RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

futvexbrasil.com

Objeto investigado	futvexbrasil.com — loja virtual "Futvex" de camisas de futebol / roupas esportivas (gTLD .com)
Natureza	Verificação de legitimidade e de risco ao consumidor (e-commerce)
Data da coleta	27/06/2026 (RDAP, DNS, HTTP/TLS, geolocalização, conteúdo, decodificação PIX)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise de conteúdo · BR Code (EMV)
Achado central	Loja recém-criada SEM identificação do operador (CNPJ/razão social/endereço); recebedor PIX = gateway "DLOCAL", não a loja
Classificação	**RISCO ALTO**
Emissão do laudo	27/06/2026 às 03:12

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **futvexbrasil.com**, realizada em **27/06/2026** 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 em português** chamada **"Futvex"** (título "Futvex"; descrição "roupas esportivas masculinas premium"), que vende **camisas de futebol** de seleções e clubes — inclusive modelos da **Copa do Mundo 2026** (Brasil, Argentina, Portugal, etc.) e camisas "retrô" — a preços entre **R$ 198,50 e R$ 399,00**. A loja é uma **vitrine Shopify** (`jtxi0c-5b.myshopify.com`) servida atrás da Cloudflare, com checkout intermediado pela plataforma brasileira **Yampi** e **pagamento por PIX**. O domínio foi registrado na **Hostinger**, com os servidores de e-mail/DNS apontados a essa provedora.

A decodificação do código **PIX "copia e cola"** fornecido (BR Code/EMV, íntegro — CRC16 conferido) mostra um **PIX dinâmico** cujo recebedor exibido é **"DLOCAL"** (cidade "SAO PAULO"), resolvido em `qrcode.dlocal.com` — o agregador/processador de pagamentos **dLocal**. Ou seja, na tela do PIX o consumidor vê o **intermediário de pagamento**, e **não o estabelecimento "Futvex"**, de modo que **não é possível verificar quem efetivamente recebe os valores**.

O conjunto de sinais é o de uma operação de e-commerce **recém-criada e com baixa transparência**: domínio **registrado há cerca de cinco semanas** (19/05/2026), **nenhuma identificação do operador** no site (sem CNPJ, razão social ou endereço — apenas um e-mail de contato), **contato sem telefone**, mecanismos de **urgência artificial** (carrinho com expiração de 10 minutos) e venda de **camisas de seleções/Copa do Mundo sem evidência de licenciamento oficial**. No Brasil, o comércio eletrônico é obrigado a informar de forma clara o **CNPJ/identificação e o endereço físico** do fornecedor (art. 5º do Decreto 7.962/2013 — "Lei do E-commerce" — e CDC), exigência **não cumprida** por este site.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: uma loja que recebe dinheiro (PIX) e dados pessoais **sem identificar quem a opera**, sem endereço ou telefone, com domínio recém-criado e com o recebedor do PIX **mascarado pelo nome do gateway**, oferece ao consumidor **risco elevado** — ausência de fornecedor localizável para troca, garantia ou reembolso, e incerteza sobre a entrega do produto. Recomenda-se **cautela máxima: não comprar nem pagar** antes de confirmar a identidade do fornecedor (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 HTTPS e os cabeçalhos foram coletados por requisição de navegador comum sobre TLS. O código PIX "copia e cola" foi fornecido pelo solicitante e decodificado localmente pelo padrão EMV/BR Code (TLV), com verificação do dígito CRC16. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (Verisign / .com — registrador Hostinger)	`rdap_raw.json`
DNS	dig @1.1.1.1 (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTP/1.1 sobre TLS (navegador comum)	`corpo.html · headers_https.txt`

Páginas de política	Download das páginas de contato/termos/trocas	`page_policies_*.html · page_pages_contact.html`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · ip-api.com · PTR reverso	`geo_ipinfo.json · geo_ipapi.json · ptr.txt`
Pagamento (PIX)	Decodificação EMV/BR Code (TLV) + verificação CRC16	`pix_decode.txt`
Intermediário (gateway)	RDAP + DNS (dlocal.com / qrcode.dlocal.com)	`rdap_dlocal.json`
Imagens / metadados	Download de assets · exiftool	`imagens/ · metadata_exiftool.txt`

