

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

tgjogos.com

Objeto investigado	tgjogos.com - casa de apostas e cassino online “TGJOGO”
Natureza	Verificação de legitimidade regulatória e de identidade do operador
Data da coleta	17/11/2026 (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 “TGJOGO” fora do `.bet.br`, servido pela mesma plataforma da SSSGAME (imagens no CDN `sssgameimgapi.com`) e sem resolução no DNS de provedor brasileiro
Classificação	**RISCO ALTO**
Emissão do laudo	18/11/2026 as 00:54

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **tgjogos.com**, realizada em **17/11/2026** 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 domínio redireciona para www.tgjogos.com, cujo título é “TGJOGO - O melhor Site de apostas esportivas e Cassino online”. A aplicação de página única carrega ícone e imagens de `cdn.sssgameimgapi.com`, o mesmo CDN da rede SSSGAME — ou seja, a TGJOGO é uma “skin” (marca) da mesma plataforma.

O primeiro problema é regulatório. Desde a regulamentação das apostas de quota fixa no Brasil, o operador autorizado pelo Ministério da Fazenda opera obrigatoriamente sob domínio `.bet.br`; **tgjogo.bet.br** e **tgjogos.bet.br** não existem (RDAP 404). Nenhum operador é identificado.

O resolvedor DNS do provedor de acesso brasileiro usado na coleta **não retorna endereço** para o domínio, enquanto os resolvedores públicos 1.1.1.1 e 8.8.8.8 retornam normalmente — comportamento compatível com as ordens de bloqueio de sites de apostas não autorizados expedidas pela Anatel a pedido da SPA/MF (a inclusão em lista oficial não foi verificada). O conteúdo foi obtido fixando o IP público obtido via 1.1.1.1.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: marca de apostas da mesma plataforma da rede SSSGAME, operando fora do regime brasileiro e já sem resolução no DNS de provedor brasileiro (Seções 4 e 5).

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	tgjogos.com
Registro	23/05/2023 · expira 23/05/2027 · **1274 dias** antes da coleta
Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)

Registrador	GoDaddy.com, LLC · abuse@godaddy.com
Servidores de nome	finley.ns.cloudflare.com · sandra.ns.cloudflare.com
DNS - A	172.67.192.90 · 104.21.20.108 · sem MX
Hospedagem	AS13335 Cloudflare, Inc. · San Francisco/US
Certificado TLS	Google Trust Services (WE1) · emitido em 17/11/2026 · válido até 15/02/2027
Domínio .bet.br	**tgjogo.bet.br e tgjogos.bet.br não registrados** (Registro.br, RDAP 404)
Resolução DNS	Provedor de acesso brasileiro: **sem resposta** · 1.1.1.1 e 8.8.8.8: resolvem (dns_comparativo_resolvedores.txt)
Ligação com a SSSGAME	Ícones e imagens servidos de `cdn.sssgameimgapi.com` — o CDN de imagens da plataforma SSSGAME

Leitura: domínio de 2023 (GoDaddy) com titular oculto, NS e proxy Cloudflare, certificado Google Trust Services emitido na data da coleta.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Aplicação de página única (`/v1794830719424/client/assets/*`) da mesma família de build da SSSGAME; o conteúdo do lobby é carregado por script.

Aspecto	Constatação
Produto	Apostas esportivas e cassino online
Plataforma	Mesma da SSSGAME (CDN `cdn.sssgameimgapi.com`)
Operador	Não identificado; sem licença, sem CNPJ

Leitura: depósitos e saques ocorrem dentro da aplicação, fora de qualquer supervisão brasileira.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Apostas fora do .bet.br; tgjogo(s).bet.br inexistentes	`rdap_raw.json`	ALTA
2	Sem resolução no DNS de provedor brasileiro (compatível com bloqueio)	`dns_comparativo_resolvedores.txt`	ALTA
3	Mesma plataforma da rede SSSGAME	`corpo_home.html`	MEDIA
4	Operador não identificado	`corpo_home.html`	ALTA

Síntese: quatro indicadores, três de severidade alta.

6. Conclusão Técnica e Recomendações

O tgjogos.com é uma marca de apostas servida pela mesma plataforma da rede SSSGAME, sem operador identificado e fora do `.bet.br`. Classificação técnica: **RISCO ALTO** — oferta de apostas ao público brasileiro fora do regime autorizado, por operador não identificado.

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@godaddy.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 17/11/2026; 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
corpo_home.html (212676 bytes)	77f55f1243189fc70b811a8737a030fa97dbc26d8966f05cc9b0e44b6e8efe40
dns_comparativo_resolvedores.txt (197 bytes)	5fd10deb530c1cd051b5446bce45e8be9f0d3deb02584b67085a36e9ac6acac6
dns_records.txt (362 bytes)	507c0ef48a11f3de7d75a4f6c968ecb747e9a9d2d3b73143cb4f485c86c1902e
geoip.json (288 bytes)	e40a421242ec0ae2c4414b0a89b38f4c4a9d0ad7dfc6a7ed6bae2f85aaa02bae
headers_home.txt (1403 bytes)	d675c270bb77c2459daf9f8aa79fc1aea0003354590df663130a90c6d1ef8fc6
rdap_raw.json (2645 bytes)	344c9364707296578e967556ed079d86831eda26f104e50e02590cceb1e540ba
tls_cert.txt (300 bytes)	6ac7dc61c97c728bf193c1ff890ff0a7552bb74c852504d56b3e0f5922ae99ba

- Fim do relatório -