RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

snowlland.com

Objeto investigado	snowlland.com — site de venda de "ingressos" que se apresenta como o parque **Snowland Gramado** (gTLD .com)
Natureza	Verificação de legitimidade e de risco ao consumidor (suspeita de falsidade/golpe)
Data da coleta	27/06/2026 (RDAP, DNS, HTTP/TLS, geolocalização, análise do site, decodificação PIX)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise de conteúdo/JS · BR Code (EMV/PIX)
Achado central	Site falso (typosquatting de snowland.com.br) que coleta CPF, cartão e PIX para recebedor alheio ao parque
Classificação	**RISCO ALTO**
Emissão do laudo	27/06/2026 às 03:50

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **snowlland.com**, realizada em **27/06/2026** 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 um site de **venda de ingressos** que se apresenta como o parque **"Snowland Gramado"** (título "Snowland Gramado — Neve de verdade o ano inteiro"), atração turística real localizada em Gramado/RS. Trata-se, porém, de um domínio **distinto e não oficial**: o nome `snowlland.com` (com "L" duplicado) é uma **variação tipográfica** (typosquatting) do site legítimo `snowland.com.br` — este registrado desde **2012**, enquanto o domínio investigado foi registrado há **cerca de um mês** (26/05/2026). O site reaproveita a identidade visual (logotipo, fotos das atrações), serve seus arquivos por um CDN de terceiros (`jhrcdn.site`) e conduz o visitante a um checkout em `/ingressos`.

No fluxo de compra, o site **coleta dados pessoais sensíveis** — nome completo, CPF, e-mail, celular/WhatsApp e data de nascimento — e apresenta campos de **cartão de crédito** (número, validade e CVV), além de gerar uma cobrança **PIX** via `/api/checkout.php`. A análise do código mostra ainda um mecanismo que, para valores acima de **R$ 500**, fraciona o pagamento em **vários PIX** sucessivos — simulando um "parcelamento" que, no PIX, **não existe** e apenas multiplica transferências irreversíveis.

A decodificação do código **PIX "copia e cola"** fornecido (BR Code/EMV, CRC16 válido) revela que o **recebedor não é o parque Snowland**, mas sim **"DIGITAL MARKETPLACE LTDA"** (cidade São Paulo), com o payload intermediado por `pix.basspago.com.br` (gateway "BassPago", da empresa Acxel Consultoria em TI Ltda., sobre infraestrutura AWS em São Paulo). Há, portanto, **incompatibilidade entre o estabelecimento anunciado** (Snowland Gramado, em Gramado/RS) **e o destinatário efetivo do dinheiro**.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: um site recém-criado, que **imita uma marca turística conhecida** por meio de domínio parecido, coleta **CPF, dados de cartão e gera PIX para terceiro** não relacionado ao parque, reúne os sinais típicos de **fraude de venda de ingressos**. Recomenda-se **não comprar, não informar dados e não pagar o PIX** (Seções 5 e 6); ingressos do Snowland devem ser adquiridos apenas pelos canais oficiais (`snowland.com.br`).

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 (arquivo `hash_manifest.txt`). O DNS foi consultado via resolvedor público 1.1.1.1; o conteúdo HTTPS, os arquivos JavaScript e os cabeçalhos foram obtidos por requisição equivalente à de um navegador comum. O código PIX "copia e cola" informado pelo solicitante foi decodificado segundo o padrão **EMV/BR Code (TLV)**, com verificação do dígito **CRC16**. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (Verisign / .com — registrador Trustname)	`rdap_raw.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME) via 1.1.1.1	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS (visitante comum)	`corpo.html` · `ingressos.html` · `headers_https.txt`

Aplicação (front-end)	Download dos scripts JS do site	`ingressos.js · qr.js · ads.js · px.js · main.js · home.js`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · ip-api.com · PTR reverso	`geo_snowlland_*.json · ptr_snowlland.txt`
Intermediário PIX	RDAP + DNS + CNPJ público (BassPago / basspago.com.br)	`rdap_basspago.json · geo_basspago_ipinfo.json`
Código PIX (BR Code)	Decodificação EMV/TLV + verificação CRC16	`pix_copia_cola.txt`
Imagens / metadados	Download de assets · exiftool	`imagens/ · metadata_exiftool.txt`

