX direto sem qualquer intermediação — é tecnicamente consistente com a operação de uma **falsa loja de delivery**, destinada a captar pagamentos e dados pessoais sem entregar o produto anunciado.

Registre-se que a validação criptográfica do HTTPS (certificado Let's Encrypt) é legítima, porém irrelevante para a aferição de idoneidade: trata-se de certificado gratuito de validação de domínio, que não atesta a identidade do estabelecimento. Não foi possível identificar o titular do domínio devido à redação dos dados de registro.

Ressalva metodológica: este laudo baseia-se em fontes abertas e na análise do conteúdo público do site na data indicada. A classificação expressa um juízo técnico de risco e não substitui decisão de autoridade policial ou judicial.

11. Recomendações

Para o consumidor / solicitante

- **Não realizar pagamentos** nem transferências PIX ao site investigado.
- **Não fornecer dados pessoais** (nome, endereço, telefone, e-mail) no formulário de pedido.
- Caso já tenha pago, acionar imediatamente o banco e solicitar o **Mecanismo Especial de Devolução (MED)** do PIX, registrando contestação de fraude.
- Registrar Boletim de Ocorrência (delegacia física ou eletrônica) e reunir comprovantes (prints, comprovante PIX).
- Denunciar o site à plataforma de anúncios em que foi visualizado (Meta/Instagram, Google) e ao consumidor.gov.br.

Para responsáveis técnicos / takedown

- Reportar abuso ao registrador **Dynadot** (abuse@dynadot.com), anexando este laudo.
- Reportar abuso ao provedor de hospedagem **AlexHost SRL** e à Cloudflare (provedora de DNS).
- Comunicar à equipe de resposta a incidentes **CERT.br / NIC.br** e à Safernet Brasil.
- Monitorar o domínio relacionado **bigusburguer.delivery** e demais nomes no padrão "[comida].delivery", pela possibilidade de pertencerem à mesma operação.

12. Adendo Investigativo — Tela de Pagamento (Checkout PIX)

Em complemento às seções anteriores, o solicitante forneceu uma **captura de tela da etapa final de pagamento** (checkout) do site investigado, registrada em 19/05/2026. A imagem foi preservada como evidência (`checkout_pix_capture_19_05_2026.png`) e seu resumo criptográfico consta do Anexo A. Este adendo examina o fluxo de pagamento **em operação** — antes avaliado apenas pelo código-fonte (Seção 8) — e decodifica o código PIX efetivamente apresentado ao consumidor.

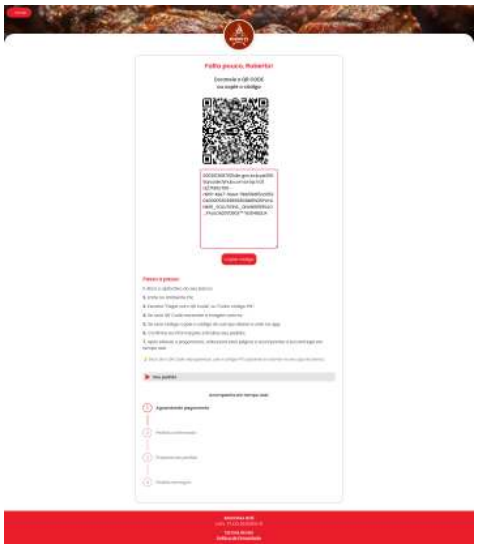

Figura 1 — Tela de pagamento capturada em 19/05/2026: cabeçalho personalizado com o nome do consumidor ("Falta pouco, Roberto!"), QR Code e código PIX "copia e cola", rastreador de pedido simulado e rodapé com CNPJ mascarado.

12.1. Decodificação do código PIX "copia e cola"

O código PIX exibido na tela foi decodificado segundo o padrão **EMV / BR Code** adotado pelo arranjo PIX do Banco Central. Trata-se de um **PIX dinâmico**: o código não carrega uma chave PIX estática, mas uma URL de payload que o aplicativo bancário do pagador consulta no instante do pagamento para obter os dados reais do recebedor e do valor.

