RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

brasa88.life

Objeto investigado	brasa88.life — cassino/apostas online voltado ao Brasil (gTLD .life)
Natureza	Verificação de legitimidade e de risco ao consumidor (apostas / "bet")
Data da coleta	11/06/2026 (RDAP, DNS, HTTP/TLS, geolocalização, análise do app)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do aplicativo (front-end)
Achado central	Cassino/apostas SEM identificação de operador e SEM autorização (Brasil)
Classificação	**RISCO ALTO**
Emissão do laudo	11/06/2026 às 16:19

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **brasa88.life**, realizada em **11/06/2026** 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.

O domínio **está no ar** e entrega um **aplicativo de cassino/apostas online ("bet")** voltado ao público brasileiro, construído como aplicação de página única (**SPA Vue** com biblioteca móvel Vant) servida atrás da **Cloudflare**. A interface é em português, a moeda é o **Real (BRL)**, o fuso configurado é **-03:00** (Brasília) e o fluxo financeiro usa **depósito e saque via PIX**. O front-end consome uma **API no mesmo domínio** (`/api`), com cadastro/login, carteira, recarga, saque, bônus, programa de agentes/indicação e jogos (roleta/"slots", motor externo `opkgame.com`). O pagamento é intermediado por um agregador identificado no código como **"pengpai"** (rotas `/pengpai/recharge`, `/pengpai/signIn` e `/dark_pix`).

O conjunto de sinais é o de uma operação **opaca e sem lastro verificável**: domínio **recém-registrado** (09/05/2026), **titular oculto** (RDAP com dados protegidos; expõe só o registrador Name.com), infraestrutura de origem **mascarada por Cloudflare**, e — no próprio aplicativo — **nenhuma identificação do operador** (sem CNPJ, razão social ou endereço), **nenhum selo de autorização regulatória brasileira** e suporte limitado a canais de **Telegram/WhatsApp**. O app embarca rastreamento agressivo de anúncios (**pixels da Kwai, TikTok e Facebook** e SDK **Adjust**, com eventos de conversão de cadastro e recarga), perfil típico de captação por tráfego pago em redes sociais.

Ponto juridicamente relevante: no Brasil, a exploração de apostas de quota fixa e jogos de azar online ("bets"/cassino) depende de **autorização federal** do Ministério da Fazenda (SPA/SIGAP, Lei 14.790/2023) e as casas autorizadas operam sob o domínio padronizado **.bet.br**. Este site usa o gTLD genérico **.life**, **não apresenta qualquer indício de autorização** e tem como público-alvo declarado o Brasil (idioma pt-BR, moeda BRL, PIX) — perfil compatível com **operação irregular/não autorizada**, categoria sujeita a bloqueio pelas autoridades brasileiras.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: uma plataforma que recebe dinheiro (PIX) e dados pessoais **sem identificar quem a opera nem comprovar autorização** oferece ao consumidor **risco elevado** — ausência de responsável localizável, ausência de garantia de pagamento de prêmios/saques e exposição de dados pessoais. Recomenda-se **não cadastrar, não depositar e não fornecer dados** (Seções 6 e 7).

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 (cadeia de custódia). O DNS foi consultado via `dig`; o conteúdo HTTP/HTTPS via `curl`; o certificado via `openssl`. A lógica de negócio — renderizada no cliente (SPA) — foi analisada a partir do **bundle JavaScript público** do site e de consultas de leitura a endpoints de configuração abertos, sem criar conta nem efetuar pagamento. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (.life — registrador Name.com)	`rdap_raw.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_dig.txt`
Conteúdo / cabeçalhos	curl (HTTPS e porta 80)	`corpo.html` · `headers_https.txt` · `headers_http80.txt`

Aplicação (front-end)	Download do bundle JS + endpoints de config abertos	`index.js`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · ip-api.com	`geo_ip.txt`
Integridade	sha256sum de todos os artefatos	`hash_manifest.txt`

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

Domínio	brasa88.life (gTLD .life — Identity Digital)
Registro	**09/05/2026** · expira 09/05/2027 (validade de 1 ano)
Idade na coleta	**~1 mês** — domínio recente
Titular	**Oculto** (RDAP com dados redigidos; expõe só o registrador)
Registrador	Name.com, Inc.
Status	clientTransferProhibited
Servidores de nome	irena / kai.ns.cloudflare.com (Cloudflare)
DNS — A	172.67.144.29 · 104.21.87.151 (Cloudflare) · AAAA presente · **sem MX** · **sem TXT/SPF**
Hospedagem (borda)	AS13335 Cloudflare, Inc. — **proxy/CDN que oculta o IP de origem**
Geolocalização do IP	Anycast Cloudflare (não revela a localização do servidor real)
Servidor web	Server: cloudflare · porta 80 → 301 HTTPS · cf-cache-status presente
Certificado TLS	CN=brasa88.life · emissor Let's Encrypt E8 (DV) · válido 09/05/2026–07/08/2026
Série / Fingerprint	0690E39D…51 · SHA-256 8B:47:0C:C0:53:CA:BE:E1:C5:8F:1A:25:CD:83:80:06…

Leitura técnica. Registro recente, validade de 1 ano e titular oculto compõem um perfil de **baixa rastreabilidade do responsável**. O uso de **Cloudflare como proxy oculta o IP de origem**, dificultando a localização do servidor que efetivamente armazena dados e processa pagamentos. O certificado DV gratuito (Let's Encrypt) comprova apenas o controle do domínio, **não a identidade de qualquer empresa**. A ausência de registros MX/TXT indica que o domínio **não mantém e-mail corporativo próprio**. Não se imputa conduta ao registrador (Name.com) nem à Cloudflare, meros intermediários de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site entrega um **cassino/casa de apostas online** em português, construído como SPA (Vue + Vuex + Vue-Router, UI móvel Vant/Element-Plus, roleta "lucky-canvas", fingerprint de dispositivo). A lógica é servida por uma **API no próprio domínio** (`/api`, atrás de Cloudflare), com cadastro/login (`/home/register`, `/home/login`), carteira, recarga, saque, bônus, **programa de agentes/indicação** e jogos servidos por provedor externo (`www.opkgame.com`). Depósito e saque são feitos por **PIX**, intermediados por um agregador identificado no código como **"pengpai"** (`/pengpai/recharge`, `/pengpai/signIn`, `/dark_pix`).

