RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

leilaojoaoemilio.com

Objeto investigado	leilaojoaoemilio.com — leiloeiro de veículos e bens (gTLD .com)
Natureza	Verificação de legitimidade e avaliação de risco ao consumidor
Data da coleta	13/06/2026 (RDAP, DNS, HTTP/TLS, geolocalização, análise de conteúdo e imagens)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise de conteúdo e metadados
Achado central	Site de leilão SEM CNPJ identificável, com domínio recente e múltiplos domínios correlatos
Classificação	**RISCO MÉDIO**
Emissão do laudo	13/06/2026 às 01:14

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **leilaojoaoemilio.com**, realizada em **13/06/2026** por técnicas de OSINT (inteligência de fontes abertas) exclusivamente passivas — requisições equivalentes às de um visitante comum e consultas a bases públicas, sem interação intrusiva ou exploração de vulnerabilidades. Evidências preservadas em arquivo com hash SHA-256.

O domínio entrega um site de leilão identificado como **"João Emílio Leiloeiro"**, apresentando-se como empresa com 37 anos de mercado, atuante no segmento de leilões de veículos, bens e imóveis para bancos, seguradoras e órgãos públicos. O site declara endereço físico em **Estrada dos Bandeirantes, 10.639 — Recreio dos Bandeirantes, Rio de Janeiro/RJ**, telefones **(21) 2888-0215 / (21) 2888-0216**, e alega ter o site **"Homologado pelo Tribunal de Justiça do Estado do RJ (TJRJ)"**. O pagamento de lotes arrematados é feito por **depósito bancário identificado ou TED**.

A investigação identificou **três fatores de risco relevantes**: (1) **ausência de CNPJ** em qualquer parte do site — nenhum número de registro do leiloeiro ou da empresa foi localizado; (2) o domínio foi **registrado em 19/01/2026** (≈5 meses), enquanto a empresa alega décadas de atuação; e (3) as imagens do CMS referenciam **múltiplos domínios distintos** (`joaoemilioleilao.org`, `joaoemilioleiloes.net`, `joaoemilioleiloeiro.net`) — padrão compatível com operação que migrou ou opera simultaneamente vários domínios. Um segundo domínio (`joaoemilioleiloeiro.net`) foi registrado pelo mesmo registrador em 02/03/2026, 6 semanas após o primeiro. A **homologação do TJRJ** foi declarada mas não verificada a partir de fontes públicas do Tribunal.

CLASSIFICAÇÃO DE RISCO	RISCO MÉDIO

Leitura: o site apresenta indicadores de presença física verificável (endereço, telefone, TJRJ claim) que o diferenciam de fraudes simples de pagamento direto, mas a **ausência de CNPJ** e a **multiplicidade de domínios recentes** são sinais de alerta que exigem cautela. Recomenda-se verificar a homologação no TJRJ, exigir CNPJ antes de qualquer pagamento, e confirmar os dados da empresa antes de participar de leilões.

2. Metodologia e Cadeia de Custódia

Empregaram-se exclusivamente **técnicas passivas de OSINT**. Toda evidência foi salva em arquivo no momento da coleta e teve hash SHA-256 calculado. O DNS foi consultado via resolvedor público 1.1.1.1 (Cloudflare); HTTP/TLS via `curl` e `openssl s_client`; metadados de imagens via `exiftool`. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (Verisign / .com — registrador easyDNS)	`rdap_raw.json`
Domínio correlato	RDAP (Verisign / .net — joaoemilioleiloeiro.net)	`rdap_net.json`
DNS	dig @1.1.1.1 (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_records.txt`
HTTP/HTTPS	curl com follow-redirect · cabeçalhos e corpo	`headers_https.txt` · `corpo_https.html`
Certificado TLS	openssl s_client / x509	`ssl_cert.txt`
Geolocalização	ipinfo.io · ip-api.com	`ipinfo_104.json` · `ipapi_104.json`
Imagens / metadados	Download de assets · exiftool -a -G1 -s	`imagens/` · `metadata_exiftool.txt`

