RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

santgreen.com

Objeto investigado	santgreen.com — plataforma de "investimento" em arbitragem esportiva automatizada (gTLD .com)
Natureza	Verificação de legitimidade e de risco ao consumidor/investidor
Data da coleta	06/07/2026 (RDAP, DNS, HTTP/TLS, geolocalização, análise do site e do app)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise de conteúdo e do aplicativo
Achado central	Captação pública com promessa de 200% de retorno + indicação multinível, SEM operador identificado e SEM autorização
Classificação	**RISCO ALTO**
Emissão do laudo	06/07/2026 às 12:39

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **santgreen.com**, realizada em **06/07/2026** 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, mantendo a cadeia de custódia.

O domínio **está no ar** e apresenta a marca **"Santgreen"** como uma suposta **tecnologia automatizada de "arbitragem esportiva"** (título do site: "Santgreen — Tecnologia Automatizada para Resultados Consistentes"; o aplicativo `app.santgreen.com` se identifica como "Santgreen - Arbitragem esportiva"). O site é uma aplicação **Next.js** servida pela **Vercel**, e a área transacional (cadastro, planos, depósito e saque) fica em `app.santgreen.com`, também na Vercel.

O modelo divulgado é o de **captação de recursos do público com promessa de rentabilidade fixa e garantida**: o cliente "aloca" um valor (planos de **R$ 50 a R$ 100.000**) e, segundo o próprio site, **recebe o dobro em 20 dias úteis** — "Aloque R$ 1.000 hoje → Receba R$ 2.000" (retorno de **200%** em ~1 mês), com "resultados diários" creditados e dois saques (dias 10 e 20). O material afirma que "a matemática garante resultados positivos independente do cenário" — uma **promessa de ganho certo e sem risco**, tecnicamente incompatível com qualquer operação legítima de mercado. Soma-se a isso um **programa de indicação multinível** (o site anuncia **8 níveis** de comissão — 12%/5%/3%/2%/1%/1%/1%/1% — enquanto os Termos de Uso citam apenas 5 níveis, contradição interna).

O conjunto de sinais é o de uma **operação opaca e sem lastro verificável**, com o padrão clássico de **pirâmide financeira / esquema Ponzi**: domínio **recém-registrado** (11/03/2026), **titular oculto**, **nenhuma identificação do operador** (sem CNPJ, razão social ou endereço em qualquer página), contato apenas por e-mail de privacidade (**ProtonMail**), contadores de "prova social" **zerados/não preenchidos** ("0+ plataformas", "R$ 0M+ volume", "0+ clientes") e **nenhum registro ou autorização** de órgão regulador (CVM/Banco Central) para ofertar investimento ao público.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: uma plataforma que **promete duplicar o dinheiro em ~1 mês**, remunera pela **indicação de novos participantes** e recebe dinheiro do público **sem identificar quem a opera nem comprovar qualquer autorização** reúne os elementos típicos de **fraude de investimento (Ponzi/pirâmide)**. Nesse modelo, os "lucros" tendem a ser pagos com o dinheiro de novos aportes até o colapso do esquema. Recomenda-se **não se 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, preservando a cadeia de custódia. O registro foi consultado por **RDAP** (Verisign, .com); o DNS por `dig`; o conteúdo e os cabeçalhos por requisições HTTPS equivalentes às de um navegador comum; o certificado por `openssl s_client`; e a geolocalização por ipinfo.io e ip-api.com. Não houve cadastro, depósito, login nem qualquer interação transacional com a plataforma. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (Verisign / .com — registrador GoDaddy)	`rdap_raw.json`
DNS	dig (A, NS, MX, TXT, SOA) — domínio e subdomínio app	`dns_records.txt`

Conteúdo / cabeçalhos	curl HTTPS (site e páginas internas)	`corpo.html · headers.txt · pg_*.html`
Aplicação (front-end)	Download dos bundles JS do site	`chunks *.js · alljs.txt`
Aplicativo transacional	HTTPS a app.santgreen.com (sem login)	`app.html · app_headers.txt`
Certificado TLS	openssl s_client / x509	`ssl_cert.txt`
Geolocalização do IP	ipinfo.io · ip-api.com	`ipinfo.json · ipapi.json`
Imagens / metadados	Download de assets · exiftool	`saint-logo-light.svg (SVG, sem EXIF)`