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

Domínio	snowlland.com (gTLD .com — Verisign)
Registro	**26/05/2026** · expira 26/05/2027 (validade de 1 ano)
Idade na coleta	**~1 mês** — domínio recente
Domínio oficial (legítimo)	**snowland.com.br** (sem "L" duplicado), registrado em **26/02/2012** — ~14 anos
Titular	**Oculto** (privacidade; RDAP expõe só o registrador)
Registrador	Fewmoretaps OU d/b/a **Trustname.com** (registro de baixo custo/anonimizado)
Última alteração	19/06/2026 (configuração de DNS/certificado)
Servidores de nome	coco.bunny.net · kiki.bunny.net (**Bunny CDN**)
DNS — A	185.22.67.114 · sem AAAA · **sem MX · sem TXT/SPF**
www	aponta para o mesmo IP (185.22.67.114)
Hospedagem (borda)	Borda Bunny CDN — **proxy/CDN que oculta o IP de origem**
Geolocalização do IP	185.22.67.114 → PTR `mx.fd.kz` · **Almaty / Cazaquistão** · AS48716 PS Internet Company
Servidor web	Server/Via: **Caddy** · HTTP/3 anunciado (Alt-Svc h3)
CDN de assets	imagens e scripts servidos por `jhrcdn.site` (CDN de terceiros)
Certificado TLS	CN=snowlland.com · emissor **Let's Encrypt** "YE1" (DV) · válido 19/06/2026–17/09/2026
Série	053CE1C8607DD5CD62384DBAAA290DE28A78
Fingerprint SHA-256	FC:7F:B7:A2:54:05:29:39:A2:69:24:7B:9E:D2:4D:16:74:1F:92:F5:D8:8D:79:27:8C:8B:B0:BD:D1:F3:ED:41

Leitura técnica. Registro recente (há ~1 mês), validade de 1 ano, titular oculto e registrador de baixo custo compõem um perfil de **baixa rastreabilidade do responsável**, em contraste com o domínio oficial `snowland.com.br`, ativo desde 2012. O uso de **Bunny CDN como proxy oculta o IP de origem**; o IP de borda observado responde por um nó no **Cazaquistão**, infraestrutura sem relação aparente com um parque sediado em Gramado/RS. 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, à Bunny CDN nem ao provedor de rede — meros intermediários de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site é uma **página de venda de ingressos** em português que reproduz a marca, o logotipo e as fotos das atrações do **Snowland Gramado**. Os arquivos (HTML estático + JavaScript) são servidos por **Caddy**, com imagens e scripts hospedados no CDN de terceiros `jhrcdn.site`. O checkout (`/ingressos`) envia os dados do comprador para `/api/checkout.php`, que devolve um código **PIX "copia e cola"** a ser pago; rotas auxiliares `/api/check-payment.php` e `/api/notify-paid.php` acompanham a confirmação. Há ainda um rastreador próprio (`px.js` → `/px.php`) e um framework de conversão do Google Ads (`ads.js`, "enhanced conversions") que repassa e-mail/telefone/nome do comprador.

Aspecto	Constatação
Tipo de serviço	Venda de ingressos em nome do parque "Snowland Gramado" (não oficial)
Tecnologia	HTML/JS estático sobre servidor Caddy, atrás de Bunny CDN · assets em jhrcdn.site
Meio de pagamento	PIX dinâmico gerado em /api/checkout.php (BR Code "copia e cola" + QR)
Recebedor do PIX	**DIGITAL MARKETPLACE LTDA** (São Paulo) — **não** "Snowland"
Intermediário (gateway)	pix.basspago.com.br ("BassPago") → bassp-prod.onz.software (AWS sa-east-1, São Paulo)
"Parcelamento" PIX	Acima de R$ 500 o código fraciona em **vários PIX** sucessivos (parcela no PIX não existe)
Dados pessoais coletados	Nome, CPF, e-mail, celular/WhatsApp e data de nascimento
Dados de cartão	**Campos de cartão** — número, validade e CVV (coleta de dados de cartão)
Identificação do operador	**Ausente** — sem CNPJ, razão social ou endereço do responsável pelo site
Vínculo com o Snowland	**Não comprovado** — domínio e recebedor distintos do parque oficial

