

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

dudugames.pro

Objeto investigado	dudugames.pro - loja de jogos digitais e assinaturas Xbox/PlayStation, pagamento via Pix
Natureza	Verificação de legitimidade da loja e do fluxo de pagamento
Data da coleta	23/11/2026 (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	Loja de 45 dias que vende jogos com **86% a 92% de desconto** (Elden Ring, Silent Hill 2 por R$ 27,90) e envia o comprador a um checkout em **checkout-cakto.site**, domínio parecido com o de uma plataforma real, mas que não pertence a ela
Classificação	**RISCO ALTO**
Emissão do laudo	23/11/2026 as 02:19

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **dudugames.pro**, realizada em **23/11/2026** 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).

A “DUDU GAMES — a maior loja de games da América Latina” vende jogos de Xbox e PlayStation, cartões-presente e assinaturas Game Pass Ultimate e PS Plus Deluxe com “entrega automática” e pagamento “à vista no PIX”. Os preços são incompatíveis com códigos originais: Elden Ring, Hogwarts Legacy, Black Myth: Wukong, Silent Hill 2 e Resident Evil 4 por **R$ 27,90**; EA Sports FC 27 por R$ 47,90; cartão-presente Xbox de R$ 100 por R$ 60; Game Pass a partir de R$ 17,90.

O botão “Comprar” leva a `www.checkout-cakto.site/checkout/…`, que cobra o valor por Pix com “taxa de serviço”. Esse domínio foi registrado em 11/09/2026 com titular oculto e roda na Vercel; o nome imita a plataforma de checkout Cakto, que opera em cakto.com.br — **não há relação técnica demonstrada** entre ele e a plataforma.

A página exibe o selo “RA1000” do Reclame Aqui e a meta-descrição “Loja sem reclamações”, não informa CNPJ e executa um script “shield” (`/api/shield/verify`) que envia tempo de carregamento e dados de tela do visitante — técnica usada para distinguir robôs de pessoas.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: descontos de quase 90% em lançamentos, checkout em domínio que imita uma plataforma conhecida, selo de reputação sem verificação e nenhuma identificação compõem o padrão de loja falsa de games (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	dudugames.pro

Registro	09/10/2026 · expira 09/10/2027 · **45 dias** antes da coleta
Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)
Registrador	GoDaddy.com, LLC · abuse@godaddy.com
Servidores de nome	ns41.domaincontrol.com · ns42.domaincontrol.com
DNS - A	216.198.79.1 · sem MX
Hospedagem	AS16509 Amazon.com, Inc. · Walnut/US · cabeçalho `server: Vercel`
Certificado TLS	Let's Encrypt (YR2) · emitido em 09/10/2026 · válido até 07/01/2027
Domínio do checkout	`checkout-cakto.site` · registrado em 11/09/2026 (GoDaddy, titular oculto) · hospedado na Vercel · **não é domínio da plataforma Cakto**, que opera em cakto.com.br
CNPJ	**Nenhum** exibido

Leitura: domínio de 45 dias com titular oculto (GoDaddy), DNS GoDaddy, sem MX; aplicação gerada no v0 e hospedada na Vercel.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Aplicação Next.js gerada no v0 (Vercel). Os links de compra são fixos no código e apontam para páginas de checkout em `checkout-cakto.site` (outra aplicação na Vercel, com rota `/api/open`); nenhum pedido foi gerado.

Aspecto	Constatação
Pagamento	Pix em checkout externo (checkout-cakto.site), com “taxa de serviço” de R$ 0,99
Preços	Lançamentos de R$ 249,90-349,90 por R$ 27,90-47,90 (86%-92% de desconto)
Selos	“RA1000” do Reclame Aqui; “Loja sem reclamações”
Identidade	Sem CNPJ, sem razão social, suporte só por WhatsApp

Leitura: o recebedor do Pix só aparece no momento do pagamento; nada no site identifica a quem o dinheiro se destina.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Descontos de 86%-92% em jogos lançados	`corpo_home.html`	ALTA
2	Checkout em domínio que imita plataforma real, sem vínculo demonstrado	`bundle_next_all.txt` · `rdap_checkout-cakto.site.json`	ALTA
3	Nenhum CNPJ ou razão social	`corpo_home.html`	ALTA
4	Selo RA1000 e “Loja sem reclamações” sem verificação	`corpo_home.html`	MEDIA
5	Script de detecção de robôs antes da navegação	`bundle_next_all.txt`	MEDIA
6	Domínio de 45 dias, titular oculto	`rdap_raw.json`	MEDIA

Síntese: seis indicadores, três de severidade alta.

6. Conclusão Técnica e Recomendações

A dudugames.pro vende jogos a preços impossíveis para códigos originais, sem identificar o vendedor, e cobra por Pix num checkout hospedado em domínio que imita uma plataforma real. Classificação técnica: **RISCO ALTO**.

Recomendações ao consumidor / solicitante

- Compre jogos digitais nas lojas oficiais (Microsoft Store, PlayStation Store) ou em revendedores conhecidos; jogo recém-lançado por R$ 27,90 não é código original.
- Confira o endereço do checkout: a plataforma Cakto opera em cakto.com.br, não em “checkout-cakto.site”.
- Desconfie de preços muito abaixo do mercado combinados com desconto extra para pagamento via Pix.
- Antes de comprar, confira o CNPJ na Receita Federal e se o domínio do site pertence de fato à empresa (consulta RDAP / Registro.br).
- Prefira cartão de crédito, que permite contestação (chargeback); o Pix é instantâneo e de difícil reversão.

Recomendações de mitigação / denúncia

- Reportar o endereço ao Google Safe Browsing e ao canal de abuso do registrador (abuse@godaddy.com).
- 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 23/11/2026; 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
bundle_next_all.txt (638222 bytes)	70e806b1f0e36a5b572174379abaca76047142f835c32fafd5aebb93a3b84115
corpo_checkout-cakto_pedido-confirmado.html (36469 bytes)	fc4b1c9c1a63f53e5f98443c50297169d3df26442afbc35482d69d15ca8a1401
corpo_home.html (161656 bytes)	0b6527fc96b774331097d40b88b57cd1748584763b8b602cffac95987bc1c689
dns_records.txt (334 bytes)	3ffb332f0c0bb6f82e51bb2182c31b153a9e9fef2f58f3e9a68a4fe4674ab5c8
geoip.json (280 bytes)	7e7bc0a546d9f06cdb5d19007f318d02373b355b38ef392434df2ab37340c98b
hash_manifest.txt.n (510 bytes)	bcd84cb2ae98efd2f0f3137ee95e52eff88e0ea91df2fac53e6f7d3559cfff3b
headers_checkout-cakto.txt (1148 bytes)	257e5372dfd9697647f8e9ca691808fac89f3d849e89a94cdd5081035a6df298
headers_home.txt (1086 bytes)	8d8c27bd0fff2e6e3bb62552d241f19d1b39cd7122bf0612cf6a850920b385f8
rdap_checkout-cakto.site.json (5197 bytes)	c109aaec07838c4f5abf08604a55f7f687ccd5a1582b3218271c89a356a9ab97
rdap_raw.json (7670 bytes)	38e342720cb0ee5b44016a909e9e45686a80c77f0aa6761da8c545d0570f2004
tls_cert.txt (298 bytes)	90e34d0094775978f76eaf79e4182a9e6a158fc16c7771a00c6925131f9f055a

- Fim do relatório -