RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

minhaprimeiravaga.click

Objeto investigado	minhaprimeiravaga.click — site que simula inscrição em concurso público federal de segurança (gTLD .click)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	28/07/2026 (RDAP, DNS, HTTP/TLS, geolocalização, bundle JS, base pública de CNPJ)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do app · consulta à base pública de CNPJ
Achado central	Falso concurso público com texto de "Emenda Constitucional" fabricado e taxa de inscrição por Pix; o mesmo código atende uma rede de 24 domínios, cada um exibindo o CNPJ de uma empresa real diferente
Classificação	**RISCO ALTO**
Emissão do laudo	28/07/2026 às 04:09

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **minhaprimeiravaga.click**, realizada em **28/07/2026** 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, sem envio de CPF e sem tentativa de pagamento. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

O domínio **está no ar** e entrega uma aplicação React intitulada "Minha Primeira Vaga — Como Conseguir a Primeira Vaga Pública na Polícia Civil e Científica em 2026", hospedada no **Heroku** (Node/Express) atrás da **Cloudflare**. O site se descreve como "assessoria educacional privada", mas **reveste-se da identidade visual do governo federal**: exibe o **Brasão da República**, a logomarca do **Governo Federal**, o logotipo da **Receita Federal**, a cor institucional do gov.br (`#1351b4`) e links para os perfis oficiais do **Ministério da Justiça e Segurança Pública** e para o `falabr.cgu.gov.br`.

O conteúdo normativo apresentado ao candidato é **fabricado**. O código do site traz o texto integral de uma suposta **"Emenda Constitucional"** que autorizaria "concursos públicos emergenciais" nas Polícias Civis, Científicas e Federal, com artigos numerados, referência ao Fundo Nacional de Segurança Pública e à Lei nº 13.756/2018, além de um "edital" cujo **Art. 6º fixa taxa de inscrição de R$ 89,70, pagável via PIX**. O mesmo material promete **6.500 vagas** e afirma que "não será necessário ensino médio completo" e que "nome negativado não impede a inscrição" — condições incompatíveis com qualquer concurso público real, em que o ingresso depende de edital publicado por banca e órgão competentes.

O funil reproduz um processo oficial de ponta a ponta: rotas `/captura`, `/quiz`, `/cargos`, `/agendamento`, `/locais-prova`, `/verificacao-documental`, `/pre-protocolo`, `/protocolo`, `/pix`, `/confirmar-inscricao` e `/receita`, servidas por APIs próprias — `/api/gerar-pix`, `/api/send-otp`, `/api/sms-pagamento`, `/api/locais-prova` e, especialmente, `/api/validate-cpf` e `/api/verificar-cpf`, esta última retornando um bloco `DADOS` com informações do titular do CPF consultado.

O achado de maior alcance, porém, está na configuração embutida no próprio bundle: o mesmo código atende uma **rede de 24 domínios** (agentefederal.click, concurseirofederal.click, queroserperito.click, fardafederal.click, vocenapolicia.click, entre outros) e, para **23 deles**, define uma razão social e um **CNPJ de uma empresa real e distinta** a ser exibida no rodapé. As consultas à base pública da Receita Federal confirmam que se trata de **empresas reais e sem relação alguma com educação ou concursos** — entre elas uma associação de defesa de direitos sociais em Rio Branco/AC, um comércio de artigos de cama, mesa e banho, uma auto elétrica e uma empresa de manutenção de equipamentos de petróleo. Parte dos CNPJs pertence a blocos **sequenciais abertos poucas semanas antes** do registro dos domínios.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: o site fabrica uma emenda constitucional e um edital para cobrar "taxa de inscrição" por Pix em um concurso que não existe, usando símbolos do governo federal e o CNPJ de empresas reais que nada têm a ver com o negócio. Recomenda-se **não pagar, não informar CPF e não enviar documentos** (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. O DNS foi consultado via resolvedor público 1.1.1.1; o conteúdo, os cabeçalhos e o código do front-end foram obtidos por requisição HTTPS de visitante comum, sem qualquer interação intrusiva, sem envio de dados pessoais e sem tentativa de compra ou de pagamento. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (Tucows/.click — registrador Key-Systems)	`rdap_raw.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS (visitante)	`corpo.html · headers_https.txt`
Aplicação (front-end)	Download do bundle JS	`app_index.js`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · PTR reverso	`ipinfo.json`
Identidades declaradas	Base pública de CNPJ (Receita Federal, via BrasilAPI)	`cnpj_*.json`

