RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

gargulagarimpo.shop

Objeto investigado	gargulagarimpo.shop — loja virtual de roupas/streetwear "Garimpo Gárgula" (gTLD .shop)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	29/06/2026 (RDAP, DNS, HTTP/TLS, geolocalização, análise do app e decodificação PIX)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise de conteúdo · BR Code/EMV · CNPJ público
Achado central	E-commerce recém-criado; itens de grife a preços irreais; PIX vai a intermediário ("ZAPCOIN") alheio à loja
Classificação	**RISCO ALTO**
Emissão do laudo	29/06/2026 às 02:38

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **gargulagarimpo.shop**, realizada em **29/06/2026** 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 ou exploração de vulnerabilidade. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (cadeia de custódia).

O domínio **está no ar** e entrega uma **loja virtual de roupas/streetwear** em português ("Garimpo Gárgula · Streetwear de Drops Numerados"), construída em **Next.js** e hospedada na **Vercel**. O catálogo anuncia **436 "peças únicas"** sob a narrativa de "garimpo/achados raros" — incluindo, com nomes de **marcas de grife e streetwear** (Adidas, Stone Island, C.P. Company, Converse, Levi's, "bapesta", Jaded London) a **preços de R$ 17 a R$ 65**, valores incompatíveis com itens autênticos. O pagamento é **exclusivamente por PIX**, gerado no servidor e intermediado pelo gateway `owem.com.br`. O checkout coleta **nome, e-mail, telefone e endereço de entrega** (via CEP); não foi observada coleta de CPF.

A decodificação do código PIX "copia e cola" fornecido (BR Code/EMV, CRC16 válido) revela que o **recebedor é "ZAPCOIN INTERMEDIACOES LTDA" (São Paulo)** — um **intermediário de pagamento** que **não corresponde** nem ao nome da loja ("Garimpo Gárgula") nem ao CNPJ exibido no rodapé do site (`26.974.270/0001-97`, GARGULIA LTDA). O consumidor, ao pagar, **não tem como confirmar que o dinheiro chega ao vendedor anunciado**. Somam-se a isto: **domínio recém-registrado** (06/06/2026, ~23 dias na coleta), titular oculto, **ausência total de páginas legais** (Termos, Privacidade, Trocas/Devolução respondem 404) e apelos de **falsa escassez** ("o que some, não volta"; "drops numerados").

Observa-se que o CNPJ exibido (GARGULIA LTDA) é **real e ativo**, com atividade de comércio varejista de vestuário desde 2017 — fato que se registra para a devida ponderação. Ainda assim, o CNPJ exibido **não comprova** que esta loja específica seja por ele operada, e o **fluxo financeiro não aponta para essa pessoa jurídica**. O conjunto de sinais — preços impossíveis de grifes, PIX a terceiro intermediário, domínio novíssimo e ausência de canais legais/de troca — configura **risco elevado de não entrega e/ou de produto falsificado** ao consumidor.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: uma loja que recebe dinheiro por PIX **em nome de um intermediário alheio**, oferece grifes a preços impossíveis, existe há poucas semanas e **não disponibiliza política de troca/devolução nem identificação verificável do operador deste site** oferece ao consumidor risco elevado de prejuízo. Recomenda-se **não comprar e não pagar o PIX** (Seções 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 HTTP/TLS e os bundles JavaScript foram obtidos por requisição equivalente à de um navegador. O código PIX "copia e cola" fornecido pelo solicitante foi decodificado pelo padrão EMV/BR Code (TLV) e teve seu CRC16 conferido. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (GMO Registry / .shop — registrador Hostinger)	`rdap_raw.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS (HTTP/2) + porta 80	`corpo.html · checkout.html · headers_https.txt`

Aplicação (front-end)	Download dos bundles JS (Next.js/Turbopack)	`chunks _next/static (analisados)`
Certificado TLS	openssl s_client / x509	`ssl_cert.txt · ssl_raw.txt`
Geolocalização do IP	ipinfo.io · ip-api.com	`geoloc.txt`
Intermediário de pagamento	RDAP + DNS de owem.com.br / qrcode.owem.com.br	`rdap_owem.json · dns_owem.txt · geo_owem.txt`
Código PIX (BR Code)	Decodificação EMV/TLV + CRC16	`pix_copia_e_cola.txt`
CNPJ exibido	Base pública (BrasilAPI / Receita)	`cnpj_lojista.json`
Imagens / metadados	Download de assets · exiftool	`imagens/ · metadata_exiftool.txt`