Campo (EMV)	Conteúdo	Interpretação
00 — Payload Format	`01`	Formato padrão do BR Code.
26 — Conta do recebedor	`GUI br.gov.bcb.pix + URL`	Identifica o arranjo PIX; PIX dinâmico (payload por URL).
26 — URL de payload	`qrcode.fyhub.com.br/qr/v3/at/7fd5a700-d9f3-49e7-9ae4-11bb58d15aa35`	Servidor de terceiro que entrega os dados efetivos da cobrança.
52 — Categoria (MCC)	`0000`	Estabelecimento sem categoria de comércio definida.
53 — Moeda	`986`	Real brasileiro (BRL).
58 — País	`BR`	Brasil.
59 — Nome do recebedor	`PAYLINKER SOLUTIONS ONLIN[E]`	**Recebedor declarado — não é "Marmitex Grill"** (campo de 25 caracteres, truncado).
60 — Cidade do recebedor	`SAO PAULO`	Cidade declarada do recebedor.
62 — Dados adicionais	`***`	Sem identificador de transação fixo no código.
63 — CRC16	`8DDA`	Dígito verificador — o código é estruturalmente íntegro.

Leitura técnica. Por ser um PIX dinâmico, o destino real do dinheiro não fica gravado no código: é resolvido pela URL `qrcode.fyhub.com.br` no momento do pagamento. O único identificador legível pelo consumidor é o nome do recebedor — e este **não é o estabelecimento anunciado**.

12.2. O recebedor não corresponde ao estabelecimento anunciado

A página se apresenta como "Marmitex Grill" e o rodapé associa a marca a um CNPJ. No entanto, o nome do recebedor inscrito no próprio código PIX é **"PAYLINKER SOLUTIONS ONLINE"** — uma denominação genérica de intermediação de pagamentos, sem qualquer relação aparente com uma marmitaria. Quem efetua o pagamento, portanto, **não transfere recursos para "Marmitex Grill"**, mas para a conta de um intermediário. Este é um dos sinais mais diretos de que a fachada comercial e o destinatário do dinheiro são entidades distintas.

12.3. Investigação do intermediário de pagamento (fyhub.com.br)

A URL de payload do PIX aponta para o domínio **fyhub.com.br**. Por ser um domínio sob o TLD `.br`, o RDAP do Registro.br divulga publicamente os dados do titular — diferentemente do `.delivery` investigado na Seção 3. A consulta complementar, realizada na emissão deste adendo, retornou:

Domínio do intermediário	fyhub.com.br
Data de registro	29/08/2025 — **~9 meses na data deste adendo**
Última alteração	09/10/2025
Data de expiração	29/08/2026
Status	active
Titular (Registrant)	**Matheus Veloso Horst — pessoa física**
Contato técnico	Matheus Veloso Horst (handle MAVHO55)
Servidores de nome	Amazon Route 53 (ns-*.awsdns-*)
Subdomínio de pagamento	qrcode.fyhub.com.br → CNAME fyhub-prod.onz.software
Endereço IP de destino	54.233.171.47 — Amazon AWS, região São Paulo (sa-east-1), Brasil

Leitura técnica. O intermediário "FYHUB / PayLinker" tem domínio recente, registrado por **pessoa física** e não por instituição financeira identificável. Sua infraestrutura de cobrança resolve para `onz.software` — plataforma de serviços bancários de terceiros (banking-as-a-service). Na prática, "FYHUB / PayLinker" opera como **agregador de links de pagamento PIX**: ao interpor essa camada entre o pagador e o beneficiário final, o arranjo torna mais difícil, para o consumidor, identificar quem de fato recebe os valores. Não se imputa aqui conduta ilícita à ONZ ou à AWS — são provedores de infraestrutura; o ponto relevante é que o checkout de uma suposta marmitaria local roteia pagamentos por um intermediário genérico, e não para uma pessoa jurídica verificável de "Marmitex Grill".

12.4. Inconsistências adicionais observadas na tela

Elemento observado	Descrição e leitura forense
CNPJ divergente	O rodapé do checkout exibe "CNPJ 37.XXX.253/0001-51", enquanto a página inicial (Seção 7) exibia "CNPJ 37.XXX.829/0002-54" — **dois números de CNPJ distintos** apresentados pelo mesmo site, ambos mascarados e não verificáveis.
Selo "ESTD 2021"	O logotipo "Marmitex Grill" estampa "ESTD 2021" (fundada em 2021), incompatível com um domínio registrado apenas em 19/12/2025 (Seção 3).
Rastreador de pedido simulado	O bloco "Acompanhe em tempo real" exibe etapas fixas (Aguardando pagamento → Pedido confirmado → Preparando → Entregue). É um elemento decorativo de template, sem integração logística real.
Captura do nome do consumidor	O cabeçalho personalizado "Falta pouco, Roberto!" confirma, na prática, a coleta de dados pessoais descrita na Seção 8.1 — o nome informado no formulário é reapresentado na tela de pagamento.

