RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

10pilaoficial.site

Objeto investigado	10pilaoficial.site — "10PilaTV Max 2026", página que vende acesso a uma "central de entretenimento" com canais de TV ao vivo, filmes e séries (gTLD .site)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	02/08/2026 (RDAP, DNS, HTTP/TLS, geolocalização, leitura do bundle JavaScript)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do bundle público
Achado central	A página de vendas anuncia "50.000 canais HD e 4K" por R$ 10 mensais, enquanto o dado estruturado e o FAQ do mesmo bundle descrevem o produto como um "guia digital de economia com streaming" — duas descrições incompatíveis do que o consumidor está comprando
Classificação	**RISCO ALTO**
Emissão do laudo	02/08/2026 às 01:38

1. Sumário Executivo

Este laudo documenta a análise técnica do endereço **10pilaoficial.site**, realizada em **02/08/2026** por técnicas de OSINT e coleta passiva — requisições equivalentes às de um visitante comum, sem preenchimento de formulário, sem geração de cobrança e sem envio de dados pessoais. Toda evidência foi preservada com hash SHA-256 (Anexo A).

O endereço **está no ar**, redireciona para `www.10pilaoficial.site` (HTTP 307) e entrega uma aplicação React servida pela **Vercel**. A oferta anunciada é uma assinatura de entretenimento em três faixas — **R$ 10 mensal, R$ 25 trimestral e R$ 79 anual** — todas descritas no bundle como incluindo "os mesmos **50.000 canais HD e 4K**". O fluxo de compra declarado é: "Você preenche nome e e-mail, gera o Pix e paga no banco. Após confirmar, o acesso vai para o e-mail."

O achado central é uma **divergência interna na descrição do produto**. O mesmo bundle que anuncia 50.000 canais ao vivo descreve o item vendido, no dado estruturado e no FAQ, como **"Plano TV Enxuta 2026"** e **"Guia digital de economia com streaming"**, cujo conteúdo seriam "orientações para Smart TV, Fire Stick, Android TV, celular e notebook". São duas naturezas de produto distintas: acesso a canais de terceiros e material informativo não são a mesma coisa, e o consumidor que paga por uma das descrições pode legitimamente receber a outra. Nenhuma evidência coletada demonstra **autorização ou licenciamento** para distribuir o conteúdo audiovisual anunciado.

O perfil de identificação é o de um endereço de baixo compromisso: domínio registrado em **28/11/2025** por **um ano**, titular não publicado no RDAP, **sem registro MX** — de modo que o próprio domínio não recebe e-mail, embora a entrega prometida ao comprador seja justamente "o acesso vai para o e-mail". Não há CNPJ, razão social, endereço ou telefone em qualquer página, e o único atendimento é um assistente de conversa embutido na página ("Oi, sou a Maria. Posso te ajudar a escolher o melhor plano?"), que orienta o visitante a começar pelo plano mensal.

Registre-se ainda que a página pré-resolve, por `dns-prefetch`, o host `tf.digirocket.site`, de domínio distinto. Esse host resolve nos mesmos endereços IP da Vercel usados pelo site — o que **não indica operador comum**, já que a Vercel compartilha esses IPs entre seus clientes. O registro é feito apenas como fato observado.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: um endereço que vende, por R$ 10, acesso a milhares de canais de TV sem demonstrar licenciamento, descreve o mesmo produto de duas formas incompatíveis, não identifica quem o opera e cobra por Pix antecipado — com entrega prometida por e-mail em um domínio que não recebe e-mail. O conjunto oferece **risco elevado** ao consumidor.

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 endereço	RDAP do registro responsável	`rdap_raw.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS (visitante comum)	`corpo_home.html · headers_home.txt`

Certificado TLS	openssl s_client + x509	`tls_cert.txt`
Hospedagem / origem	ipinfo.io + PTR reverso	`geoip.json`
Aplicação	Leitura do bundle JavaScript público	`bundle_index.js`
Integridade	SHA-256 de cada arquivo coletado	`hash_manifest.txt`

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

Domínio	10pilaoficial.site (gTLD .site — Radix)
Registro	**28/11/2025** · expira 28/11/2026 (validade de 1 ano)
Última alteração	03/12/2025
Idade na coleta	**~8 meses**
Registrador	HOSTINGER operations, UAB
Titular	**Não publicado** (o RDAP expõe apenas o registrador)
Status	client transfer prohibited
Nameservers	ns1.vercel-dns.com · ns2.vercel-dns.com
Endereço IP	64.29.17.65 (AS16509 Amazon, via Vercel) · cabeçalho `server: Vercel`
Registro MX	**Nenhum** — o domínio não recebe e-mail
Registro TXT	google-site-verification (verificação do Google Search Console)
Certificado TLS	Let's Encrypt (YR2) · emitido em **02/08/2026**, o próprio dia da coleta → 31/10/2026
Identificação legal	**Ausente** — sem CNPJ, razão social, endereço ou telefone
Host pré-resolvido	`tf.digirocket.site` (dns-prefetch) — mesmos IPs Vercel, compartilhados entre clientes

