RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

snowsland.com

Objeto investigado	snowsland.com — site de venda de ingressos imitando o parque "Snowland Gramado" (gTLD .com)
Natureza	Verificação de legitimidade, autenticidade da marca e risco ao consumidor
Data da coleta	26/06/2026 (RDAP, DNS, HTTP/TLS, geolocalização, análise do app e do checkout PIX)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise de conteúdo, JS e decodificação do BR Code (PIX)
Achado central	Clone/typosquat de marca real ("Snowland Gramado") com pagamento PIX a beneficiário não relacionado
Classificação	**RISCO ALTO**
Emissão do laudo	26/06/2026 às 02:42

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **snowsland.com**, realizada em **26/06/2026** 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).

O domínio **está no ar** e hospeda um site de **venda de ingressos** que se apresenta como o parque **"Snowland Gramado"** — atração de neve indoor real, localizada em Gramado/RS e operada pelo grupo **Gramado Parks**. O site copia identidade visual, textos, endereço, telefone 0800, e-mails `@gramadoparks.com` e links de redes sociais **oficiais** do parque verdadeiro, mas usa um domínio **distinto e propositalmente parecido** (`snowsland.com`, com um "s" a mais; o site oficial é `snowlandgramado.com.br`). O checkout coleta **nome, CPF, e-mail, WhatsApp e data de nascimento** e direciona o pagamento para **PIX**, gerado por uma API própria (`/api/checkout.php`) através do intermediário `pix.basspago.com.br`.

O ponto decisivo está no **recebedor do PIX**. O código "copia e cola" fornecido decodifica para o beneficiário **"DIGITAL_MARKETPLACE_LTDA"**, em **SÃO PAULO** — que **não corresponde** ao parque anunciado (Snowland / Gramado Parks, Gramado/RS). Somam-se a isso: domínio **recém-registrado** (24/05/2026), titular oculto, **hospedagem no Cazaquistão** (incompatível com uma atração turística gaúcha), ativos gráficos da marca servidos de um **CDN de terceiro** (`jhrcdn.site`) e um **roteiro de checkout manipulativo** que simula "instabilidade no cartão" para empurrar o cliente ao PIX com falso desconto. O conjunto caracteriza um **site fraudulento de venda de ingressos falsos por usurpação de marca real**.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: um site que **se faz passar por um parque real**, recebe dinheiro por PIX e coleta dados pessoais, mas dirige o pagamento a um **beneficiário sem relação com o estabelecimento**, oferece ao consumidor **risco elevado** — alta probabilidade de o "ingresso" não existir, perda do valor pago e exposição de dados pessoais. Recomenda-se **comprar apenas no site oficial** e **não pagar o PIX** (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 (manifesto de integridade preservado em `evidencias/hash_manifest.txt`). O DNS foi consultado via resolvedor público 1.1.1.1; o conteúdo HTML, os bundles JavaScript e os cabeçalhos foram coletados por requisição equivalente à de um navegador comum. O código PIX "copia e cola" informado pelo solicitante foi decodificado pelo padrão EMV/BR Code (TLV) e teve o CRC16 conferido. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (Verisign / .com)	`rdap_raw.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns.txt`
Conteúdo / cabeçalhos	curl (HTTPS e porta 80)	`corpo.html` · `headers_https.txt` · `headers_port80.txt`
Aplicação (front-end)	Download dos JS e das páginas /ingressos e /contato	`assets_js_*.js` · `ingressos.html` · `contato.html`
Certificado TLS	openssl s_client / x509	`tls.txt`
Geolocalização do IP	ipinfo.io · ip-api.com · PTR	`ipinfo.json` · `ipapi.json` · `ptr.txt`

Intermediário de pagamento	RDAP + DNS (basspago.com.br)	`rdap_basspago.json`
Checkout PIX	Decodificação EMV/BR Code (TLV) + CRC16	`pix_decode.txt`
Imagens / metadados	Download de assets · exiftool	`imagens/ · metadata_exiftool.txt`