Aspecto	Constatação
Tipo de serviço	Cassino / apostas online ("bet") em BRL, público brasileiro (pt-BR, fuso -03:00)
Tecnologia	SPA Vue + Vant atrás de Cloudflare · API em /api · jogos externos (opkgame.com) — perfil white-label replicável
Meio de pagamento	Depósito e saque via PIX, intermediados pelo agregador "pengpai" (/pengpai/… · /dark_pix)
Rastreamento de anúncios	Pixels Kwai, TikTok e Facebook + SDK Adjust, com eventos de conversão de cadastro/recarga (sendFBregister, sendFBRechatge)
Dados pessoais coletados	Cadastro de usuário (telefone/usuário, senha) e dados de saque PIX; fingerprint de dispositivo
Identificação do operador	**Ausente** — sem CNPJ, razão social ou endereço no site/app
Autorização / licença	**Ausente** — sem selo SPA/SIGAP; apenas checkbox genérico "Tenho 18 anos"
Domínio	.life (genérico) — **não** o padrão .bet.br exigido das casas autorizadas no Brasil
Contato divulgado	Suporte via Telegram/WhatsApp · sem e-mail corporativo (sem MX)

Leitura técnica. O fluxo financeiro é real e operante: o usuário deposita por PIX e fornece dados de cadastro e de saque. O **risco não está na tecnologia, mas na ausência de responsável identificável e de autorização**: não há a quem cobrar prêmios/saques não pagos, nem garantia de tratamento adequado dos dados. A arquitetura (framework de cassino padronizado, gateway "pengpai", jogos de `opkgame.com` e origem oculta por Cloudflare) é típica de **plataformas de apostas replicadas em escala**, em que vários sites compartilham o mesmo backend e captam jogadores por tráfego pago. Não se imputa conduta ao provedor de jogos (opkgame), ao agregador de pagamento ("pengpai") nem à Cloudflare; descreve-se o fato e separa-se inferência de prova.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Cassino/apostas sem indício de autorização federal (SPA/SIGAP); em .life, não .bet.br	`corpo.html · index.js · RDAP`	ALTA
2	Sem identificação do operador (CNPJ/razão social/endereço)	`index.js · corpo.html`	ALTA
3	Recebe PIX e coleta dados pessoais sem responsável localizável	`index.js`	ALTA
4	Origem mascarada por Cloudflare (IP do servidor real oculto)	`dns_dig.txt · headers_https.txt`	MÉDIA
5	Domínio recém-registrado (~1 mês), validade de 1 ano	`rdap_raw.json — 09/05/2026`	MÉDIA
6	Titular oculto (RDAP com dados redigidos)	`rdap_raw.json`	MÉDIA
7	Rastreamento agressivo de anúncios (Kwai/TikTok/Facebook/Adjust) com eventos de recarga	`index.js · corpo.html`	MÉDIA

8	Plataforma white-label replicável (Vue/Vant; gateway "pengpai"; jogos opkgame.com)	`index.js`	MÉDIA
9	Suporte só por Telegram/WhatsApp; sem e-mail próprio (sem MX/TXT)	`index.js` · `dns_dig.txt`	BAIXA
10	Certificado DV gratuito (comprova só controle do domínio, não identidade)	`tls_cert.txt`	BAIXA

Síntese: 3 indicadores de severidade ALTA, 5 MÉDIA e 2 BAIXA. **Nenhum fator de legitimidade** (operador identificado, autorização brasileira, contato corporativo, histórico) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 11/06/2026, conclui-se que **brasa88.life** é um **cassino/casa de apostas online em operação**, voltado ao público brasileiro (pt-BR, BRL, PIX), que recebe depósitos via PIX e coleta dados pessoais, porém **sem identificar quem o opera** e **sem qualquer indício de autorização** para explorar jogos de azar/apostas no Brasil — usando o gTLD **.life** em vez do padrão regulado **.bet.br**, com a origem mascarada por Cloudflare e a lógica em uma plataforma white-label compartilhável (gateway "pengpai", jogos opkgame.com). Soma-se a isso o registro recente, o titular oculto, o rastreamento agressivo de anúncios e o contato limitado a Telegram/WhatsApp. Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não se cadastrar, não depositar e não fornecer dados pessoais ou bancários** ao site.
- Desconfiar de anúncios e mensagens (Kwai, TikTok, Instagram, Facebook, WhatsApp, Telegram) que conduzam a `brasa88.life` ou prometam bônus/ganhos fáceis.
- Se já houve depósito: acionar 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 à **Secretaria de Prêmios e Apostas (SPA/Ministério da Fazenda)** e à **Anatel** como cassino/apostas sem autorização, e reportar aos canais de abuse do registrador (Name.com) e da Cloudflare, anexando este laudo.
- 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, de jogos e de pagamento citados (Cloudflare, Name.com, opkgame, "pengpai"), meros intermediários.

— Fim do relatório —

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