RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

betdacopa.com

Objeto investigado	betdacopa.com — "Bet na Copa": apostas esportivas e cassino online (gTLD .com)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	21/06/2026 (RDAP, DNS, HTTP/TLS, geolocalização, análise da aplicação)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise de bundles JS · decodificação do PIX (checkout)
Achado central	Casa de apostas SEM autorização; recebedor do PIX ("Legacy Gaming BR Ltda") oculto no site
Classificação	**RISCO ALTO**
Emissão do laudo	21/06/2026 às 01:27

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **betdacopa.com**, realizada em **21/06/2026** 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 (cadeia de custódia, Seção 2).

O domínio **está no ar** e entrega uma plataforma de **apostas esportivas e cassino online** em português, intitulada **"Bet na Copa"** ("Apostas Esportivas e Cassino ao Vivo" — esportes, cassino ao vivo, "crash games" e "slots"). Tecnicamente é uma aplicação de página única (SPA React/Vite) **gerada pelo construtor de aplicativos por IA "Lovable"**, hospedada na **Vercel** e apoiada em um **backend BaaS Supabase** (projeto `xruclgoqzaxwvclaaodf`). O fluxo financeiro usa **PIX** para depósito e saque (funções de borda `pix-deposit` / `pix-reconcile`, provedor interno identificado como "novus"), com bônus de boas-vindas de até R$1.000 no primeiro depósito e um **programa de afiliados** (CPA/RevShare). O cadastro coleta **nome, CPF, RG, e-mail, telefone e senha**, além de **dados bancários/chave PIX** para saque.

O conjunto de sinais é o de uma operação **opaca e sem lastro verificável**: domínio **recém-registrado** (22/04/2026, ~2 meses), **titular oculto**, e — no próprio site — **nenhuma identificação do operador** (sem CNPJ, razão social ou endereço), **nenhum selo de autorização regulatória brasileira** e contato restrito a canais internos de suporte. A imagem de compartilhamento social (og:image) declarada pelo site pertence, na verdade, a **outra marca ("Apostas Online 365")** e o rodapé exibe "© 2024" — indícios de **plataforma de template/white-label reaproveitada** sem ajuste dos textos de modelo.

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 **.com** genérico, **não apresenta qualquer indício de autorização** e tem como público-alvo declarado o Brasil (idioma pt-BR, moeda BRL, coleta de CPF, PIX) — perfil compatível com **operação irregular/não autorizada**, categoria sujeita a bloqueio pelas autoridades brasileiras. O nome "Bet na Copa" explora ainda o apelo do período de Copa do Mundo de 2026.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: uma plataforma que recebe dinheiro (PIX) e dados sensíveis (CPF, RG, senha, dados bancários) **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** (Seção 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; o conteúdo HTTP/HTTPS, os cabeçalhos e os pacotes JavaScript (bundles) da aplicação foram coletados por requisição de visitante comum (HTTPS) e analisados localmente. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (Verisign / .com — registrador GoDaddy)	`rdap_raw.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS (porta 443) e porta 80	`corpo.html` · `headers_https.txt` · `headers_http80.txt`

Checkout PIX	Decodificação EMV/BR Code (TLV) + RDAP/DNS do PSP	`pix_copia_cola.txt · rdap_mtbank.json · dns_mtbank.txt`
Aplicação (front-end)	Download dos bundles JS (Vite)	`app_index.js · app_deposit.js · app_register.js · app_affiliates.js · app_supabase.js · notas_app.txt`
Certificado TLS	openssl s_client / x509	`ssl_cert.txt · ssl_raw.txt`
Geolocalização do IP	ipinfo.io · ip-api.com	`ipinfo_129.json · ipapi_129.json`
Imagens / metadados	Download de assets · exiftool	`imagens/ · metadata_exiftool.txt`
Integridade	sha256sum de todos os artefatos	`hash_manifest.txt`

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

Domínio	betdacopa.com (gTLD .com — Verisign)
Registro	**22/04/2026** · expira 22/04/2027 (validade de 1 ano) · alteração em 30/05/2026
Idade na coleta	**~2 meses** — domínio recente
Titular	**Oculto** (privacidade; RDAP expõe só o registrador)
Registrador	GoDaddy.com, LLC
Status	active
Servidores de nome	ns1 / ns2.vercel-dns.com (Vercel / NS1)
DNS — A	216.150.1.129 · 216.150.16.193 (Vercel — anycast) · sem AAAA · sem MX · sem TXT/SPF
www	aponta para os mesmos IPs Vercel
Hospedagem	Vercel (plataforma serverless) — Server: Vercel; entrega pela borda gru1 (São Paulo) · IP anunciado em AS16509 Amazon
Geolocalização do IP	Anycast (ipinfo reporta Walnut/CA como ponto de presença — não revela a localização real do app)
Backend de aplicação	BaaS Supabase — `xruclgoqzaxwvclaaodf.supabase.co` (banco, autenticação e funções de borda)
Construtor / stack	SPA React/Vite gerada por **Lovable** (app builder por IA); assets de imagem em Cloudflare R2
Servidor web	Server: Vercel · porta 80 → 308 HTTPS
Certificado TLS	CN=*.betdacopa.com (wildcard) · emissor Let's Encrypt YR1 (DV) · válido 30/05/2026–28/08/2026
Série / Fingerprint	05F0074CAF3BB1802103C7488A95996F4479 · SHA-256 28:7C:9B:40:6E:89:6B:C0:EE:16:AE:5B:DE:3D:38:0E…