Leitura técnica. O registro de um ano com titular oculto e a hospedagem em plataforma de publicação instantânea compõem uma estrutura de custo e de vínculo baixíssimos — trocar de endereço, nesse arranjo, custa o preço de um novo domínio. A ausência de MX é especialmente relevante porque **contradiz o próprio fluxo de entrega anunciado**: o site promete enviar o acesso por e-mail, mas o domínio não está configurado para trocar mensagens.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

A aplicação é uma **SPA React** (bundle `index-DG_EftmU.js`, 35 KB, mais um *vendor* com React e React Router) publicada na Vercel. O bundle não contém nenhum endpoint de API próprio: a rota `/checkout?produto=plano-tv-enxuta-2026` é client-side, e o fluxo de cobrança não foi acionado nesta coleta. Todo o conteúdo abaixo foi lido do código público entregue ao navegador.

Item verificado	Constatação
Plano mensal	R$ 10 — apresentado pelo assistente como "o caminho mais rápido" para testar
Plano trimestral	R$ 25
Plano anual	R$ 79
Conteúdo anunciado	"Todos incluem os mesmos **50.000 canais HD e 4K**"
Descrição no dado estruturado	"Guia digital de economia com streaming" · "Plano TV Enxuta 2026"
Resposta do FAQ	"O Plano TV Enxuta 2026 inclui **orientações** para Smart TV, Fire Stick, Android TV, celular e notebook"
Meio de pagamento	**Pix** — "você preenche nome e e-mail, gera o Pix e paga no banco"
Entrega	"Após confirmar, o acesso vai para o e-mail" — domínio sem registro MX
Garantia	Declarada de 7 dias ("o produto comunica garantia de 7 dias")
Atendimento	Assistente embutido na página ("Oi, sou a Maria"), sem telefone ou e-mail publicado
Licenciamento	Nenhuma evidência de autorização para distribuir o conteúdo anunciado

Aspecto	Constatação
Tipo de serviço	Assinatura de acesso a canais de TV, filmes e séries (ou "guia", conforme a descrição consultada)
Tecnologia	React (SPA) publicada na Vercel · redirecionamento 307 para www
Hospedagem	Vercel (IPs Amazon/AWS) — publicação instantânea, sem vínculo cadastral exigido
Correio eletrônico	Ausente — sem MX, apesar de a entrega ser prometida por e-mail
Identificação do fornecedor	Nenhuma — sem CNPJ, razão social, endereço ou telefone
Documentos legais	Nenhuma página de termos, privacidade ou contato foi encontrada
Indexação	Configurado para indexação ampla (index, follow, max-image-preview:large) e verificado no Search Console
Certificado	Let's Encrypt emitido no dia da coleta — renovação automática da plataforma
Relato público	Reclame AQUI, 19/06/2026: compra no site sem resposta e sem recebimento do produto

Leitura técnica. Não há no código função maliciosa: o risco está no **modelo comercial**. O consumidor paga adiantado por Pix — meio sem mecanismo de contestação equivalente ao do cartão — para um fornecedor não identificado, contra a promessa de receber por e-mail o acesso a um catálogo cuja autorização de distribuição não é demonstrada em nenhum ponto do site. A divergência entre "50.000 canais" e "guia de orientações" agrava o quadro, porque **impede o comprador de saber, antes de pagar, o que exatamente está contratando**.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Anúncio de acesso a 50.000 canais de TV sem qualquer evidência de licenciamento ou autorização de distribuição	`bundle_index.js` · `corpo_home.html`	ALTA
2	O mesmo produto é descrito como acesso a canais e como guia digital de orientações — descrições incompatíveis	`bundle_index.js`	ALTA
3	Nenhuma identificação legal do fornecedor e nenhuma página de termos, privacidade ou contato	`corpo_home.html`	ALTA
4	Pagamento antecipado exclusivamente por Pix, sem gateway ou adquirente identificado na página	`bundle_index.js`	ALTA
5	Entrega prometida por e-mail em domínio que não possui registro MX	`dns_records.txt` · `bundle_index.js`	MÉDIA
6	Domínio registrado por apenas 1 ano, com titular não publicado	`rdap_raw.json`	MÉDIA
7	Hospedagem em plataforma de publicação instantânea, sem vínculo cadastral exigido do publicador	`headers_home.txt` · `geoip.json`	MÉDIA
8	Atendimento limitado a assistente embutido na própria página, sem canal externo verificável	`bundle_index.js`	BAIXA

