RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT de campanha coordenada de falso concurso público

"Concurso SEDES/DF" · 4 anúncios + 2 páginas de golpe

Objeto investigado	4 endereços de anúncio (go.*.site) + 2 páginas de golpe (inscrevasedes.site e inscrevasedesbr.site) que se passam pelo concurso público da SEDES-DF
Natureza	Falsa inscrição em concurso público — captura de dados pessoais e cobrança de "taxa" via PIX
Data da coleta	14/07/2026 (RDAP, DNS, HTTP/TLS, análise do cloaker e do fluxo, decodificação PIX)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise de conteúdo/JS · EMV/BR Code
Achado central	Golpe de falso concurso SEDES/DF que usa camuflagem (cloaking) contra revisores e paga a "taxa" a recebedor sem relação com o GDF
Classificação	**RISCO ALTO**
Emissão do laudo	14/07/2026 às 16:11

1. Sumário Executivo

Este laudo documenta a investigação técnica de uma **campanha coordenada de golpe** que se passa pelo **concurso público da Secretaria de Desenvolvimento Social do Distrito Federal (SEDES-DF)**, realizada em **14/07/2026** por técnicas de OSINT e análise passiva — requisições equivalentes às de um visitante comum e consultas a bases públicas, sem qualquer interação intrusiva. Toda evidência foi preservada em arquivo com hash SHA-256 (cadeia de custódia).

O solicitante forneceu **quatro links de anúncio** (todos no formato `go.<domínio>.site/c/<código>`, com parâmetros de **Google Ads** — `gad_source` e `gad_campaignid`): `sedesdfpedagogo.site`, `administracaosedesdf.site`, `novidade2026sedesdf.site` e `direitosedesdf.site`. Todos os nomes imitam a sigla da SEDES-DF, foram registrados **entre 30/06 e 07/07/2026** no mesmo registrador (NameSilo) e usam a Cloudflare — perfil de **rede única operada pela mesma pessoa/grupo**.

Cada link não abre a página final diretamente: serve um **script de camuflagem (cloaking)** que coleta a "impressão digital" do visitante (navegador, tela, fuso, canvas, WebGL, indício de automação) e a envia ao endpoint `/c/<código>/detect`. Conforme o visitante, o servidor decide: para uma **vítima real** (celular, português do Brasil, fuso de São Paulo) carrega em iframe a **página de golpe** (`inscrevasedesbr.site` ou `inscrevasedes.site`); para um **revisor/robô** devolve uma **página-isca acadêmica inócua** que inclusive declara "não possuir vínculo oficial com a SEDES-DF". Essa dupla face serve para **burlar a moderação de anúncios do Google** e a análise de quem investiga, entregando o golpe apenas ao público-alvo pago.

A página de golpe reproduz o visual de um **portal oficial de concurso ("SEDES/DF — Concurso Quadrix")**, com editais, cronograma e tabela de cargos/taxas (R$ 84 para nível médio, R$ 113 para superior). O fluxo de inscrição coleta **CPF, nome, data de nascimento, nome da mãe, RG, endereço completo, e-mail, telefone e senha** e, ao final, gera uma cobrança **PIX**. A decodificação do código PIX "copia e cola" mostra que o **recebedor** não é o Governo do DF nem a banca, e sim **"NATIONAL CORPORATE PARTNE(RS)"** (São Paulo), por meio de um agregador de pagamentos — ou seja, **a "taxa de inscrição" vai para um terceiro sem relação com o certame**.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: trata-se de um **golpe de falso concurso público** que combina uso indevido da imagem de um órgão do GDF, camuflagem para escapar da revisão de anúncios, coleta de dados sensíveis (inclusive enriquecidos por consultas de CPF em bases de terceiros) e cobrança de "taxa" via PIX a beneficiário alheio ao certame. Recomenda-se **não preencher, não pagar e não fornecer dados**, e denunciar (Seções 4 a 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 comportamento do cloaker foi observado enviando ao endpoint `/detect` duas impressões digitais de visitante (perfil de vítima e perfil de robô), registrando cada resposta. O código PIX "copia e cola" fornecido pelo solicitante foi decodificado pelo padrão EMV/BR Code (TLV). Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro dos domínios	RDAP (.site / NameSilo; .com.br / Registro.br)	`rdap_raw.json · rdap_*.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_dig.txt`

Camuflagem (cloaking)	Requisição ao /c//detect com 2 perfis de visitante	`corpo_go_cloaker.html` · `detect_victim.json` · `detect_bot_whitepage.json` · `cloaker_detect_resultados.txt`
Página de golpe e fluxo	Coleta do HTML/JS de cada etapa da "inscrição"	`pagina-golpe/*.html`
Certificados TLS	openssl s_client / x509	`tls_certificados.txt`
Intermediário de pagamento	RDAP + certificado EV (owem.com.br)	`intermediario/rdap_owem.com.br.json`
Código PIX	Decodificação EMV/BR Code (TLV) + CRC16	`pix_copiaecola.txt` · `pix_decodificado.txt`

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

A campanha usa **três camadas de domínio**: (a) os quatro domínios de anúncio, com o subdomínio `go.` que hospeda o cloaker; (b) os dois domínios da página de golpe; e (c) o domínio do intermediário de pagamento. Todos os domínios de golpe são **.site recém-registrados, no registrador NameSilo, com DNS na Cloudflare** — que atua como proxy e **oculta o IP de origem**.