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

Domínio	gargulagarimpo.shop (gTLD .shop — GMO Registry)
Registro	**06/06/2026** · expira 06/06/2027 (validade de 1 ano)
Idade na coleta	**~23 dias** — domínio recém-registrado
Titular	**Oculto** (privacidade; RDAP expõe só o registrador)
Registrador	Hostinger operations, UAB (IANA ID 1636)
Status	client transfer prohibited
Servidores de nome	andy / monika.ns.cloudflare.com (Cloudflare — apenas DNS)
DNS — A	216.150.1.1 (anycast Vercel/AWS) · sem AAAA · sem MX · sem TXT/SPF
www	CNAME cname.vercel-dns.com → 66.33.60.130 · 76.76.21.61
Hospedagem	Vercel (Next.js) sobre AWS · edge "gru1" (São Paulo) na resposta HTTP
Geolocalização do IP	Anycast (org. Vercel/Amazon, AS16509) — não revela a localização do operador
Servidor web	Server: Vercel · porta 80 → 308 HTTPS
Certificado TLS	CN=gargulagarimpo.shop · emissor Let's Encrypt YR2 (DV) · válido 09/06/2026–07/09/2026
Série / Fingerprint	0551BE85E8A24298…239C3A80 · SHA-256 53:71:C0:AC:7E:F0:7E:91:EA:80:C3:A1:59:DD:37:A0…

Leitura técnica. Registro muito recente, validade de 1 ano e titular oculto compõem um perfil de **baixa rastreabilidade do responsável**. A loja é uma aplicação **Next.js publicada na Vercel** (plataforma de hospedagem legítima e de uso amplo) com DNS na Cloudflare; o certificado DV gratuito (Let's Encrypt) comprova apenas o controle do domínio, **não a identidade de qualquer empresa**. Não se imputa conduta ao registrador (Hostinger), à Cloudflare nem à Vercel/Amazon, meros intermediários de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site entrega uma **loja virtual de roupas e acessórios** ("Garimpo Gárgula"), em português (pt-BR), construída em **Next.js** (App Router/RSC). O catálogo lista **436 itens** (293 femininos, 143 masculinos) em categorias como blusas/jaquetas, camisetas, calças, vestidos, corsets, sapatos e bolsas, sob a narrativa de **"peças únicas / drops numerados"** e **"garimpo exclusivo"**. Diversos itens usam nomes de **marcas conhecidas** (ex.: "adidas vintage fleece jacket" R$ 45,90; "sueter stone island" R$ 34,50; "tenis bapesta" R$ 59,50; "tenis converse" R$ 55,40) — **preços incompatíveis com produtos autênticos**. O pagamento é **exclusivamente por PIX**, com o BR Code gerado no servidor (Server Actions Next.js) e intermediado por `owem.com.br`. O checkout coleta dados de contato e **endereço de entrega via CEP**.

Aspecto	Constatação
Tipo de serviço	Loja virtual de roupas/streetwear "Garimpo Gárgula" (436 itens anunciados como peças únicas)
Tecnologia	Next.js (RSC/Turbopack) hospedado na Vercel · imagens via proxy images.weserv.nl · Pixel do TikTok
Meio de pagamento	**Exclusivamente PIX** ("pagamento seguro via Pix · confirmação na hora"); sem cartão/boleto
Intermediário (gateway)	owem.com.br (qrcode.owem.com.br) — payload PIX gerado no servidor
Recebedor do PIX	**ZAPCOIN INTERMEDIACOES LTDA** (São Paulo) — **não** é "Garimpo Gárgula" nem o CNPJ exibido
Dados pessoais coletados	Nome, e-mail, telefone (WhatsApp) e endereço de entrega (CEP/logradouro). **Não** observada coleta de CPF
Identificação do operador	Rodapé exibe CNPJ 26.974.270/0001-97 = **GARGULIA LTDA** (ATIVA, vestuário, Cesário Lange/SP, desde 2017) — real, mas não comprova a operação deste site
Páginas legais	**Ausentes** — /termos, /privacidade, /trocas, /sobre respondem **404**
Contato divulgado	Instagram @gargulagarimpo · WhatsApp wa.me/5515981732101 (DDD 15) · sem e-mail corporativo (sem MX)
Apelos de marketing	Falsa escassez ("o que some, não volta"; "peças numeradas") e promo de estreia ("10 peças por R$ 199,90 · frete grátis")

Leitura técnica. O ponto central é a **desconexão entre quem anuncia e quem recebe**: o pagamento por PIX é feito a **"ZAPCOIN INTERMEDIACOES LTDA"**, um intermediário de pagamento, e não à loja nem ao CNPJ exibido. Embora o uso de sub-adquirentes/gateways que registram a chave PIX em nome próprio seja prática existente no mercado, do ponto de vista do consumidor isso **impede a conferência do destino do dinheiro**. Combinado a **grifes a preços impossíveis**, **domínio de poucas semanas** e **ausência de política de troca/devolução** (páginas 404), o perfil é compatível com **loja de não entrega e/ou de produto falsificado**. Registra-se, para ponderação, que o CNPJ exibido é real e ativo; ainda assim, ele não recebe o PIX nem comprova a titularidade deste domínio. Não se imputa conduta às plataformas de infraestrutura e de pagamento citadas (Vercel, Cloudflare, Hostinger, owem).

