RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

betdacopa.bet

Objeto investigado	betdacopa.bet — plataforma de cassino e apostas esportivas (gTLD .bet)
Natureza	Verificação de legitimidade, autorização e risco ao consumidor
Data da coleta	10/07/2026 (RDAP, DNS, HTTP/TLS, geolocalização, análise do app e do PIX)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise de conteúdo, do app e do BR Code PIX
Achado central	"Bet" sem autorização brasileira; PIX recebido por HUB/agregador, não pelo operador
Classificação	**RISCO ALTO**
Emissão do laudo	11/07/2026 às 00:14

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **betdacopa.bet**, realizada em **10/07/2026** 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 uma **plataforma de cassino online e apostas esportivas em português** (título "BETDACOPA — Plataforma de cassino e apostas esportivas"), construída como aplicação **Next.js** servida atrás da **Cloudflare**. A marca real exibida no produto é **"Meta"** (logotipo `logometa.png`, Instagram `@meta.igaming`) — betdacopa.bet é um **rótulo/skin** dessa plataforma. O front-end consome APIs próprias (`/api/…`) com cadastro, carteira e **depósito via PIX** (`/api/payments/deposit`). O cadastro coleta **CPF, RG, nome completo, e-mail, telefone/WhatsApp, data de nascimento, senha** e **chave PIX** para saque.

O único responsável indicado no rodapé é uma empresa **offshore**: "Meta é operado pela **Enigma Digital Solutions Limitada**, Registro 3102916990, Ofident Building, San Jose, **Costa Rica**, licenciado e regulamentado pelo **Governo da Ilha Autônoma de Anjouan (Comores)**". Não há **CNPJ brasileiro**, razão social nacional nem **autorização federal**: a licença de Anjouan é um selo **estrangeiro** sem validade no Brasil, e o domínio é **.bet** genérico — não o padrão **.bet.br** exigido das casas autorizadas.

O código PIX de pagamento fornecido foi decodificado (BR Code/EMV, **CRC16 válido**). O **recebedor** não é a "betdacopa"/"Meta", e sim **"HUB PAGAMENTO E RECEBIMENTO"** — um **agregador de pagamentos** genérico (cidade Passo Fundo/RS), com o payload dinâmico intermediado por `pix.onlyup.com.br`. Ou seja, o dinheiro do apostador entra em uma **conta de intermediação**, ocultando o beneficiário final e desvinculando o pagamento da marca anunciada.

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 **.bet** genérico, invoca apenas licença estrangeira (Anjouan) e tem como público-alvo o Brasil (pt-BR, BRL, coleta de CPF, 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 sensíveis (CPF, RG, senha, chave PIX) **sem operador brasileiro identificável e sem autorização**, e cujo pagamento é desviado para um **agregador de intermediação** em vez da própria marca, 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 5 e 6).

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 (DNS-over-HTTPS); o conteúdo HTTPS e os bundles JavaScript foram obtidos por requisição de visitante comum; o certificado TLS foi lido via `openssl s_client`; e o código PIX "copia e cola" fornecido foi decodificado pelo padrão EMV/BR Code (TLV), com validação de CRC16. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (Identity Digital / .bet — registrador GoDaddy)	`rdap_raw.json`

DNS	DoH 1.1.1.1 (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_a.json`
Conteúdo / cabeçalhos	HTTP/1.1 sobre TLS (visitante comum)	`corpo.html · headers_https.txt`
Aplicação (front-end)	Download dos bundles JS (Next.js) do site	`js/ (31 chunks)`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io	`(registrado no laudo)`
Intermediário PIX	RDAP + DNS (onlyup.com.br / pix.onlyup.com.br)	`rdap_onlyup.json`
Código PIX (BR Code)	Decodificação EMV/TLV + validação CRC16	`pix_copiaecola.txt`