Domínios de anúncio (cloaker)	go.sedesdfpedagogo.site · go.administracaosedesdf.site · go.novidade2026sedesdf.site · go.direitosedesdf.site
Registro (anúncio)	novidade2026: 30/06/2026 · pedagogo/administracao/direito: 07/07/2026 (validade 1 ano)
Domínios da página de golpe	inscrevasedesbr.site (reg. 06/07/2026) · inscrevasedes.site (reg. 30/06/2026)
Registrador	NameSilo, LLC (todos) · titular oculto por privacidade
Servidores de nome	Cloudflare (noel/sarah e alan/rayne .ns.cloudflare.com)
DNS — A (go / golpe)	faixas Cloudflare 104.21.x / 172.67.x · sem MX · sem TXT/SPF
Hospedagem (borda)	AS13335 Cloudflare, Inc. — proxy/CDN que oculta o servidor de origem · PoP de São Paulo (GRU)
Certificado TLS (golpe)	DV emitido por Google Trust Services (WE1) via Cloudflare — comprova só controle do domínio
Intermediário de pagamento	qrcode.owem.com.br → OWEM PAY INSTITUIÇÃO DE PAGAMENTO LTDA · CNPJ 37.839.059/0001-88 (cert. EV) · São Paulo

Leitura técnica. O padrão é homogêneo: mesmos registrador e DNS, nomes que exploram a sigla "sedesdf", registros concentrados em pouco mais de uma semana e origem mascarada por Cloudflare — indicativos de **uma única operação replicada em vários domínios descartáveis**. Os certificados são DV gratuitos e provam apenas controle do domínio, **não a identidade de qualquer órgão público**. O único certificado que identifica uma pessoa jurídica real é o do **intermediário de pagamento** (OWEM PAY) — provedor de infraestrutura financeira, a quem **não se imputa conduta**; o elemento suspeito é o **recebedor** da cobrança (Seção 4). Não se imputa conduta à Cloudflare, ao NameSilo nem ao Google (Ads), meros intermediários.

4. Camuflagem, Fluxo de "Inscrição", Pagamento e Dados Coletados

Camuflagem (cloaking). O anúncio leva a `go.<domínio>/c/<código>`, que exibe um "Carregando…" e, por trás, coleta a impressão digital do dispositivo e a envia por `POST /c/<código>/detect`. A resposta observada foi: para o perfil de **vítima** (Android, pt-BR, fuso de São Paulo) → `mode=iframe` apontando para a página de golpe; para o perfil de **robô/revisor** → `mode=white-html`, um artigo acadêmico inócuo sobre a SEDES-DF que até nega vínculo oficial. Os quatro anúncios convergem para apenas duas páginas de golpe (`inscrevasedesbr.site` e `inscrevasedes.site`, de conteúdo idêntico).

Aspecto	Constatação
O que aparenta ser	Portal oficial de concurso público da SEDES-DF (banca "Quadrix"), com editais, cronograma e cargos
Cargos/taxas exibidos	Nível médio R$ 84,00 · nível superior R$ 113,00 (Agente/Cuidador Social, Direito, Economia, Pedagogia, Psicologia etc.)
Fluxo de inscrição	index → termos → login (CPF) → cadastro (dados completos) → resumo → pagamento PIX
Dados pessoais coletados	CPF, nome, data de nascimento, sexo, e-mail, tipo/nº de RG e UF, nome da mãe, endereço completo (CEP/rua/nº/bairro/cidade/UF), telefone, celular e senha

Enriquecimento por CPF	O cadastro consulta o CPF digitado em APIs de terceiros (amnesiatecnologia.lat, api-apela.online, zipcardx.online, consultarvaloreshoje.info, magmadatahub.com, searchapi.dnnl.live) para preencher/validar o nome — uso de bases de dados pessoais alheias
Meio de pagamento	PIX gerado por gateway interno ("washpay": apigerar-washpay.php / check-washpay.php / webhook-washpay-sedesdf.php), com upsell de "Seguro Reembolso" (+20%) e contagem regressiva de 10 min
Recebedor do PIX	**"NATIONAL CORPORATE PARTNE(RS)", São Paulo** — nome genérico, sem relação com SEDES-DF/GDF/Quadrix
Intermediário do PIX	qrcode.owem.com.br (OWEM PAY Inst. de Pagamento) — agregador; o beneficiário final fica ocultado atrás dele
Identificação do operador	**Ausente** — nenhum CNPJ, órgão ou responsável real; uso indevido do nome SEDES-DF e da banca Quadrix

Código PIX decodificado (EMV/BR Code). Campo 26 (intermediário): `qrcode.owem.com.br/v2/qr/cob/1114…bdb`; campo 59 (recebedor): `NATIONAL CORPORATE PARTNE`; campo 60 (cidade): `SAO PAULO`; campo 53 (moeda): 986/BRL; campo 62 (txid): mascarado; CRC16 **válido**. Em um concurso legítimo, a taxa é paga por boleto/GRU **à banca ou ao órgão** — nunca por PIX a um recebedor de nome corporativo genérico.