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

Domínio	santgreen.com (gTLD .com — Verisign)
Registro	**11/03/2026** · expira 11/03/2027 · última alteração 13/03/2026
Idade na coleta	**~4 meses** — domínio recente
Titular	**Oculto** (privacidade de registro; o RDAP expõe apenas o registrador)
Registrador	GoDaddy.com, LLC (IANA 146)
Status	clientDelete/Renew/Transfer/UpdateProhibited (travas padrão do registrador)
Servidores de nome	ns1 / ns2.vercel-dns.com (DNS gerenciado pela Vercel / NS1)
DNS — A	216.150.1.193 · 216.150.16.65 (Vercel/AWS, anycast)
Subdomínio app	app.santgreen.com → 216.150.16.129 · 216.150.16.1 (mesma infra Vercel)
E-mail (MX)	mail.protonmail.ch · mailsec.protonmail.ch — **ProtonMail** (e-mail de privacidade)
TXT / SPF	v=spf1 include:_spf.protonmail.ch · verificações Google, Facebook e ProtonMail
Hospedagem	AS16509 Amazon (AWS) sob a plataforma **Vercel, Inc.** — serverless/edge · Server: Vercel · x-powered-by: Next.js
Geolocalização do IP	Anycast (edge Vercel; nós observados em São Paulo/gru1 e EUA/iad1) — **não revela o operador**
Certificado TLS	CN=*.santgreen.com (wildcard) · emissor Let's Encrypt R13 (DV) · válido 13/05/2026–11/08/2026
Série / Fingerprint	06D1B534AA57C4B59D950EAA933809918D10 · SHA-256 21:DF:74:BD:68:90:D1:E0:A3:C3:E1:03:73:10:4E:27…

Leitura técnica. Registro recente (~4 meses), validade de 1 ano e titular oculto compõem um perfil de **baixa rastreabilidade do responsável**. A hospedagem na **Vercel** (plataforma serverless sobre AWS) e o DNS gerenciado por ela são infraestrutura legítima e de uso comum — não constituem, por si, indício de fraude, mas o modelo **anycast/edge não revela a localização de quem opera o serviço**. O e-mail em **ProtonMail** reforça a opção por anonimato de contato. O certificado **wildcard DV gratuito** comprova apenas o controle do domínio, **não a identidade de qualquer empresa**. Não se imputa conduta ao registrador (GoDaddy), à Vercel, à Amazon (AWS) nem à ProtonMail, meros intermediários de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site apresenta a **Santgreen** como uma "tecnologia automatizada de arbitragem esportiva" que operaria "em mais de 5.000 plataformas" gerando "resultados consistentes de forma 100% automática". O funcionamento divulgado é: (1) **cadastrar-se**, (2) **escolher um plano** (valor "alocado", de R$ 50 a R$ 100.000) e (3) **receber resultados diários** creditados automaticamente, com dois saques (dia 10 e dia 20). O retorno anunciado é de **200% em 20 dias úteis** (o dobro do valor). A área transacional — cadastro, planos, depósito e saque — fica no aplicativo `app.santgreen.com`. O meio de pagamento identificado é o **PIX** (referência a "Pix" nos scripts do app); os endpoints de depósito/saque exigem login e não foram acessados (coleta estritamente passiva).

Aspecto	Constatação
Tipo de serviço	Captação de recursos do público com promessa de rentabilidade ("robô de arbitragem esportiva")
Promessa de retorno	**200% em 20 dias úteis** ("Aloque R$ 1.000 → Receba R$ 2.000"); "resultados garantidos independente do cenário"
Planos / ticket	De R$ 50 a R$ 100.000 por "plano de operação"; ciclo de 20 dias úteis
Programa de indicação	Multinível — site anuncia **8 níveis** (12/5/3/2/1/1/1/1%); Termos citam 5 níveis (contradição interna)
Tecnologia	Aplicação Next.js na Vercel (site institucional + app.santgreen.com)
Meio de pagamento	Depósito/saque via PIX (fluxo no app, atrás de login)
Intermediário (gateway)	Não identificado no front-end público (fluxo por trás de autenticação)
Dados coletados	Cadastro exige dados pessoais (nome, e-mail, senha) e, para saque, dados bancários/PIX do usuário
Identificação do operador	**Ausente** — sem CNPJ, razão social ou endereço em qualquer página (inclusive Termos)
Autorização / registro	**Ausente** — sem registro na CVM/BCB para ofertar investimento ao público
"Prova social"	Contadores da home **zerados/não preenchidos**: "0+ plataformas", "R$ 0M+ volume", "0+ clientes"
Contato divulgado	E-mail em ProtonMail (privacidade); sem telefone, endereço ou canal corporativo verificável