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

Domínio	minhaprimeiravaga.click (gTLD .click — Tucows Registry)
Registro	**09/07/2026** · expira 09/07/2027 (validade de 1 ano)
Idade na coleta	**~3 semanas** — domínio muito recente
Titular	**Redigido** no RDAP (o registro informa remoção do contato do titular)
Registrador	Key-Systems, LLC (IANA 1345)
Servidores de nome	cecelia.ns.cloudflare.com · leonard.ns.cloudflare.com
DNS — A	172.67.184.186 · 104.21.19.22 (Cloudflare anycast) · AAAA 2606:4700:… · **sem MX** · sem TXT
Hospedagem	Cloudflare (proxy) sobre **Heroku** — cabeçalhos `via: 2.0 heroku-router`, `x-powered-by: Express` e relatório NEL para nel.heroku.com
Certificado TLS	CN=minhaprimeiravaga.click · emissor Google Trust Services WE1 (DV) · válido 10/07/2026–08/10/2026
Rastreamento de terceiro	`web-telemetry.cloud` — dois scripts carregados, um deles nomeado `primeiravaga-track.js`
Rede associada	**24 domínios** configurados no mesmo bundle, 23 com CNPJ próprio de empresa real distinta

Leitura técnica. Domínio de **três semanas**, com titular redigido e validade de um ano, hospedado em plataforma de aplicação (Heroku) atrás da Cloudflare — perfil de **baixa rastreabilidade e alta descartabilidade**. Não há registro MX: o site não tem e-mail próprio, apesar de simular um processo de inscrição oficial. O certificado DV gratuito comprova apenas o controle do domínio, **não a identidade de qualquer empresa** e muito menos vínculo com o poder público. A presença de um **tracker de terceiro** (web-telemetry.cloud) sobre um fluxo que coleta CPF e telefone amplia a exposição dos dados do candidato. Não se imputa conduta ao registrador, à Cloudflare nem ao Heroku, meros provedores de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site simula, do início ao fim, uma **inscrição em concurso público federal**. O quadro abaixo resume os elementos institucionais reproduzidos e o conteúdo normativo apresentado, ambos extraídos do bundle JavaScript público (`app_index.js`).

Elemento apresentado ao candidato	Constatação
Brasão da República e logo do Governo Federal	`Carregados como imagens; site é privado e não tem vínculo com o poder público`
Logotipo da Receita Federal	`servicos.receitafederal.gov.br/assets/images/receitaAzul.svg`
Perfis do Ministério da Justiça (MJSP)	`Links para facebook.com/MJSPgov, instagram/twitter @mjspgov e falabr.cgu.gov.br`
Cor institucional gov.br	`#1351b4 aplicada aos elementos de interface`
"Emenda Constitucional"	`Texto fabricado, com Arts. 1º a 9º, autorizando "concursos públicos emergenciais" nas polícias`
"Edital" — Art. 6º	`"A taxa de inscrição será de R$ 89,70 … pagável via PIX, boleto bancário ou cartão de crédito"`
Promessas de acesso	`"6.500 vagas"; "Não será necessário ensino médio completo"; "Nome negativado não impede a inscrição"`
Rotas do funil	`/captura · /quiz · /cargos · /agendamento · /locais-prova · /verificacao-documental · /pre-protocolo · /protocolo · /pix · /confirmar-inscricao · /receita`
APIs próprias	`/api/gerar-pix · /api/validate-cpf · /api/verificar-cpf · /api/send-otp · /api/sms-pagamento · /api/sms-agendamento · /api/locais-prova`