Leitura técnica. Registro recente, validade de 1 ano e titular oculto compõem um perfil de **baixa rastreabilidade do responsável**. A escolha de uma stack "no-code/low-code" (Lovable + Vercel + Supabase) permite colocar uma casa de apostas no ar **com rapidez e sem revelar a identidade do operador**; a infraestrutura serverless não expõe um servidor de origem nominal. O certificado DV wildcard gratuito (Let's Encrypt) comprova apenas o controle do domínio, **não a identidade de qualquer empresa**. Não se imputa conduta ao registrador (GoDaddy), à Vercel, à Supabase, à Cloudflare nem à Amazon (AWS), meros intermediários de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site entrega uma **casa de apostas esportivas com cassino online** em português (pt-BR), com seções de esportes (futebol), cassino ao vivo, "crash games" e "slots", bônus de boas-vindas de até R$1.000 e captação por tráfego pago (Google Tag Manager e verificação de domínio do Facebook/Meta presentes no HTML). A lógica de negócio roda sobre **Supabase** (tabelas como `players`, `transactions`, `bets`, `user_roles`), e o PIX é processado por **funções de borda** (`pix-deposit` e `pix-reconcile`), que retornam o **"Pix Copia e Cola"** e o QR Code ao usuário; o provedor de pagamento referenciado internamente é "novus". Há ainda área administrativa e portal de afiliados.

Aspecto	Constatação
Tipo de serviço	Apostas esportivas + cassino ao vivo, crash games e slots ("Bet na Copa")
Tecnologia	SPA React/Vite gerada por Lovable · hospedagem Vercel · backend Supabase (BaaS) · imagens Cloudflare R2
Meio de pagamento	Depósito e saque via PIX (funções pix-deposit / pix-reconcile; retorna Pix Copia e Cola + QR)
Intermediário (gateway)	No checkout, PIX intermediado por **MT Instituição de Pagamento S.A.** (qrcode.mtbank.com.br); no código, provedor referenciado como "novus" — ver Seção 5
Recebedor do PIX	**LEGACY GAMING BR LTDA** (Cuité/PB) — **não divulgado no site** e distinto da marca "Bet na Copa" (ver Seção 5)
Dados pessoais coletados	Nome completo, CPF, RG, e-mail, telefone e senha; dados bancários/conta e chave PIX para saque
Identificação do operador	**Ausente** — sem CNPJ, razão social ou endereço no site
Autorização / licença	**Ausente** — sem selo SPA/SIGAP; apenas menção genérica a "Jogo Responsável" e "18+"
Domínio	.com (genérico) — **não** o padrão .bet.br exigido das casas autorizadas no Brasil
Indício de white-label	og:image pertence a outra marca ("Apostas Online 365"); rodapé "© 2024" — template reaproveitado sem ajuste
Afiliados / captação	Portal de afiliados com CPA/RevShare; GTM + verificação de domínio Facebook (tráfego pago)

Leitura técnica. O fluxo financeiro é real e operante: o usuário deposita por PIX e fornece CPF, RG, senha e dados bancários. 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 (app gerado por IA + hospedagem serverless + BaaS + og:image de outra marca) é típica de **plataformas de apostas replicadas em escala**, criadas rapidamente e descartáveis. Caso seja fornecida captura da tela de pagamento (pasta `pix/`), o laudo pode ser complementado com a decodificação do BR Code (EMV) e a checagem do recebedor PIX.
Imagens. Os assets baixados (favicon 256×256; og:image 1920×1080 PNG) **não contêm metadados EXIF/GPS/autor** — coerente com material de template. A og:image declarada exibe o layout de marca distinta ("Apostas Online 365"), reforçando o reaproveitamento de modelo. Ver `imagens/metadata_exiftool.txt`.

5. Recebedor do PIX (decodificação do checkout)

O solicitante forneceu o código **"PIX Copia e Cola"** exibido na tela de pagamento da plataforma. Ele foi decodificado pelo padrão **EMV / BR Code (TLV)** e seu dígito verificador **CRC16 foi conferido e está íntegro**, o que confirma a autenticidade estrutural do código. Trata-se de um **QR dinâmico de cobrança** (ponto de iniciação 12). A decodificação revela o beneficiário e o prestador de serviço de pagamento (PSP):

Tipo	BR Code EMV · QR PIX **dinâmico** (cobrança) · CRC16 **A749 verificado**
GUI	br.gov.bcb.pix