Leitura técnica. Não há concurso: há uma **fábrica de captura de dados e de cobrança**. A combinação de camuflagem, impersonação de órgão público, coleta de dados sensíveis com enriquecimento por CPF e cobrança via PIX a beneficiário alheio caracteriza **golpe de falso concurso**. O risco ao cidadão é duplo: **perda financeira** (taxa + "seguro" que nunca geram inscrição) e **vazamento/uso indevido de dados pessoais** (CPF, RG, nome da mãe, endereço, senha) — insumo para fraudes futuras. Não se imputa conduta ao intermediário de pagamento nem aos provedores de infraestrutura; o suspeito é o operador da campanha e o recebedor do PIX.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Impersonação de órgão público (SEDES-DF) e da banca (Quadrix), sem qualquer vínculo oficial	`pagina-golpe/*.html`	ALTA
2	Camuflagem (cloaking): mostra golpe à vítima e página-isca a revisores/robôs	`detect_victim.json` · `detect_bot_whitepage.json`	ALTA
3	Cobrança de "taxa" via PIX a recebedor alheio ao certame ("NATIONAL CORPORATE PARTNERS")	`pix_decodificado.txt`	ALTA
4	Coleta massiva de dados sensíveis (CPF, RG, nome da mãe, endereço, senha)	`cadastro.html`	ALTA
5	Enriquecimento do CPF em APIs de dados de terceiros (bases pessoais alheias)	`cadastro.html`	ALTA
6	Rede de domínios .site descartáveis, mesmo registrador, registro concentrado (30/06–07/07/2026)	`rdap_*.json`	MÉDIA
7	Origem mascarada por Cloudflare (IP do servidor real oculto); sem MX/SPF	`dns_dig.txt`	MÉDIA
8	Tráfego pago (Google Ads) direcionando ao cloaker (gad_source/gad_campaignid)	`headers/URLs de anúncio`	MÉDIA
9	Urgência artificial: contagem regressiva de 10 min e upsell de "Seguro Reembolso" (+20%)	`final.html`	MÉDIA
10	Certificados DV que não identificam nenhum órgão público	`tls_certificados.txt`	BAIXA

Síntese: 5 indicadores de severidade ALTA, 4 MÉDIA e 1 BAIXA. **Nenhum fator de legitimidade** (órgão/banca reais, canal oficial, pagamento ao ente público) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 14/07/2026, conclui-se que os quatro anúncios e as duas páginas de golpe integram uma **campanha coordenada de falso concurso público da SEDES-DF**, que usa **camuflagem (cloaking)** para escapar da revisão de anúncios, **captura dados pessoais sensíveis** (com enriquecimento por consultas de CPF) e **cobra uma "taxa de inscrição" via PIX a um recebedor sem qualquer relação com o Governo do DF ou a banca**. Não há órgão, CNPJ ou responsável legítimo identificável. Classifica-se o caso como **RISCO ALTO** ao cidadão.

Recomendações ao consumidor / solicitante

- **Não preencher os formulários, não pagar o PIX e não fornecer CPF, RG, nome da mãe, endereço, senha ou dados pessoais** a esses sites.
- Conferir sempre o concurso pelos **canais oficiais**: o site do Governo do DF (gov.br/df), o Diário Oficial do DF e o site oficial da banca. Concursos legítimos **não cobram taxa por PIX** a pessoa/empresa de nome genérico.
- Se já houve pagamento: acionar o banco e o mecanismo **MED** do PIX, reunir comprovantes e registrar reclamação em **consumidor.gov.br** e Boletim de Ocorrência. Se dados foram enviados, redobrar atenção a fraudes e considerar troca de senhas reutilizadas.

Recomendações de mitigação / denúncia

- Denunciar os anúncios ao **Google Ads** (uso de cloaking e impersonação de órgão público) e reportar os domínios aos canais de abuse da **Cloudflare** e do registrador **NameSilo**, anexando este laudo, para retirada do ar.
- Comunicar a **SEDES-DF / Governo do DF** e a banca **Quadrix** sobre o uso indevido de seus nomes, e reportar o recebedor do PIX ("NATIONAL CORPORATE PARTNERS") ao intermediário **OWEM PAY** e ao **Banco Central**.
- Preservar este relatório e as evidências (hashes SHA-256) para eventual uso administrativo, policial ou judicial (inclusive Polícia Civil do DF / Ministério Público).

Ressalva metodológica: este laudo baseia-se em fontes abertas e reflete o estado dos endereços 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.