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

Domínio	leilaojoaoemilio.com (gTLD .com — Verisign)
Registro	**19/01/2026** · expira 19/01/2027 (validade de 1 ano)
Idade na coleta	**≈5 meses** — domínio recente
Titular	**Oculto** (privacidade; RDAP expõe apenas o registrador)
Registrador	easyDNS Technologies Inc.
Status RDAP	clientTransferProhibited · clientUpdateProhibited
Domínio correlato	`joaoemilioleiloeiro.net` registrado em **02/03/2026** pelo mesmo registrador (easyDNS) · Cloudflare
Servidores de nome	dahlia / johnny.ns.cloudflare.com (Cloudflare)
DNS — A	104.21.19.61 · 172.67.185.73 (Cloudflare anycast) · AAAA presente
DNS — MX	mx0001/mx0002.neo.space — email via Neo.space (serviço externo de email corporativo)
DNS — TXT	brevo-code (marketing por email via Brevo/Sendinblue) · neo-verification · SPF neo.space
www	CNAME não detectado — resolv direto nos IPs Cloudflare
Hospedagem (borda)	AS13335 Cloudflare, Inc. — proxy/CDN que oculta o IP de origem
Geolocalização do IP	Anycast Cloudflare (US/Canadá — não revela localização real do servidor)
Servidor web	Server: cloudflare · porta 80 → 301 HTTPS
Certificado TLS	CN=leilaojoaoemilio.com · emissor Google Trust Services WE1 (DV) · válido 18/05/2026–16/08/2026
Serial / Fingerprint	7730403C9183725F0ECA74F2EA189DED · SHA-256 42:75:DC:32…5D:CE:EB:60

Leitura técnica. Domínio recém-registrado (5 meses), titular oculto e uso de Cloudflare como proxy de borda ocultam o IP e a localização real do servidor. O registrador easyDNS é o mesmo dos dois domínios correlatos recentemente criados. Certificado DV (gratuito) confirma apenas controle do domínio — **não a identidade da empresa**. Não se imputa conduta ao registrador (easyDNS), à Cloudflare, à Google (emissor TLS) ou à Neo.space (email), meros intermediários de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site entrega uma **plataforma de leilões públicos e judiciais** em português (pt-BR), identificada como "João Emílio Leiloeiro". Apresenta leilões nas categorias veículos, motos, sucatas, imóveis, pesados, caminhões, náuticos e utilitários — com datas agendadas (15/06/2026 a 15/12/2026) e a modalidade **"Lance Único"**. A plataforma usa PHP/jQuery no back-end, Matomo auto-hospedado para analytics e Facebook Pixel (ID 977251658104460) para rastreamento.

Aspecto	Constatação
Tipo de serviço	Leiloeiro público — veículos, imóveis, bens diversos (incluindo modalidade "Lance Único")
Tecnologia	PHP/jQuery (plataforma de leilão) · Cloudflare CDN · Matomo auto-hospedado · Facebook Pixel
Meio de pagamento	Depósito bancário identificado e TED (conforme FAQ) — remetente envia comprovante por e-mail
Dados pessoais coletados	Nome, CPF/CNPJ, e-mail, telefone e dados bancários (para liberação de lotes)
Identificação do operador	**CNPJ AUSENTE** — nenhum número de CNPJ, matrícula JUCERJA ou registro de leiloeiro localizado em qualquer página do site
Autorização TJRJ	Alegada ("Site Homologado pelo Tribunal de Justiça do Estado do RJ") — **não verificada** por fonte pública do Tribunal nesta investigação
Contato declarado	(21) 2888-0215 / (21) 2888-0216 · WhatsApp +55 21 2888-0215 · e-mail via Cloudflare email-protection
Endereço declarado	Estr. dos Bandeirantes, 10.639 — Recreio dos Bandeirantes, Rio de Janeiro/RJ, 22783-116
Email marketing	Brevo/Sendinblue (TXT brevo-code no DNS) — plataforma de envio de e-mails em massa
Domínios no CMS	Imagens rotuladas com origem em joaoemilioleilao.org, joaoemilioleiloes.net, joaoemilioleiloeiro.net e leilaojoaoemilio.com — indica uso compartilhado ou migração de domínios

Leitura técnica. O fluxo de pagamento (TED/depósito identificado) é típico de leiloeiros tradicionais e distinto de fraudes simples via PIX avulso. Contudo, a **ausência de CNPJ** impede que o consumidor confirme a existência legal da empresa antes de pagar. A **modalidade "Lance Único"** merece atenção especial: é modalidade comum em fraudes de leilão onde o arrematante paga mas não recebe o bem. A presença de imagens provenientes de múltiplos domínios no mesmo CMS sugere migração ou operação multi-site, com conteúdo e histórico transferidos.
Imagens. Logo criado com GIMP 2.10.18 em 14/01/2021 (anterior ao registro do domínio, em 2026) — coerente com empresa pré-existente que migrou de domínio. Banner "alerta" (originado de joaoemilioleilao.org) tem Author EXIF "**top1**" e data de criação 18/12/2025 — autor genérico/anônimo, sem EXIF/GPS significativo.