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

Domínio	betdacopa.bet (gTLD .bet — Identity Digital)
Registro	**08/05/2026** · expira 08/05/2027 (validade de 1 ano)
Idade na coleta	**~2 meses** — domínio recente
Titular	**Oculto** (RDAP expõe apenas o registrador)
Registrador	GoDaddy.com, LLC
Status	clientDelete/Renew/Transfer/UpdateProhibited
Servidores de nome	elmo / bethany.ns.cloudflare.com (Cloudflare)
DNS — A	172.67.157.243 · 104.21.74.118 (Cloudflare) · AAAA presente · sem MX · sem TXT/SPF
www	aponta para os mesmos IPs Cloudflare
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 / stack	Server: cloudflare · **X-Powered-By: Next.js** (X-Nextjs-Cache HIT) · edge CF-RAY …-GRU (São Paulo)
Certificado TLS	CN=betdacopa.bet · emissor Let's Encrypt YE2 (DV) · válido 09/07/2026–07/10/2026
Série / Fingerprint	0590C3B987B3C7D81832177E30D328C1F7BC · SHA-256 E1:F4:61:AE:83:DC:83:C8:31:3D:E8:65:91:AE:00:BA…

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 armazena dados e processa pagamentos; os cabeçalhos revelam apenas que a aplicação é **Next.js** servida pela borda da Cloudflare em São Paulo (GRU). O certificado DV gratuito (Let's Encrypt) comprova apenas o controle do domínio, **não a identidade de qualquer empresa**. Não se imputa conduta ao registrador (GoDaddy) nem à Cloudflare, meros intermediários de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site entrega uma **plataforma de cassino online e apostas esportivas** em português (pt-BR), construída em **Next.js** atrás da Cloudflare. A marca do produto é **"Meta"** (logotipo `logometa.png`; Instagram `@meta.igaming`), da qual **betdacopa.bet** é um rótulo. A lógica é servida por **APIs próprias** (`/api/…`: autenticação, carteira, jogos, cupons, notificações e **pagamentos**). O **depósito é feito por PIX** (`POST /api/payments/deposit`), que gera um BR Code dinâmico intermediado por `pix.onlyup.com.br`. O site embute rastreadores de marketing (Google Tag Manager, **Meta Pixel**), atendimento por **WhatsApp (DigiSac)** e uma biblioteca **anti-inspeção** (`disable-devtool`).

Aspecto	Constatação
Tipo de serviço	Cassino online + apostas esportivas (plataforma "Meta"; skin "BETDACOPA")
Tecnologia	SPA Next.js atrás de Cloudflare · APIs próprias /api/… · GTM + Meta Pixel · WhatsApp DigiSac · anti-devtool
Meio de pagamento	Depósito via PIX — POST /api/payments/deposit (BR Code dinâmico)
Intermediário (gateway)	**onlyup.com.br** (pix.onlyup.com.br → onlyup-prod.onz.software, AWS São Paulo) — registrante Bruno Marin Mota, CNPJ 45.299.812/0001-18, contato bm_mota@hotmail.com
Recebedor do PIX	**"HUB PAGAMENTO E RECEBIMENTO"** (Passo Fundo/RS) — agregador genérico, **não** a marca "betdacopa"/"Meta"
Dados pessoais coletados	CPF, RG, nome completo, e-mail, telefone/WhatsApp, data de nascimento, senha e chave PIX (saque)
Identificação do operador	**Offshore, sem CNPJ BR** — "Enigma Digital Solutions Limitada", Reg. 3102916990, San Jose/Costa Rica
Autorização / licença	**Ausente no Brasil** — invoca apenas licença de **Anjouan (Comores)**; sem selo SPA/SIGAP
Domínio	.bet (genérico) — **não** o padrão .bet.br exigido das casas autorizadas no Brasil
Contato divulgado	Atendimento por WhatsApp (DigiSac) e Instagram · sem canal corporativo verificável