Leitura técnica. A promessa de **retorno fixo e garantido de 200% em ~1 mês** é o principal sinal de alerta: nenhuma operação de mercado lícita (inclusive "arbitragem") entrega ganho certo, diário e sem risco. Combinada com a **remuneração por indicação em vários níveis**, a estrutura corresponde ao padrão de **pirâmide financeira / esquema Ponzi**, em que a "rentabilidade" prometida depende da entrada contínua de novos aportes. A oferta pública desse tipo de "investimento" sem registro configura, em tese, **captação irregular** (competência da CVM) e pode caracterizar crime contra a economia popular e estelionato — avaliação que cabe às autoridades. O risco ao consumidor é agravado pela **ausência total de operador identificável**: não há a quem cobrar os valores prometidos.
Imagens. O logotipo entregue é um **SVG** (`saint-logo-light.svg`) sem metadados EXIF/GPS/autor (formato vetorial). Não foram localizadas fotografias com metadados relevantes no site; por isso não se emitiu relatório complementar de imagens.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Promessa de retorno fixo e garantido (200% em 20 dias úteis) — ganho certo e sem risco	`pg_resultados.html` · `pg_termos-de-uso.html`	ALTA
2	Remuneração por indicação multinível (até 8 níveis) — estrutura de pirâmide	`pg_indicacao.html`	ALTA

3	Captação de recursos do público sem registro/autorização (CVM/BCB)	`corpo.html` · `pg_termos-de-uso.html`	ALTA
4	Nenhuma identificação do operador (sem CNPJ, razão social ou endereço)	`todas as páginas`	ALTA
5	Recebe PIX e vincula dados bancários do usuário, sem responsável localizável	`app.html`	ALTA
6	Domínio recém-registrado (~4 meses), validade de 1 ano, titular oculto	`RDAP — 11/03/2026`	MÉDIA
7	Contradição interna: 8 níveis de indicação na home x 5 níveis nos Termos	`pg_indicacao.html` · `pg_termos-de-uso.html`	MÉDIA
8	"Prova social" fabricada/zerada (contadores "0+" não preenchidos)	`corpo.html`	MÉDIA
9	Contato apenas por e-mail de privacidade (ProtonMail); sem canal corporativo	`dns_records.txt` · `corpo.html`	BAIXA
10	Narrativa de "arbitragem" vaga e não verificável como fonte do lucro	`pg_tecnologia.html` · `pg_faq.html`	BAIXA

Síntese: 5 indicadores de severidade ALTA, 3 MÉDIA e 2 BAIXA. **Nenhum fator de legitimidade** (operador identificado, registro/autorização, contato corporativo, prova social real) foi constatado. O quadro é consistente com **fraude de investimento do tipo pirâmide/Ponzi**.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 06/07/2026, conclui-se que **santgreen.com** opera uma plataforma que **capta recursos do público prometendo rentabilidade fixa e garantida** (200% em 20 dias úteis) e **remunera a indicação de novos participantes em múltiplos níveis**, recebendo valores por PIX — porém **sem identificar quem a opera** (sem CNPJ, razão social ou endereço) e **sem qualquer registro ou autorização** de órgão regulador para ofertar investimento. Esse conjunto de características corresponde ao padrão típico de **pirâmide financeira / esquema Ponzi**. Sinais adicionais (domínio recém-registrado, titular oculto, contato anônimo por ProtonMail, contadores de prova social zerados e contradição interna sobre o número de níveis de indicação) reforçam a avaliação. Classifica-se o caso como **RISCO ALTO** ao consumidor/investidor.

Recomendações ao consumidor / solicitante

- **Não se cadastrar, não depositar e não fornecer dados pessoais, senha ou dados bancários/PIX** ao site ou ao app.
- Desconfiar de qualquer promessa de **ganho fixo e garantido** ("dobre seu dinheiro", "resultado diário sem risco") e de convites para **ganhar indicando amigos** — são marcas de pirâmide/Ponzi.
- Se já houve depósito: acionar imediatamente o banco e o mecanismo **MED** do PIX, reunir comprovantes/prints e registrar reclamação em **consumidor.gov.br** e Boletim de Ocorrência (Polícia Civil).

Recomendações de mitigação / denúncia

- Comunicar o caso à **CVM** (oferta pública irregular de investimento) e ao **Ministério Público** / **Polícia Civil** (indícios de pirâmide financeira e estelionato), anexando este laudo.
- Reportar o domínio aos canais de *abuse* do registrador (**GoDaddy**) e da hospedagem (**Vercel**), e a plataformas onde houver anúncios (Instagram, Meta, YouTube, Telegram), solicitando remoção.
- Preservar este relatório e as evidências (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.