12.5. Atualização da leitura técnica (revisão da Seção 8.2)

A Seção 8.2, baseada apenas no código-fonte, descreveu o pagamento como "PIX direto, sem gateway". A captura permite **precisar** esse achado: há, sim, uma camada de intermediação — um agregador de links de pagamento PIX (FYHUB / PayLinker) — porém **não se trata de um gateway de cartão regulado**, com mecanismos de estorno e chargeback. O pagamento continua sendo um PIX, cujo recebedor declarado é uma entidade genérica de "soluções online", e não a marmitaria anunciada. A substância da conclusão anterior — ausência de rastreabilidade ao estabelecimento e inexistência de proteção ao consumidor — é, portanto, **reforçada**, e não contrariada.

Conclusão do adendo. A análise da tela de pagamento acrescenta evidências convergentes às já consolidadas no corpo do laudo: o destinatário do dinheiro não é o estabelecimento exibido, há dois CNPJs incompatíveis no mesmo site e um selo de fundação ("ESTD 2021") inconsistente com a idade real do domínio. Estes achados **somam-se aos 12 indicadores da Seção 9** e mantêm inalterada a classificação de **ALTO RISCO DE FRAUDE**. Reitera-se a recomendação de não efetuar pagamentos PIX ao endereço investigado e, em caso de pagamento já realizado, de acionar imediatamente o banco e o Mecanismo Especial de Devolução (MED), conforme a Seção 11.

Anexo A — Manifesto de Integridade das Evidências

Os arquivos abaixo foram preservados na subpasta `evidencias/` e seus resumos criptográficos (SHA-256) foram calculados no momento da coleta. Qualquer alteração posterior de um arquivo modificará seu hash, permitindo a detecção. O manifesto também está salvo em texto em `evidencias/hash_manifest.txt`.

Arquivo	SHA-256
`corpo_https.html`	`4d7257da5af78e26d51a9d651108bdb9b24ef5e116ee95b30678e6e3344f7ffd`
`headers_https.txt`	`fe3f785d4ff7b676467c17d8982eded6ab848f5e92d02e3177ca80e1b7e6b09a`
`rdap_raw.json`	`82bcb09a349f13df207dc6b2464b87649cf4700575af4136c791d1b387fe9d0f`
`ssl_cert.txt`	`61091c31d0f291cb8030cea4c415e1759a5083cb9f3b9a5570cc4b87f2e57e2e`
`js_delivry.js`	`4611512bd767fdb2a29484541405ae7b5d585f2c30d77ae7c857a1db07261154`
`js_all.js`	`5101e851a23398954fbfa2389b67bd72cdb3bdfbefe26abdf98016157a796cbb`
`logomarmitexgrill.webp`	`0c5fed8ffcff5ec4a0546fd7c31fa7ef1ba3d1efe10f3f7444ab91ad2f638202`
`checkout_pix_capture_19_05_2026.png`	`b67f9d4599432e5beeb2e6d7d5fe59e76ee35a4a9b89ea1c4999c40f12ea3954`
`rdap_fyhub.json`	`cdd9b8bb5908a6e5583b39ccddf74711d48225d920f19ffde4f31cf9a91b5a31`

Coleta principal realizada em 19/05/2026, 05:15–05:20 UTC. Os dois últimos artefatos referem-se ao Adendo da Seção 12: a captura da tela de pagamento (registrada em 19/05/2026) e a consulta RDAP complementar ao domínio do intermediário. Algoritmo de verificação: SHA-256. Comando de verificação sugerido: `sha256sum -c hash_manifest.txt` (após ajustar o cabeçalho do arquivo).

— Fim do relatório —

Documento gerado por Dono do Site — OSINT & Investigação Digital · Relatório técnico baseado em dados públicos e análise de conteúdo aberto.