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

Domínio	snowsland.com (gTLD .com — Verisign)
Registro	**24/05/2026** · expira 24/05/2027 (validade de 1 ano)
Idade na coleta	**~1 mês** — domínio recente · última alteração 19/06/2026
Titular	**Oculto** (privacidade; RDAP expõe só o status do registro)
Status	active
Servidores de nome	coco.bunny.net · kiki.bunny.net (rede Bunny.net / BunnyCDN)
DNS — A	185.22.67.114 · sem AAAA · sem MX · sem TXT/SPF
www	aponta para o mesmo IP (185.22.67.114)
Hospedagem	**AS48716 PS Internet Company LLP (PSKZ) — Almaty, Cazaquistão**
PTR reverso	mx.fd.kz
Geolocalização do IP	Almaty/KZ (ipinfo.io e ip-api.com convergem) — **fora do Brasil**
Servidor web	Server: Caddy · porta 80 → 301 HTTPS · HTTP/2 + HTTP/3 (alt-svc h3)
Ativos da marca	servidos de `jhrcdn.site` (CDN de terceiro, atrás de Cloudflare)
Certificado TLS	CN=snowsland.com · emissor Let's Encrypt (YE2, DV) · válido 19/06/2026–17/09/2026
Série / Fingerprint	0509F16C090F2B19EE1C03A7F14EC09A705C · SHA-256 20:98:9A:DC:58:B7:63:1C:D2:58:C7:90:26:04:B7:3B…

Leitura técnica. Registro recente, validade de 1 ano e titular oculto compõem um perfil de **baixa rastreabilidade do responsável**. A **hospedagem no Cazaquistão** (AS48716/PSKZ) é **incompatível** com uma atração turística sediada em Gramado/RS, cujo site oficial roda em infraestrutura brasileira. O certificado DV gratuito (Let's Encrypt) comprova apenas o controle do domínio, **não a identidade de qualquer empresa**, e foi emitido em 19/06/2026 — mesma data da última alteração do registro, sugerindo troca/ativação recente da hospedagem. Não se imputa conduta à Bunny.net, à Cloudflare, ao provedor cazaque nem ao emissor do certificado — todos meros intermediários de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site reproduz o parque **"Snowland Gramado"**: páginas institucionais (atrações, FAQ, contato) e uma loja de **ingressos** com carrinho, combos e "extras". O endereço (RS-235, Linha Carazal, 5000 — Gramado/RS), o telefone **0800 800 3737**, os e-mails `@gramadoparks.com` e os perfis de redes sociais exibidos pertencem ao **parque verdadeiro** e foram **copiados**. Ao finalizar a compra, o front-end envia os dados do comprador para `/api/checkout.php`, que retorna um código PIX gerado pelo intermediário `pix.basspago.com.br`; o valor é exibido com "20% de desconto no PIX" e o roteiro **simula recusa/instabilidade do cartão** para conduzir o cliente ao PIX.

Aspecto	Constatação
Tipo de serviço	Venda de ingressos do parque "Snowland Gramado" (loja própria com checkout PIX)
Marca / identidade	**Usurpada** — clone do parque real; oficial é snowlandgramado.com.br (Gramado Parks)
Tecnologia	Site estático (servidor Caddy) · checkout em /api/checkout.php · ativos em jhrcdn.site
Meio de pagamento	PIX dinâmico via gateway pix.basspago.com.br (BassPago) · com cartão é simulada "instabilidade"
Recebedor do PIX	**DIGITAL_MARKETPLACE_LTDA — SÃO PAULO** (não corresponde ao parque anunciado)
Dados pessoais coletados	Nome, CPF, e-mail, WhatsApp e data de nascimento (formulário de checkout)
Manipulação no checkout	Falsa recusa do cartão + "20% off no PIX" + valor limitado a R$ 499,94 por transação
Rastreamento	Pixel próprio (px.php) e Google Ads "enhanced conversions" (envia nome/e-mail/telefone)
Identificação do operador	**Ausente** — só dados copiados do parque real; sem CNPJ próprio verificável
Autorização da marca	**Ausente** — sem vínculo demonstrável com Snowland / Gramado Parks