URL de cobrança (PSP)	`qrcode.mtbank.com.br/spi/qr-code/cob/03ad18cf16824b10a856dbdf913421d0`
Recebedor (campo 59)	**LEGACY GAMING BR LTDA**
Cidade / CEP (60/61)	Cuité — PB · 58175-000
Moeda / País (53/58)	BRL (986) · BR
Identificador (txid)	*** (genérico — gerado por cobrança)
Intermediário (PSP)	**MT INSTITUIÇÃO DE PAGAMENTO S.A.** · CNPJ 50.871.921/0001-06 (RDAP registro.br · domínio desde 08/11/2023) · infraestrutura AWS São Paulo

Leitura técnica. O dinheiro depositado pelo apostador é direcionado a **"LEGACY GAMING BR LTDA"** (Cuité/PB) — entidade que **não é divulgada em nenhum ponto do site** e que **difere da marca anunciada** ("Bet na Copa"). Esse é o primeiro elemento que permite tentar identificar o operador por trás da plataforma: recomenda-se verificar o nome/CNPJ junto à **Receita Federal** e cruzá-lo com a lista de empresas **autorizadas pela SPA/Ministério da Fazenda**. A cobrança é intermediada pela **MT Instituição de Pagamento S.A.** (PSP regulado, via `qrcode.mtbank.com.br`); **não se imputa conduta a esse intermediário de pagamento** — descreve-se apenas o fato técnico. A divergência entre a marca exibida e o recebedor real, somada à omissão dessa identificação no próprio site, **reforça a opacidade** já apontada.

6. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Apostas/cassino sem identificação do operador (CNPJ/razão social/endereço)	`corpo.html` · `app_index.js`	ALTA
2	Sem indício de autorização federal (SPA/SIGAP); em .com, não .bet.br	`app_index.js` · `RDAP`	ALTA
3	Recebe PIX e coleta CPF/RG/senha/dados bancários sem responsável localizável	`app_register.js` · `app_deposit.js`	ALTA
4	Recebedor do PIX ("Legacy Gaming BR Ltda") oculto no site e distinto da marca anunciada	`pix_copia_cola.txt`	ALTA
5	Plataforma white-label reaproveitada (og:image de "Apostas Online 365"; rodapé © 2024)	`corpo.html` · `og_image.png`	MÉDIA
6	Domínio recém-registrado (~2 meses), validade de 1 ano	`RDAP — 22/04/2026`	MÉDIA
7	Titular oculto (privacidade de registro)	`RDAP — só registrador`	MÉDIA
8	Branding oportunista vinculado à Copa do Mundo ("Bet na Copa")	`corpo.html`	MÉDIA
9	Programa de afiliados (CPA/RevShare) + captação por tráfego pago (Meta/GTM)	`app_affiliates.js` · `corpo.html`	MÉDIA
10	Bônus agressivo (R$1.000) como isca de cadastro/depósito	`og_image.png` · `app_deposit.js`	BAIXA
11	Sem e-mail próprio (sem MX/TXT); identidade restrita a canais internos	`dns_records.txt` · `app_index.js`	BAIXA

Síntese: 4 indicadores de severidade ALTA, 5 MÉDIA e 2 BAIXA. **Nenhum fator de legitimidade** (operador identificado, autorização brasileira, contato corporativo, histórico) foi constatado.

7. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 21/06/2026, conclui-se que **betdacopa.com** ("Bet na Copa") é uma **casa de apostas esportivas com cassino online em operação**, voltada ao público brasileiro (pt-BR, BRL, CPF, PIX), que recebe depósitos via PIX e coleta dados pessoais e bancários, porém **sem identificar no próprio site quem a opera** e **sem qualquer indício de autorização** para explorar jogos de

azar/apostas no Brasil — usando domínio **.com** em vez do padrão regulado **.bet.br**, sobre uma stack serverless (Lovable/Vercel/Supabase) e com indícios claros de **template/white-label reaproveitado** (og:image de outra marca, rodapé "© 2024"). A decodificação do PIX do checkout revela que os depósitos são direcionados a **"LEGACY GAMING BR LTDA" (Cuité/PB)**, entidade ausente do site e distinta da marca anunciada, intermediada pela MT Instituição de Pagamento S.A. Soma-se a isso o registro recente, o titular oculto e o branding oportunista de Copa do Mundo. Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não se cadastrar, não depositar e não fornecer CPF, RG, senha, dados bancários ou pessoais** ao site.
- Desconfiar de anúncios e mensagens (Instagram, Facebook, WhatsApp, Telegram, SMS) que conduzam a `betdacopa.com` 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 casa de apostas/cassino sem autorização, e reportar aos canais de abuse do registrador (GoDaddy), da Vercel, da Supabase e da Cloudflare, anexando este laudo.
- Verificar o recebedor do PIX **"LEGACY GAMING BR LTDA" (Cuité/PB)** na Receita Federal e cruzar com a lista de casas autorizadas pela SPA; em caso de não pagamento de saque, o nome do beneficiário e o PSP (MT Instituição de Pagamento S.A.) são elementos úteis para reclamação ao banco/Bacen e eventual ação.
- Preservar este relatório e as evidências (pasta `evidencias/`, 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 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.