5. Indicadores de Risco

#	Indicador	Evidência / fonte	Sev.
1	CNPJ do leiloeiro/empresa ausente em todo o site	`HTML, FAQ, Termos de Uso`	ALTA
2	Domínio registrado há ≈5 meses para empresa que alega 37 anos de mercado	`RDAP — 19/01/2026`	ALTA
3	Múltiplos domínios recentes com o mesmo registrador (easyDNS/Cloudflare)	`RDAP: leilaojoaoemilio.com (jan/26) · joaoemilioleiloeiro.net (mar/26)`	ALTA

4	Homologação TJRJ alegada, não verificada por fonte pública do Tribunal	`Texto do site — sem referência a processo ou número`	MÉDIA
5	Titular do domínio oculto (privacidade de registro)	`RDAP — sem dados do registrante`	MÉDIA
6	Imagens do CMS referenciam ≥3 domínios distintos (padrão de migração ou multi-site)	`Nomes de arquivo das imagens no HTML`	MÉDIA
7	Modalidade "Lance Único" presente — associada a fraudes de leilão no Brasil	`HTML — seção de leilões`	MÉDIA
8	Email de marketing externo (Brevo) combinado com email corporativo de terceiro (Neo.space)	`TXT DNS: brevo-code · neo-verification`	BAIXA
9	Template Matomo com variável {{nomeDoUsuario}} não substituída no código-fonte	`HTML — script Matomo`	BAIXA
10	Certificado TLS gratuito DV (não comprova identidade empresarial)	`ssl_cert.txt — Google Trust WE1`	BAIXA

Síntese: 3 indicadores de severidade ALTA, 4 MÉDIA e 3 BAIXA. Nenhum dos itens ALTOS por si só confirma fraude, mas o conjunto — **empresa sem CNPJ + domínio recente + múltiplos domínios correlatos** — eleva o risco e justifica cautela antes de qualquer pagamento.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas em 13/06/2026, conclui-se que **leilaojoaoemilio.com** apresenta-se como **leiloeiro público com histórico declarado de décadas**, endereço físico em Recreio dos Bandeirantes/RJ, telefone e WhatsApp válidos e método de pagamento tradicional (TED). Entretanto, a investigação não localizou **nenhum CNPJ** ou número de registro do leiloeiro em qualquer página do site — dado obrigatório para que o consumidor confirme a existência legal da empresa. Soma-se a isso o registro recente do domínio (5 meses), a existência de um segundo domínio quase idêntico criado logo depois pelo mesmo registrador, e imagens do CMS originadas de múltiplos domínios. A homologação pelo TJRJ, se real, é verificável no site do Tribunal; esta investigação **não confirmou nem negou** tal homologação. Classifica-se o caso como **RISCO MÉDIO** — situação que exige diligência do consumidor antes de participar de leilões ou efetuar qualquer pagamento.

Recomendações ao consumidor / solicitante

- **Exigir o CNPJ da empresa ou matrícula do leiloeiro (JUCERJA/RJ) antes de se cadastrar ou pagar qualquer valor.** Um leiloeiro público registrado deve ter esses dados disponíveis.
- Verificar a homologação no TJRJ: acesse o site do Tribunal de Justiça do Estado do Rio de Janeiro (www.tjrj.jus.br) e consulte a lista de leiloeiros oficiais homologados; confirme se o domínio `leilaojoaoemilio.com` ou o nome "João Emílio Leiloeiro" consta na listagem oficial.
- Ligar para os telefones divulgados **(21) 2888-0215 / (21) 2888-0216** e confirmar o endereço (Estr. dos Bandeirantes, 10.639, Recreio dos Bandeirantes) antes de qualquer pagamento.
- Desconfiar de anúncios em redes sociais (Instagram, Facebook, WhatsApp) que redirecionem para esse domínio com promessas de lotes com preços muito abaixo do mercado.
- Se já efetuou pagamento sem receber o bem: reunir comprovantes, registrar reclamação em **consumidor.gov.br** e **Boletim de Ocorrência**, e acionar o banco para recuperação via MED do PIX (se aplicável).

Recomendações de mitigação / denúncia

- Caso a empresa não comprove CNPJ e homologação, denunciar à **Junta Comercial do Estado do RJ (JUCERJA)** e ao **Ministério Público do Rio de Janeiro** por exercício irregular da profissão de leiloeiro

(Decretos Federais nº 21.981/32 e nº 22.247/33).

• Reportar o domínio ao registrador (easyDNS, abuse@easydns.com) e à Cloudflare caso seja confirmada atividade fraudulenta.

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 serviços citados (easyDNS, Cloudflare, Neo.space, Brevo, Google).

— Fim do relatório —

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