Aspecto	Constatação
Tipo de serviço	Simulação de inscrição em concurso público das Polícias Civil, Científica e Federal
Tecnologia	SPA React em Node/Express no Heroku, atrás da Cloudflare · tracker web-telemetry.cloud
Meio de pagamento	Pix (rota `/api/gerar-pix`, QR gerado por api.qrserver.com) — "taxa de inscrição" de R$ 89,70
Dados coletados	**CPF**, nome completo, telefone (com verificação por SMS/OTP), CEP e endereço (via opencep.com)
Consulta de CPF	**/api/verificar-cpf retorna um bloco DADOS com informações do titular** — consulta a dados pessoais a partir do CPF informado
Impersonação institucional	**Brasão da República, Governo Federal, Receita Federal e MJSP** em site privado sem vínculo público
Base normativa	**Fabricada** — "Emenda Constitucional" e "edital" inexistentes
Rede de domínios	**24 hostnames** no mesmo bundle: agentefederal.click, alvoconcurso.click, concurseirofederal.click, concursomentor.click, concursosnarede.click, entrarnacarreirapolicial.click, fardafederal.click, focopolicial.click, minhaprimeiravaga.click, oportunidadefederal.click, orientacaofederal.click, planodeestudos.click, queroserescrivao.click, queroserperito.click, rotafederal.click, seletivopolicial.click, semcursinho.click, suacarreirafederal.click, vagapolicial.click, vidadeservidor.click, vocenapolicia.click, zeroadopolicial.click, mentoriaparavaga.com, querosermentorado.com
CNPJs exibidos	**23 CNPJs distintos de empresas reais**, um por domínio, todos rotulados "Assessoria Educacional"

Contato declarado	meucnpj@contabilizei.com.br · (41) 99788-0145

Leitura técnica. Concurso público no Brasil depende de **edital publicado por órgão e banca competentes**, com taxa recolhida à instituição organizadora — nunca por Pix a um site privado de três semanas. O site inverte cada uma dessas garantias: cria a norma que o autoriza, cria o edital, cria a taxa e recebe o pagamento. Os elementos de "verificação documental", "protocolo", "agendamento" e "locais de prova" existem para dar verossimilhança ao trâmite; a confirmação por SMS/OTP e a consulta de CPF que devolve dados do titular reforçam no candidato a sensação de estar diante de um sistema oficial. A dimensão mais grave é a **rede**: o mesmo código serve 24 endereços, cada um vestindo o CNPJ de uma empresa real diferente — arquitetura desenhada para **diluir responsabilidade e sobreviver a bloqueios**. As empresas cujos CNPJs aparecem são, no que a evidência permite afirmar, **terceiros alheios**, possivelmente vítimas de apropriação de identidade; não se lhes imputa conduta, tampouco ao escritório de contabilidade cujo e-mail é exibido como contato, aos provedores de infraestrutura ou ao intermediário de pagamento.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Texto de "Emenda Constitucional" e de "edital" fabricados para justificar um concurso inexistente	`app_index.js`	ALTA
2	Cobrança de "taxa de inscrição" de R$ 89,70 por Pix em processo seletivo que não existe	`app_index.js`	ALTA
3	Uso do Brasão da República, da logomarca do Governo Federal, do logotipo da Receita Federal e de canais do MJSP em site privado	`app_index.js` · `corpo.html`	ALTA
4	Rede de 24 domínios servidos pelo mesmo código, cada um exibindo o CNPJ de uma empresa real diferente	`app_index.js`	ALTA
5	Rota /api/verificar-cpf retorna dados pessoais do titular a partir do CPF informado	`app_index.js`	ALTA
6	Promessas incompatíveis com concurso real ("6.500 vagas", dispensa de ensino médio, nome negativado não impede)	`app_index.js`	ALTA
7	Domínio com ~3 semanas, titular redigido, validade de 1 ano, em plataforma de aplicação (Heroku)	`rdap_raw.json` · `headers_https.txt`	MÉDIA
8	CNPJs exibidos incluem blocos sequenciais abertos poucas semanas antes do registro dos domínios	`cnpj_67915618000152.json` · `cnpj_67916728000139.json`	MÉDIA
9	Tracker de terceiro (web-telemetry.cloud) sobre fluxo que coleta CPF e telefone	`corpo.html`	MÉDIA
10	Sem registro MX apesar de simular processo oficial de inscrição	`dns_records.txt`	BAIXA