PIX decodificado (BR Code/EMV, CRC16 válido). Recebedor: **ZAPCOIN INTERMEDIACOES LTDA** · Cidade: SAO PAULO · Valor: **R$ 43,80** · Moeda: 986 (BRL) · País: BR · Chave/URL: `qrcode.owem.com.br/pix/dbafqpjokij2gc7rgvu7hopfyw` · MCC: 0000 · Iniciação: 12 (dinâmica) · TxID: *** (ocultado). O domínio do intermediário `owem.com.br` foi registrado em 29/07/2025 por **pessoa física** (CPF mascarado nos dados públicos), com DNS na Cloudflare e o subdomínio qrcode em Google Cloud.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Marcas de grife/streetwear (Adidas, Stone Island, C.P. Company, "bapesta", Converse, Levi's) a R$ 17–65, incompatível com itens autênticos	`corpo.html · catálogo`	ALTA

2	PIX vai a intermediário ("ZAPCOIN INTERMEDIACOES LTDA") que não é a loja nem o CNPJ exibido	`pix_copia_e_cola.txt`	ALTA
3	Pagamento exclusivamente por PIX, sem cartão/boleto e sem gateway nomeado ao consumidor	`corpo.html · app JS`	ALTA
4	Domínio recém-registrado (~23 dias), validade de 1 ano, titular oculto	`RDAP — 06/06/2026`	MÉDIA
5	Ausência de páginas legais (Termos, Privacidade, Trocas/Devolução → 404), em desacordo com o CDC	`HTTP 404 nas rotas legais`	MÉDIA
6	Falsa escassez/urgência ("o que some não volta"; "peças numeradas"; promo de estreia)	`corpo.html · app JS`	MÉDIA
7	Intermediário owem.com.br registrado por pessoa física; PIX gerado no servidor	`rdap_owem.json`	MÉDIA
8	CNPJ exibido (GARGULIA LTDA) real e ativo, porém não recebe o PIX nem comprova a operação deste site	`cnpj_lojista.json`	MÉDIA
9	Contato só por Instagram/WhatsApp; sem e-mail próprio (sem MX/TXT)	`dns_records.txt`	BAIXA
10	Imagens de produto sem metadados (reprocessadas); origem do catálogo não verificável	`metadata_exiftool.txt`	BAIXA

Síntese: 3 indicadores de severidade ALTA, 5 MÉDIA e 2 BAIXA. O CNPJ ativo é o único elemento de possível legitimidade, mas **não se conecta ao fluxo financeiro** (que vai a um terceiro) nem comprova a titularidade deste site — pelo que **não neutraliza** os indicadores de risco ao consumidor.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 29/06/2026, conclui-se que **gargulagarimpo.shop** é uma **loja virtual de roupas em operação**, voltada ao público brasileiro, que anuncia **itens de grife a preços irreais** e recebe pagamento **exclusivamente por PIX** em nome de um **intermediário ("ZAPCOIN INTERMEDIACOES LTDA")** que não corresponde à loja nem ao CNPJ exibido. O domínio tem **poucas semanas**, o titular do registro está oculto e o site **não disponibiliza política de troca/devolução nem identificação verificável do operador deste endereço**. Embora o CNPJ exibido (GARGULIA LTDA) seja real e ativo, ele não recebe o pagamento e não comprova a operação deste site. O conjunto configura **RISCO ALTO** de não entrega e/ou de produto falsificado ao consumidor.

Recomendações ao consumidor / solicitante

- **Não comprar, não pagar o PIX e não fornecer dados pessoais ou de endereço** ao site.
- Desconfiar de **marcas conhecidas a preços muito abaixo do mercado** e de anúncios (Instagram, TikTok, WhatsApp) que prometam "achados raros"/"drops numerados" com pagamento só por PIX.
- Antes de qualquer PIX, conferir o **nome do recebedor** no app do banco: aqui ele é **"ZAPCOIN INTERMEDIACOES LTDA"**, e não a loja — sinal de alerta.
- Se já houve pagamento: acionar imediatamente o banco e o mecanismo **MED** do PIX, reunir comprovantes e registrar reclamação em **consumidor.gov.br** e Boletim de Ocorrência.

Recomendações de mitigação / denúncia

- Denunciar o domínio aos canais de **abuse** do registrador (Hostinger), da Cloudflare e da Vercel, e reportar o golpe à **Polícia Civil** e ao **Procon**, anexando este laudo.
- Comunicar o **PSP/intermediário** envolvido (owem) e o banco do recebedor sobre uso da conta PIX em possível fraude de e-commerce, para apuração e eventual bloqueio.

- Preservar este relatório e as evidências (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. 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 e de pagamento citados, nem à pessoa jurídica cujo CNPJ é exibido no site, cuja relação efetiva com esta loja não foi possível confirmar por fontes abertas.

— Fim do relatório —

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