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

Domínio	futvexbrasil.com (gTLD .com — Verisign)
Registro	**19/05/2026** · expira 19/05/2027 (validade de 1 ano)
Idade na coleta	**~5–6 semanas** — domínio recente
Registrador	HOSTINGER operations, UAB (abuse-tracker@hostinger.com)
Titular	Não exposto no RDAP (privacidade de registro)
Status	clientTransferProhibited
Servidores de nome	apollo / athena.dns-parking.com (Hostinger)
DNS — A	23.227.38.65 (Shopify) · sem AAAA
www	CNAME → shops.myshopify.com → 23.227.38.74 (Shopify)
MX / e-mail	mx1 / mx2.hostinger.com · SPF: include:_spf.mail.hostinger.com
Hospedagem (loja)	Shopify, Inc. — vitrine jtxi0c-5b.myshopify.com (cabeçalho "powered-by: Shopify")
Borda / CDN	AS13335 Cloudflare, Inc. (anycast) — PTR myshopify.com
Geolocalização do IP	Anycast (ipinfo: Ottawa/CA) — não revela a localização real do servidor
Servidor web	Server: cloudflare · content-language pt-BR · país de atendimento BR
Certificado TLS	CN=futvexbrasil.com · emissor Let's Encrypt E7 (DV) · válido 19/05/2026–17/08/2026
Série / Fingerprint	05559C4EA97239B97A88798537AF2B033D30 · SHA-256 B8:92:6F:5D:F1:4E:03:FC:93:D3:2A:CD:1E:21:AB:68…

Leitura técnica. A loja é uma **vitrine Shopify** (plataforma legítima de e-commerce) com domínio próprio registrado na **Hostinger** há poucas semanas e validade de apenas um ano — perfil de **operação nova e de baixo custo**. O endereço IP público pertence à infraestrutura da Shopify/Cloudflare e **não identifica o lojista**; o certificado DV gratuito (Let's Encrypt) comprova apenas o controle do domínio, **não a identidade de qualquer empresa**. **Não se imputa qualquer conduta** à Shopify, à Hostinger, à Cloudflare ou ao gateway de pagamento — são meros provedores de infraestrutura; a responsabilidade pelo conteúdo e pela operação comercial é do lojista, que aqui permanece não identificado.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site entrega uma **loja virtual de camisas de futebol e roupas esportivas** ("Futvex"), em português (pt-BR, moeda BRL), construída sobre **Shopify** (tema "concept"). O catálogo inclui camisas de seleções para a **Copa do Mundo 2026** (Brasil, Argentina, Portugal, França, Inglaterra, Alemanha, etc.) e camisas "retrô" de clubes, com preços anunciados entre **R$ 198,50 e R$ 399,00** e oferta de "frete grátis". O fluxo de compra usa complementos de **aumento de ticket e urgência** (app "Kaching Bundles/Cart", com **carrinho que expira em 10 minutos**) e o **checkout é intermediado pela plataforma brasileira Yampi**; o pagamento é por **PIX** (e há referência a PayPal).

A decodificação do **PIX "copia e cola"** fornecido confirma um **PIX dinâmico** (BR Code/EMV íntegro, CRC16 = 79E2 conferido) com payload em `qrcode.dlocal.com/qr/25021356/v1/…`, recebedor **"DLOCAL"**, cidade "SAO PAULO", moeda 986 (BRL). O recebedor exibido é, portanto, o **agregador de pagamentos dLocal** — empresa de processamento transfronteiriço (domínio `dlocal.com` registrado em 2013, infraestrutura AWS/Cloudflare) — e **não o estabelecimento "Futvex"**.

Aspecto	Constatação
Tipo de serviço	Loja virtual (e-commerce) de camisas de futebol e roupas esportivas — "Futvex"
Plataforma	Shopify (jtxi0c-5b.myshopify.com) · tema "concept" · apps Kaching Bundles/Cart e GoPixel (rastreamento)
Meio de pagamento	PIX (checkout intermediado pela Yampi) · referência a PayPal
Recebedor do PIX	**"DLOCAL"** (agregador dLocal · qrcode.dlocal.com) — **não** a loja "Futvex"; consumidor não identifica o destino real
Dados pessoais coletados	Dados de cadastro/checkout: nome, e-mail, telefone, endereço de entrega e dados de pagamento (padrão de checkout Shopify/Yampi)
Identificação do operador	**Ausente** — sem CNPJ, razão social ou endereço físico; apenas e-mail (contato@futvexbrasil.com / contato@futvex.com) e horário de atendimento
Contato divulgado	E-mail e "WhatsApp" (campo vazio na página); **sem telefone e sem endereço**
Licenciamento dos produtos	Vende camisas de seleções/Copa do Mundo 2026 e de clubes **sem evidência de licenciamento oficial** (indício de produto não oficial/réplica)
Táticas de conversão	Urgência artificial (carrinho expira em 10 min), bundles/upsell, "frete grátis"