Leitura técnica. O fluxo financeiro é real e operante: o BR Code fornecido tem **CRC16 válido** e paga um recebedor cujo nome é o de um **agregador de pagamentos** ("HUB PAGAMENTO E RECEBIMENTO"), e não o da casa de apostas anunciada. Esse arranjo — depósito do apostador → conta de intermediação → beneficiário final oculto — **desvincula o dinheiro da marca** e dificulta o rastreio de quem efetivamente recebe. O **risco não está na tecnologia** (Cloudflare, Next.js, o intermediário Onz/onlyup são infraestrutura), mas na **ausência de operador brasileiro identificável, na ausência de autorização e na coleta de PII sensível** (CPF, RG, chave PIX) por uma estrutura offshore. Não se imputa conduta ilícita aos provedores de infraestrutura e de pagamento citados; descreve-se o fato e separa-se inferência de prova.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	"Bet"/cassino sem autorização federal brasileira (SPA/SIGAP); em .bet, não .bet.br	`corpo.html · RDAP`	ALTA
2	Operador apenas offshore (Costa Rica/Anjouan), sem CNPJ nem razão social brasileira	`corpo.html (rodapé)`	ALTA
3	Recebedor do PIX é agregador ("HUB PAGAMENTO E RECEBIMENTO"), não a marca anunciada	`pix_copiaecola.txt`	ALTA
4	Coleta CPF, RG, senha e chave PIX sem responsável brasileiro localizável	`js/ · corpo.html`	ALTA

5	Pagamento roteado por conta de intermediação, ocultando o beneficiário final	`pix_copiaecola.txt` · `rdap_onlyup.json`	MÉDIA
6	Origem mascarada por Cloudflare (IP do servidor real oculto)	`headers_https.txt` · `dns_a.json`	MÉDIA
7	Domínio recém-registrado (~2 meses), validade de 1 ano, titular oculto	`RDAP — 08/05/2026`	MÉDIA
8	Marca do produto ("Meta") diverge do domínio ("betdacopa"): plataforma replicável/skin	`corpo.html` · `logometa.png`	MÉDIA
9	Biblioteca anti-inspeção (disable-devtool) para dificultar análise	`js/`	BAIXA
10	Intermediário PIX com contato em e-mail gratuito (Hotmail)	`rdap_onlyup.json`	BAIXA

Síntese: 4 indicadores de severidade ALTA, 4 MÉDIA e 2 BAIXA. **Nenhum fator de legitimidade** (operador brasileiro identificado, autorização SPA/SIGAP, recebedor PIX coincidente com a marca, contato corporativo verificável) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 10/07/2026, conclui-se que **betdacopa.bet** é uma **plataforma de cassino e apostas esportivas em operação**, voltada ao público brasileiro (pt-BR, BRL, CPF, PIX), que recebe depósitos via PIX e coleta dados pessoais e bancários sensíveis, porém **sem operador brasileiro identificável** (apenas uma empresa offshore em Costa Rica/Anjouan) e **sem qualquer autorização** para explorar jogos de azar/apostas no Brasil — usando **.bet** em vez do padrão regulado **.bet.br**, com a origem mascarada por Cloudflare. O código PIX fornecido, com CRC16 válido, paga um **agregador de intermediação** ("HUB PAGAMENTO E RECEBIMENTO", via onlyup.com.br) e não a marca anunciada, ocultando o beneficiário final. Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não se cadastrar, não depositar e não fornecer CPF, RG, senha, chave PIX ou dados pessoais** ao site.
- Desconfiar de anúncios e mensagens (Instagram, WhatsApp, Telegram, SMS) que conduzam a `betdacopa.bet`/"Meta" ou prometam bônus/ganhos fáceis.
- Se já houve depósito: acionar o banco e o mecanismo **MED** do PIX, reunir comprovantes (incluindo o código PIX e o recebedor "HUB PAGAMENTO E RECEBIMENTO") 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 apostas/cassino sem autorização, e reportar aos canais de *abuse* do registrador (GoDaddy) e da Cloudflare, anexando este laudo.
- Reportar o recebedor PIX ao **intermediário** (onlyup.com.br / infraestrutura Onz) e ao **banco/PSP** do beneficiário, e comunicar o **Banco Central** (canal de PIX) sobre o uso da conta de agregação para receber depósitos de plataforma de apostas não autorizada.
- Preservar este relatório e as evidências (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 e de pagamento citados.

— Fim do relatório —

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