Síntese: 4 indicadores de severidade ALTA, 3 MÉDIA e 1 BAIXA. Como único **fator de legitimidade** registra-se a declaração de garantia de 7 dias — que, sem fornecedor identificado nem canal de contato, não tem a quem ser dirigida.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em **02/08/2026**, **10pilaoficial.site** oferece **risco alto** ao consumidor. O site vende, por R$ 10 a R$ 79 pagos antecipadamente via Pix, acesso a um acervo de "50.000 canais HD e 4K" sem demonstrar em nenhum ponto autorização para distribuí-lo, e simultaneamente descreve o mesmo produto, em seu dado estruturado e em seu FAQ, como um "guia digital de economia com streaming" — de modo que o comprador **não tem como saber o que receberá antes de pagar**. Não há identificação legal do fornecedor, não há página de termos ou de contato, o domínio foi registrado por um ano com titular oculto e não possui registro MX, embora a entrega prometida seja por e-mail. Os pontos aqui descritos são corrigíveis: publicar identificação legal, uniformizar a descrição do produto, comprovar o licenciamento do conteúdo e configurar um canal de contato alterariam substancialmente esta classificação.

Recomendações ao consumidor / solicitante

- **Não pagar antecipadamente por Pix** a fornecedor que não publica CNPJ, endereço ou telefone — no Pix não há mecanismo de contestação equivalente ao do cartão de crédito.
- Desconfiar de oferta de milhares de canais de TV por valor simbólico: serviços licenciados têm custo de conteúdo e identificam a empresa responsável.
- Exigir, antes de comprar, descrição única e inequívoca do que está sendo vendido — acesso a canais e guia de orientações são produtos diferentes.
- Quem já pagou deve preservar comprovante, data, valor e as telas da oferta, e registrar reclamação no consumidor.gov.br; havendo Pix, procurar o próprio banco quanto aos mecanismos disponíveis, observando os prazos.

Recomendações de mitigação / denúncia

- Ao responsável pelo site: publicar razão social, CNPJ, endereço e canal de contato; uniformizar a descrição do produto entre a página de vendas, o dado estruturado e o FAQ; e configurar registro MX, já que a entrega prometida é por e-mail.
- Aos detentores de direitos do conteúdo audiovisual anunciado: as evidências deste laudo permitem instruir comunicação aos seus canais de proteção de direitos.

- Aos canais de *abuse* do registrador (Hostinger) e da plataforma de hospedagem (Vercel): o material preservado pode instruir comunicação, observando que ambos são provedores de infraestrutura sem responsabilidade sobre o conteúdo do cliente.
- Ao consumidor lesado: reunir comprovante e telas como base documental de reclamação administrativa e, se for o caso, de boletim de ocorrência.

Ressalva metodológica: este laudo baseia-se em fontes abertas e reflete o estado do endereço na data indicada. A coleta foi integralmente passiva — requisições equivalentes às de um visitante comum, sem criação de conta, sem envio de dados pessoais, sem tentativa de compra e sem qualquer interação intrusiva. Não se imputa conduta ilícita a provedores de infraestrutura (registrador, hospedagem, CDN, autoridade certificadora) nem a intermediários de pagamento regulados, que não respondem pelo conteúdo publicado por seus clientes. A classificação de risco é juízo técnico sobre o conjunto de indicadores observados, não decisão judicial nem afirmação sobre a intenção de quem opera o endereço. Sinais aqui descritos como alerta podem decorrer de escolhas de configuração e ser corrigidos pelo próprio responsável pelo site.

Anexo A — Manifesto de Integridade (SHA-256)

Hashes SHA-256 das evidências preservadas no momento da coleta (cadeia de custódia).

Arquivo	SHA-256
`corpo_home.html (6452 bytes)`	`1481281680ab9dbf85f7a24f36a735c93865c9a1f501993bce8a4a123a4d4dcf`
`dns_records.txt (412 bytes)`	`dd4da21da6d5fc76ca9badd59a56478b8cd10fa23f09679e05f75894fb56e9a6`
`geoip.json (279 bytes)`	`9020b267a9a73ae65168d143c89dfd03e7c902f6c78727c746ea00d827eae92f`
`headers_home.txt (807 bytes)`	`59f716347b9c86219c13e766502375e2b8b4d80328d3168e93cdb33c0ce2a84e`
`rdap_raw.json (5170 bytes)`	`659bbdaad3e36c56ccbc1c0f64549dbd6e69b7190656b12d3baa58db44d41806`
`tls_cert.txt (303 bytes)`	`5136c64ec85ce0cd908f28abc7c1a45161e1a20114964ac6760d96cc0d1752bc`

— Fim do relatório —