Leitura técnica. A tecnologia (Shopify + Yampi + dLocal) é, em si, **legítima e amplamente usada** por lojas reais; o risco aqui **não está nos provedores**, mas na **opacidade do lojista**: recebe pagamento e dados pessoais **sem se identificar** (sem CNPJ/razão social/endereço, exigência legal do e-commerce brasileiro) e exibe no PIX o nome do **intermediário** em vez do estabelecimento, removendo a transparência sobre o destino do dinheiro. Esse arranjo — domínio novo, vitrine genérica, urgência artificial e produtos de seleções sem licenciamento — é **compatível com o padrão de lojas-fantasma/dropshipping de baixa confiabilidade**, em que há risco de não entrega, de produto diverso do anunciado e de dificuldade de troca/reembolso. Trata-se de **juízo técnico de risco**, e não de afirmação de fraude consumada.
Imagens. Os assets gráficos baixados (fotos de produto e logo) estão hospedados no CDN da Shopify e foram entregues **sem metadados EXIF/GPS/autor** (removidos na reotimização do servidor), com **perfil de cor ICC uniforme** (Little CMS / CC0) — coerente com material reprocessado em massa, típico de catálogos de template/dropshipping. Não há, nas imagens, dado que identifique o operador. Ver `imagens/metadata_exiftool.txt`.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Loja recebe pagamento sem identificar o operador (sem CNPJ/razão social/endereço) — descumpre o art. 5º do Decreto 7.962/2013	`page_policies_*.html` · `corpo.html`	ALTA

2	Recebedor do PIX é o gateway "DLOCAL", não a loja — destino do dinheiro não verificável pelo consumidor	`pix_decode.txt`	ALTA
3	Domínio recém-registrado (~5–6 semanas), validade de 1 ano	`rdap_raw.json` — 19/05/2026	ALTA
4	Contato sem telefone e sem endereço físico (só e-mail; campo WhatsApp vazio)	`page_policies_contact-information.html`	MÉDIA
5	Camisas de seleções/Copa do Mundo 2026 e de clubes sem evidência de licenciamento oficial (possível réplica)	`corpo.html`	MÉDIA
6	Urgência artificial: carrinho expira em 10 minutos (app Kaching)	`corpo.html`	MÉDIA
7	Origem da loja atrás de Cloudflare/Shopify; lojista não localizável por dados de rede	`dns_records.txt` · `headers_https.txt`	MÉDIA
8	Imagens de catálogo sem metadados e com ICC uniforme (reprocessamento em massa / template)	`metadata_exiftool.txt`	BAIXA
9	Preços "premium" (R$ 198–399) com "frete grátis" e bundles/upsell — padrão de conversão agressiva	`corpo.html`	BAIXA

Síntese: 3 indicadores de severidade ALTA, 4 MÉDIA e 2 BAIXA. **Nenhum fator de legitimidade verificável** (operador identificado por CNPJ/razão social, endereço, telefone, histórico ou licenciamento de produto) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 27/06/2026, conclui-se que **futvexbrasil.com** é uma **loja virtual em operação** ("Futvex", sobre Shopify), voltada ao público brasileiro, que vende camisas de futebol e recebe pagamento por **PIX**, porém **sem identificar quem a opera** (não há CNPJ, razão social, endereço ou telefone — apenas um e-mail), com **domínio recém-criado** e com o **recebedor do PIX mascarado pelo nome do gateway "DLOCAL"**, de modo que o consumidor não consegue verificar o destino do pagamento. Soma-se a venda de camisas de seleções/Copa do Mundo **sem evidência de licenciamento oficial** e o uso de **urgência artificial** no carrinho. Esse conjunto descumpre o dever legal de identificação do fornecedor no e-commerce (Decreto 7.962/2013 e CDC) e configura **baixa confiabilidade**. Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não efetuar compras nem pagar o PIX** enquanto não houver identificação clara do fornecedor (CNPJ, razão social e endereço) e confirmação de sua idoneidade.
- Desconfiar de **preços, "frete grátis" e contagem regressiva** de carrinho usados para pressionar a decisão; verificar a reputação do site no **Reclame Aqui** e em **consumidor.gov.br** antes de comprar.
- Tratar camisas de seleções/clubes vendidas como "oficiais/premium" por loja não identificada como **possíveis réplicas não licenciadas**.
- Se já houve pagamento: reunir comprovantes, acionar o **banco** e o mecanismo **MED** do PIX, e registrar reclamação em **consumidor.gov.br** e, se for o caso, Boletim de Ocorrência.

Recomendações de mitigação / denúncia

- Reportar a loja aos canais de abuse da **Shopify** (plataforma) e da **Hostinger** (registrador do domínio), bem como ao **Procon** e à **SaferNet/consumidor.gov.br**, anexando este laudo, por descumprimento do dever de identificação do fornecedor no comércio eletrônico.
- 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. 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 (Shopify, Hostinger, Cloudflare, Yampi e dLocal), meros intermediários técnicos.

— Fim do relatório —

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