Síntese: 6 indicadores de severidade ALTA, 3 MÉDIA e 1 BAIXA. **Nenhum fator de legitimidade** (edital verificável, órgão organizador, banca, vínculo com o poder público, identidade coerente do operador) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 28/07/2026, conclui-se que **minhaprimeiravaga.click** é um **falso concurso público**: um site privado de três semanas que fabrica uma "Emenda Constitucional" e um "edital", veste-se com o Brasão da República e as marcas do Governo Federal, da Receita Federal e do Ministério da Justiça, coleta CPF e telefone com verificação por SMS e cobra por Pix uma "taxa de inscrição" de R$ 89,70 para um processo seletivo que não existe. O mesmo código atende uma **rede de 24 domínios**, cada um exibindo no rodapé o CNPJ de uma **empresa real e distinta**, sem relação com educação ou concursos — arquitetura voltada a diluir responsabilidade. Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não pagar, não informar CPF, não enviar documentos e não confirmar códigos recebidos por SMS**.
- Conferir a existência do concurso **exclusivamente** no site oficial do órgão e da banca organizadora e no Diário Oficial. Concurso real tem edital publicado, banca identificada e taxa recolhida por GRU ou boleto da organizadora — **nunca por Pix a um site particular**.
- Desconfiar de qualquer seleção que dispense escolaridade, ignore restrição cadastral ou prometa milhares de vagas com inscrição imediata: são promessas incompatíveis com o regime constitucional de acesso a cargos públicos.
- Se já houve pagamento: acionar o banco e o mecanismo **MED** do Pix, reunir comprovantes e prints, e registrar Boletim de Ocorrência e reclamação em **consumidor.gov.br**.
- Se CPF e telefone já foram informados: monitorar consultas e negativações, ativar verificação em duas etapas nos aplicativos bancários e desconfiar de contatos que citem "sua inscrição".

Recomendações de mitigação / denúncia

- Denunciar a rede de 24 domínios à **Polícia Federal** e ao **Ministério da Justiça e Segurança Pública** (uso indevido de símbolos e identidade da União e falso concurso), instruindo com este laudo.
- Comunicar a **Autoridade Nacional de Proteção de Dados (ANPD)** quanto à coleta de CPF e à rota que devolve dados pessoais do titular consultado.
- Reportar os domínios aos canais de *abuse* do registrador (Key-Systems), da Cloudflare e do Heroku, e comunicar as empresas cujos CNPJs são exibidos nos rodapés, que podem ser vítimas de apropriação de identidade.
- 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. Nenhum CPF foi informado ao site e nenhum pagamento foi realizado; os textos, rotas e configurações descritos foram lidos no bundle JavaScript público. A classificação expressa um juízo técnico de risco e não substitui decisão de autoridade policial, administrativa ou judicial. Não se imputa conduta ilícita às empresas cujos CNPJs aparecem nos rodapés da rede (que podem ser vítimas de apropriação de identidade), ao escritório de contabilidade cujo e-mail é exibido como contato, aos provedores de infraestrutura (Key-Systems, Cloudflare, Heroku) nem a intermediários de pagamento.

Anexo A — Manifesto de Integridade (SHA-256)

Hashes SHA-256 das evidências preservadas no momento da coleta (cadeia de custódia).

Arquivo	SHA-256
`app_index.js`	`cc11bff3c7806088df3aab999c692ad40f7c3245f2fc8120702ea25aa9502859`
`cnpj_13523862000140.json`	`ba1e58f114c3f64fa151b8ebb2e863a6f7a6a45e5bff1dd92439c5f49991fdf3`
`cnpj_21257172000115.json`	`6ed662733c6831cec6a34915d64e9e1d2927036d88490cdda697bf2df4846641`
`cnpj_61755368000154.json`	`d87205b67f8c83e082fc12dacecca37384eb206a08156737e7e9252f83bd2c71`
`cnpj_67915618000152.json`	`4eb4473a605e93673076df90000c533c2dd80983cc194d2ff61f71f382f08702`
`cnpj_67916728000139.json`	`e171838e28a359b476850f51faa6f089aa51daedffc3bbc82c9b9df522ffb6a1`
`corpo.html`	`a65a29110749ebd1bd5fa91835880099163c244e1aaa5979732a489bf0081a1a`
`dns_records.txt`	`34a433ee81b0b8588211c9bce41418654f7afaeecdcb5f8feb019654ae367ee3`
`headers_https.txt`	`c8f20198fb3529b901bdbe45dff48a6562ab0efd99e38eaf79d843e1a257ca4f`
`ipinfo.json`	`056a9d50a556b0346844a454db161e04a4fb1e8bc153779728b52637173dc3b5`
`rdap_raw.json`	`554eea0e18a88e95ec5a875b1f9bba107d2dab252d6fb49501f85c34ef73aeaf`
`tls_cert.txt`	`158fc1f91f10b77ffa4deb42688bcbb86cb45baaf35b85c20b7394c342de69d7`

— Fim do relatório —