Leitura técnica. O dado mais relevante é a **divergência do recebedor**: o BR Code (EMV) válido (CRC16 conferido: 749E) aponta para **DIGITAL_MARKETPLACE_LTDA**, em São Paulo, ao passo que o site se anuncia como um parque de Gramado/RS. O pagamento trafega por um **gateway brasileiro legítimo** — BassPago, cujo domínio `basspago.com.br` está registrado para **ACXEL CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO LTDA** (CNPJ 36.897.358/0001-06) — mas isso apenas fornece os "trilhos" do PIX; o beneficiário final é uma conta de terceiro **sem relação demonstrável com o parque**. **Não se imputa conduta ao intermediário de pagamento** (BassPago/Acxel), que pode ele próprio estar sendo utilizado por um sub-lojista fraudulento. O conjunto — marca copiada, desconto forçado, recusa simulada do cartão e teto de R$ 499,94 — é típico de **lojas-fantasma de ingressos/produtos** operadas em escala.
Imagens. Os ativos baixados (logos, fotos das atrações, banners) são imagens web reotimizadas: as WebP carregam **perfil ICC sRGB uniforme da Google** (típico de conversão automática de material capturado de terceiros) e **nenhum dado EXIF/GPS/autor**; o ícone de meios de pagamento (`ico-payments.png`) preserva metadados **Adobe Photoshop 26.3 (Windows)** com criação em 04/02/2025. Nenhuma evidência de captação fotográfica própria do parque foi encontrada — coerente com **reuso de material da marca original**. Ver `imagens/metadata_exiftool.txt`.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Recebedor do PIX (DIGITAL_MARKETPLACE_LTDA/SP) não corresponde ao parque anunciado	`pix_decode.txt`	ALTA
2	Usurpação de marca real (clone do "Snowland Gramado"); domínio typosquat com "s" extra	`corpo.html · ingressos.html`	ALTA
3	Checkout manipulativo: recusa simulada do cartão para forçar PIX + falso desconto	`assets_js_ingressos.js`	ALTA
4	Hospedagem offshore (Cazaquistão) incompatível com atração de Gramado/RS	`ipinfo.json · ipapi.json · ptr.txt`	ALTA

5	Domínio recém-registrado (~1 mês), validade de 1 ano, titular oculto	`RDAP — 24/05/2026`	MÉDIA
6	Coleta de CPF, WhatsApp, e-mail e data de nascimento sem operador identificável	`ingressos.html`	MÉDIA
7	Ativos da marca servidos de CDN de terceiro (jhrcdn.site)	`corpo.html`	MÉDIA
8	Valor do PIX limitado a R$ 499,94 por transação (abaixo de limiar)	`assets_js_ingressos.js`	MÉDIA
9	Preços com "descontos" e falsa âncora (De R$ 329) para induzir urgência	`assets_js_ingressos.js`	BAIXA
10	Tráfego pago: Google Ads enhanced conversions com PII do comprador	`assets_js_ads.js`	BAIXA

Síntese: 4 indicadores de severidade ALTA, 4 MÉDIA e 2 BAIXA. **Nenhum fator de legitimidade** (vínculo real com a marca, operador identificável, recebedor coerente, infraestrutura compatível) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 26/06/2026, conclui-se que **snowsland.com** é um **site fraudulento de venda de ingressos** que **se faz passar pelo parque real "Snowland Gramado"** (Gramado/RS, grupo Gramado Parks, cujo site oficial é `snowlandgramado.com.br`). O site reaproveita identidade visual, textos e contatos do parque verdadeiro, mas opera sob **domínio typosquat recém-registrado**, **hospedagem no Cazaquistão**, **titular oculto** e um **checkout manipulativo** que conduz o cliente ao **PIX** — cujo recebedor decodificado, **DIGITAL_MARKETPLACE_LTDA (São Paulo)**, **não tem relação com o estabelecimento anunciado**. Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não pagar o PIX, não informar CPF/dados pessoais e não comprar** neste site. Adquirir ingressos apenas no canal oficial do parque (`snowlandgramado.com.br` / Gramado Parks).
- Conferir sempre o **nome do recebedor** antes de confirmar um PIX: se não for o estabelecimento esperado, **não concluir** o pagamento.
- Se já houve pagamento: acionar imediatamente o banco e o mecanismo **MED** do PIX, reunir comprovantes e registrar reclamação em **consumidor.gov.br** e Boletim de Ocorrência (inclusive na Polícia Civil/Delegacia de crimes cibernéticos).

Recomendações de mitigação / denúncia

- Comunicar o **parque Snowland / Gramado Parks** para que acione abuso de marca e oriente seus clientes, e denunciar o domínio aos canais de **abuse** do registrador, da Bunny.net e da Cloudflare (CDN jhrcdn.site), anexando este laudo.
- Reportar o recebedor e o pedido PIX ao **intermediário de pagamento (BassPago/Acxel)** e à instituição financeira do recebedor, para apuração e eventual encerramento da conta do sub-lojista.
- 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 (Bunny.net, Cloudflare, provedor de hospedagem, BassPago/Acxel), que figuram como intermediários.

— Fim do relatório —

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