Decodificação do PIX (BR Code/EMV). O código informado decodifica em: 26 GUI `br.gov.bcb.pix` + URL `pix.basspago.com.br/qr/v3/at/2ae0f079-…-0d72bd4f6943` (PIX dinâmico); 52 MCC 0000; 53 moeda 986 (BRL); 58 país BR; 59 recebedor **"DIGITAL_MARKETPLACE_LTDA"**; 60 cidade **SAO_PAULO**; 62 txid "***"; 63 CRC16 **384B (válido)**. O nome do recebedor é genérico e **não corresponde** ao estabelecimento anunciado (Snowland Gramado).
Leitura técnica. O conjunto — domínio parecido com o oficial, marca/fotos reaproveitadas, coleta de CPF e cartão, e PIX destinado a um "marketplace" genérico por meio de um intermediário de pagamento — é compatível com **fraude de venda de ingressos** (o consumidor paga e não recebe o ingresso, ou tem dados/cartão expostos). O risco não está na tecnologia em si, mas na **ausência de responsável identificável** e no **descasamento entre quem é anunciado e quem recebe o dinheiro**. O intermediário BassPago (Acxel Consultoria em TI Ltda., CNPJ 36.897.358/0001-06) e a AWS são **provedores de infraestrutura/pagamento**; descreve-se o fato sem lhes imputar conduta — cabe a eles, mediante denúncia, identificar e bloquear o subadquirente/recebedor.
Imagens. Os assets baixados (logos, fotos das atrações) são, em sua maioria, WebP otimizados para web, **sem metadados EXIF/GPS/autor** e com perfil de cor uniforme (sRGB/Google) — coerente com material de template otimizado por CDN; um único PNG (ícone de meios de pagamento) preserva XMP de **Adobe Photoshop 26.3 (Windows), criado em 02/2025**. Ver `imagens/metadata_exiftool.txt`.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Imitação da marca "Snowland Gramado" por domínio parecido (snow**ll**and vs. snowland) — typosquatting	`corpo.html · RDAP`	ALTA
2	Recebedor do PIX ("Digital Marketplace Ltda", SP) não corresponde ao estabelecimento anunciado	`pix_copia_cola.txt`	ALTA
3	Coleta de dados de cartão (número, validade, CVV) além de CPF e PIX	`ingressos.html · ingressos.js`	ALTA
4	Sem identificação do operador (CNPJ/razão social/endereço) no site	`corpo.html · ingressos.html`	ALTA

5	Falso "parcelamento" via múltiplos PIX acima de R$ 500 (irreversíveis)	`ingressos.js`	MÉDIA
6	Domínio recém-registrado (~1 mês), validade de 1 ano	`RDAP — 26/05/2026`	MÉDIA
7	Titular oculto + registrador de baixo custo (Trustname)	`RDAP — só registrador`	MÉDIA
8	Origem mascarada por Bunny CDN; IP de borda no Cazaquistão	`dns_records.txt · geo_snowlland_ipinfo.json`	MÉDIA
9	Coleta de CPF e data de nascimento de visitantes	`ingressos.html`	BAIXA
10	Assets em CDN descartável de terceiros (jhrcdn.site) com metadados removidos	`corpo.html · metadata_exiftool.txt`	BAIXA

Síntese: 4 indicadores de severidade ALTA, 4 MÉDIA e 2 BAIXA. **Nenhum fator de legitimidade** (vínculo comprovado com o parque, operador identificado, recebedor coerente, histórico do domínio) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 27/06/2026, conclui-se que **snowlland.com** é um site de **venda de ingressos que se faz passar pelo parque "Snowland Gramado"** sem demonstrar vínculo com ele. O domínio é uma **variação tipográfica** do site oficial `snowland.com.br` (este de 2012), foi **registrado há cerca de um mês**, tem **titular oculto** e **origem mascarada por CDN** (borda no Cazaquistão). No checkout, **coleta CPF, dados de cartão e gera PIX** cujo recebedor é **"Digital Marketplace Ltda" (São Paulo)** — pessoa diversa do parque —, com mecanismo de **múltiplos PIX** para valores maiores. O conjunto é compatível com **fraude de venda de ingressos** e expõe o consumidor a perda financeira e a vazamento de dados pessoais e de cartão. Classifica-se o caso como **RISCO ALTO**.

Recomendações ao consumidor / solicitante

- **Não comprar, não informar CPF/dados de cartão e não pagar o PIX** em `snowlland.com`.
- Adquirir ingressos do Snowland **apenas pelos canais oficiais** (`snowland.com.br` e pontos autorizados), conferindo sempre o endereço do site e o nome do recebedor do PIX antes de pagar.
- Desconfiar de anúncios e mensagens (Instagram, Facebook, WhatsApp, TikTok, Google) que conduzam a `snowlland.com` ou prometam ingressos com desconto/urgência.
- Se já houve pagamento: acionar imediatamente o **banco** e o mecanismo **MED** do PIX, **cancelar/monitorar o cartão** informado, reunir comprovantes e registrar **Boletim de Ocorrência** e reclamação em **consumidor.gov.br**.

Recomendações de mitigação / denúncia

- Denunciar o domínio aos canais de **abuse** do registrador (Trustname) e da **Bunny CDN**, e comunicar o intermediário de pagamento **BassPago** (basspago.com.br) para identificação e bloqueio do recebedor/subadquirente, anexando este laudo.
- Comunicar o ocorrido ao **Snowland Gramado** (titular da marca), que pode requerer a remoção do domínio por uso indevido de marca, e reportar a URL como golpe ao Google/Meta e aos navegadores (Safe Browsing).
- 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 (registrador, Bunny CDN, AWS, BassPago/Acxel), meros intermediários técnicos.

— Fim do relatório —