

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

zezao.net

Objeto investigado	zezao.net - cassino e apostas “ZEZAO”
Natureza	Verificação do regime de operação no Brasil e de vínculos com outros domínios
Data da coleta	28/11/2026 (RDAP, DNS, HTTP/TLS, geolocalização, bases públicas, análise do código da página)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do HTML e dos scripts
Achado central	Cassino em português com depósito por Pix, operado por empresa declarada na Costa Rica com licença de Anjouan, que compartilha o mesmo código com **outros quatro cassinos**
Classificação	**RISCO ALTO**
Emissão do laudo	28/11/2026 as 01:06

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **zezao.net**, realizada em **28/11/2026** por técnicas de OSINT (inteligência de fontes abertas) e análise passiva — requisições equivalentes às de um visitante comum e consultas a bases públicas, sem cadastro, sem compra e sem envio de dados pessoais. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

O `zezao.net` foi registrado em 26/06/2026 (NameCheap, Inc.), está atrás da Cloudflare e publica um cassino com apostas esportivas em português (`lang="pt-BR"`). O código da página trata depósito e saque por **Pix**, pede CPF e exige que a chave Pix esteja no nome do apostador.

O rodapé atribui a operação à “Enigma Digital Solutions Limitada”, em San José (Costa Rica), “licenciada” pelo governo da ilha de Anjouan (Comores). Licença estrangeira não autoriza a oferta de apostas no Brasil, que exige autorização da SPA/MF e domínio .bet.br; `zezao.bet.br` não existe.

A página é a mesma aplicação Next.js de `metaigaming.io`, `v10.bet`, `vainabet.io`, `brotabet.co`: 28 dos 29 arquivos de script são idênticos, as imagens vêm do mesmo servidor (`cdn.meta-img.xyz`) e o rodapé é o mesmo. A metatag `og:url` aponta para `zezao.io`, outro domínio da mesma marca na mesma conta da Cloudflare.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: são várias marcas sobre uma única plataforma, o que permite trocar de nome quando um domínio é bloqueado; nenhuma tem autorização brasileira.

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 bundle JavaScript foram obtidos por requisição HTTPS de visitante comum. Nenhum formulário foi preenchido e nenhum dado pessoal foi enviado. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (rdap.org / registro do gTLD / Registro.br)	`rdap_raw.json · rdap_*.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME) via 1.1.1.1	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS (visitante comum) e navegador headless; home, páginas legais e scripts	`corpo_*.html · headers_home.txt · bundle*.txt`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · PTR reverso	`geoip.json`
CNPJ declarado	Validação por módulo 11 · base pública BrasilAPI/Receita	`cnpj_publico_*.json`
Consolidação	Extração de fatos e hashes SHA-256	`hash_manifest.txt`

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

Domínio	zezao.net
Registro	26/06/2026 · expira 26/06/2027 · **155 dias** antes da coleta
Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)

Registrador	NameCheap, Inc. · abuse@namecheap.com
Servidores de nome	bethany.ns.cloudflare.com · nick.ns.cloudflare.com
DNS - A	104.21.41.38 · 172.67.142.83 · MX: out, route3.mx.cloudflare.net
Hospedagem	AS13335 Cloudflare, Inc. · San Francisco/US · cabeçalho `server: cloudflare`
Certificado TLS	Let's Encrypt (YE2) · emitido em 09/10/2026 · válido até 07/01/2027
Rodapé	“Meta é operado pela Enigma Digital Solutions Limitada… San Jose, Costa Rica. Licenciado… pelo Governo da Ilha Autônoma de Anjouan”
Código compartilhado	28 de 29 arquivos Next.js idênticos aos de `metaigaming.io`, `v10.bet`, `vainabet.io`, `brotabet.co`
Domínio .bet.br	`zezao.bet.br` — NXDOMAIN

Leitura: domínio de 155 dias com titular oculto, atrás da Cloudflare.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Aplicação Next.js com rastreamento de campanhas (Utmify, Facebook Pixel, Google Tag Manager) e chat de atendimento (Digisac, Intercom, LiveChat).

