

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

1win.fyi

Objeto investigado	1win.fyi - portal de divulgação “Play at 1win International”
Natureza	Verificação de vínculo com a marca 1win e do acesso no Brasil
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	Portal que promove cadastro, código promocional e aplicativo da 1win, com versão em português, fora de domínio .bet.br e **bloqueado** no provedor local
Classificação	**RISCO ALTO**
Emissão do laudo	28/11/2026 as 01:05

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **1win.fyi**, 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 `1win.fyi` foi registrado em 17/08/2023 no mesmo registrador usado pela 1win (URL Solutions/Pananames), com titular oculto e atrás da Cloudflare. A página, montada em OpenCart, se apresenta como “Play at 1win International – Bookmaker, Sport betting and Casino” e oferece cadastro, “promo code”, aplicativo e Aviator, em mais de 20 idiomas, entre eles o português.

O portal descreve a 1win como operando “sob licença internacional”, com depósitos em moeda local e criptomoedas, e direciona o contato para um robô no Telegram (`t.me/link_1win_bot`) e um telefone da Índia. O provedor de internet local responde **NXDOMAIN** (domínio inexistente) para `1win.fyi`, enquanto os resolvedores públicos 1.1.1.1 e 8.8.8.8 devolvem o IP normalmente e o mesmo resolvedor local resolve `google.com` — padrão compatível com bloqueio por ordem da Anatel.

Não foi possível determinar se o portal é operado pela própria 1win ou por um afiliado: o domínio não compartilha IP nem aplicação com o 1win.com. Em qualquer caso, ele leva o público ao cassino fora do regime autorizado no Brasil.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: o domínio funciona como porta de entrada para a 1win e já está bloqueado no provedor local.

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	1win.fyi
Registro	17/08/2023 · expira 17/08/2027 · **1199 dias** antes da coleta

Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)
Registrador	URL Solutions, Inc. · abuse@pananames.com
Servidores de nome	dean.ns.cloudflare.com · aryanna.ns.cloudflare.com
DNS - A	172.67.137.143 · 104.21.62.171 · MX: _dc-mx.46ce8d09f09d.1win.fyi
Hospedagem	AS13335 Cloudflare, Inc. · San Francisco/US
Resolvedor local	NXDOMAIN no provedor local; IP normal em 1.1.1.1 e 8.8.8.8
Plataforma	OpenCart (cookie `OCSESSID`, cache `jetcache`)
Contatos da página	`t.me/link_1win_bot` · telefone `+91 79016 56971` (Índia)

Leitura: domínio de 2023 com titular oculto, mesmo registrador da marca, atrás da Cloudflare.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Loja OpenCart adaptada como página institucional de divulgação, sem checkout próprio.

Aspecto	Constatação
Conteúdo	Cadastro, código promocional, aplicativo e jogos da 1win
Idiomas	Mais de 20, inclusive português
Contato	Robô no Telegram e telefone da Índia
Acesso no Brasil	NXDOMAIN no provedor local

Leitura: o portal promove um operador sem autorização brasileira e já é alvo de bloqueio.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Promoção da 1win ao público de língua portuguesa fora de domínio .bet.br	`corpo_home_resolve.html`	ALTA
2	Domínio não resolve no provedor local (padrão de bloqueio)	`resolvedores.txt`	ALTA
3	Contato só por robô de Telegram e telefone estrangeiro	`corpo_home_resolve.html`	MEDIA
4	Titular oculto	`rdap_raw.json`	BAIXA

Síntese: quatro indicadores, dois de severidade alta.

6. Conclusão Técnica e Recomendações

O 1win.fyi é um portal de divulgação da 1win, com versão em português, fora do regime autorizado no Brasil e bloqueado no provedor local. Classificação técnica: **RISCO ALTO**.

Recomendações ao consumidor / solicitante

- Não deposite em endereços alternativos (“espelhos”) de uma casa de apostas: eles existem justamente para manter o acesso depois que o domínio principal é bloqueado no Brasil.
- 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@pananames.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 (210 bytes)	724d1344c1292e6037928901e9c00b0f666c69cbd1101d5311128a9e0d19fbed
corpo_home.html (0 bytes)	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
corpo_home_resolve.html (37843 bytes)	f8073c87c883f69f607e1f065dbb78ff0119159be8b77f0704be0b50138ca8e8
dns_records.txt (440 bytes)	3598d8420bd9bd83d46c1ba01237b8fb88a5e8d6e73c62071a43f028559135d8
geoip.json (289 bytes)	ee2e6b6a22c784435c4622b44e46930c0a754ddc95f58bb5605089d448301764
headers_home.txt (0 bytes)	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
headers_home_resolve.txt (1184 bytes)	0c8aca7a3f4daa4dc43caecaa0378335a47d6e1725e3b98142e5ce743423ea7a
rdap_raw.json (7634 bytes)	613fa286ad2b8a239d45c31b9219171c0f0d6c3be65e7a8c073043ab7781cd75
resolvedores.txt (439 bytes)	b74fd547ffaf207ee0681b025d249b77825dd2a9dadd260bbaa8cd67fc2724a1
tls_cert.txt (67 bytes)	fd4601dcf3b285b522c6d9ff265c3abdaa04536ae1abbe191f0a02a66956b40a

- Fim do relatório -