Aspecto	Constatação
Pagamento	Depósito e saque por Pix, com CPF
Operador declarado	Enigma Digital Solutions Limitada (Costa Rica)
Licença declarada	Anjouan (Comores), sem número verificável na página
Marcas irmãs	`metaigaming.io`, `v10.bet`, `vainabet.io`, `brotabet.co`

Leitura: o apostador deposita por Pix em operador estrangeiro sem autorização no Brasil, sem a proteção da regulamentação nacional.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Cassino em português com depósito por Pix ao público brasileiro fora de domínio .bet.br	`corpo_home_resolve.html`	ALTA
2	Mesmo código (28 de 29 arquivos) de outros quatro cassinos com outros nomes	`rede_comparacao.txt`	ALTA
3	Operador declarado no exterior com licença de Anjouan, sem autorização brasileira	`corpo_home_resolve.html`	MEDIA
4	Domínio com titular oculto, 155 dias antes da coleta	`rdap_raw.json`	BAIXA

Síntese: 4 indicadores, 2 de severidade alta.

6. Conclusão Técnica e Recomendações

O zezao.net oferece cassino e apostas com depósito por Pix ao público brasileiro, fora do regime autorizado pela SPA/MF, como uma de pelo menos cinco marcas sobre a mesma plataforma. Classificação técnica: **RISCO ALTO**.

Recomendações ao consumidor / solicitante

- No Brasil, só operam legalmente as casas de apostas autorizadas pelo Ministério da Fazenda, sob domínio `.bet.br`; consulte a lista oficial da SPA/MF antes de depositar.
- Não instale aplicativos (APK) baixados fora das lojas oficiais nem informe CPF e dados bancários a operadores sem identificação verificável.
- Em disputa com operador fora do regime autorizado, o apostador não conta com a proteção da regulamentação brasileira para reaver saldo ou saques.

Recomendações de mitigação / denúncia

- Reportar o endereço ao Google Safe Browsing e ao canal de abuso do registrador (abuse@namecheap.com).
- Comunicar à Secretaria de Prêmios e Apostas (SPA/MF) e à Anatel a oferta de apostas ao público brasileiro fora do regime autorizado.
- Vítimas que pagaram via Pix: acionar o banco imediatamente pedindo o MED (Mecanismo Especial de Devolução), registrar boletim de ocorrência e reclamação em consumidor.gov.br / Procon, anexando este laudo.

Ressalva: este laudo expressa **juízo técnico de risco** com base em evidências públicas coletadas passivamente em 28/11/2026; não é decisão judicial e não imputa crime a nenhuma pessoa física ou jurídica. Registradores, provedores de hospedagem/CDN, plataformas de loja e intermediários de pagamento são citados apenas como fatos técnicos, sem imputação de conduta. O titular do site pode usar estes achados para corrigir as inconsistências apontadas. Os fatos podem mudar após a coleta.

Anexo A - Manifesto de Integridade (SHA-256)

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

Arquivo	SHA-256
bet_br_check.txt (211 bytes)	24206b5870837133c57134436184333e3d1fea39e0e5624cc5cb902fc393ea00
bundle_js.txt (398017 bytes)	bb1e0ee328e0537400e4b29826bcab977170133ef6bdb993310531b6356adf97
corpo_home.html (46957 bytes)	ed7c3c0555e3f180c7309914e07f777e1cde6c0129c32dadc04924f517f3be10
corpo_home_resolve.html (46957 bytes)	ed7c3c0555e3f180c7309914e07f777e1cde6c0129c32dadc04924f517f3be10
dns_records.txt (528 bytes)	ac5a106c0f78d6c4fea91447f9de929ea0483a9e15c03b8e1f72b80447139149
geoip.json (287 bytes)	2b72ee0e2ceead8a0541f21517fa91466c135a892ff3dfe65f80773d87a84e8e
headers_home.txt (1061 bytes)	16710c1436c9cfbd81913eba9e43c9fc206649610a2082206230f5181caf42ac
headers_home_resolve.txt (1019 bytes)	9dc377e36fb3e5b26dc387b6905b797901803cc4c9c1e722f963d7c4c23e4483
rdap_raw.json (2550 bytes)	ec464ed6aa999f35b55989e0f0e17b8cfc7f053579f05c6b12c6b33a513926c5
rede_comparacao.txt (502 bytes)	e2ea62569ba35001cad6ce3177ec4bdf35dd739d3c6b33415d9c55671cc1e6a2
resolvedores.txt (218 bytes)	d2078909aef1bb3ffcd97e0fad7e8814e7687a62c6f88e0b691df64aaa376fd2
tls_cert.txt (294 bytes)	4814de82e65d7df263b0d3f5b97746c988ff7c7d3a8e9afbb736ef0da8384da4

- Fim do relatório -