RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

pagamentomunicipal.com

Objeto investigado	pagamentomunicipal.com - página que se apresenta como "Portal do Contribuinte" e cobra "Taxas de Abertura de CNPJ" por Pix (gTLD .com)
Natureza	Verificação de legitimidade e de risco ao contribuinte / empresário
Data da coleta	10/08/2026 (RDAP, DNS, HTTP/TLS, geolocalização, bundle JS) - reverificação em 11/08/2026
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do app
Achado central	Portal falso de órgão público municipal, com fatura nominal e ameaças legais, cobrando R$ 112,00 por Pix em domínio registrado 3 dias antes
Classificação	**RISCO ALTO**
Emissão do laudo	11/08/2026 as 08:53

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **pagamentomunicipal.com**, realizada em **10/08/2026** 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 e sem envio de qualquer dado. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

Na data da coleta o domínio **estava no ar** e entregava uma página em português intitulada **"Taxas de Abertura de CNPJ - Portal do Contribuinte"**, com o logotipo do **gov.br** carregado diretamente do site oficial do governo federal. A página exibia uma **fatura nominal** - razão social "EDILENE PEREIRA AMORIM COMERCIO LTDA", protocolo "ABE-1041.8827", natureza "LTDA - ME", emissão e vencimento no **mesmo dia** - discriminando sete supostas taxas ("DARF - Registro CNPJ", "Taxa Junta Comercial", "Emissão NIRE", "Alvará de Funcionamento", "Licença Sanitária", "Inscrição Estadual", "Taxa Bombeiros (AVCB)") que somavam **R$ 112,00**, pagáveis por **Pix** com contagem regressiva de 15 minutos.

A página acompanhava uma seção de **"Advertência Legal - Consequências do Não Pagamento"** que ameaçava inscrição em Dívida Ativa Municipal (Lei 6.830/80), protesto extrajudicial em cartório (Lei 9.492/97), negativação em SERASA/SPC, execução fiscal com **bloqueio via BACENJUD/SISBAJUD**, multa de 20% e responsabilização pessoal dos sócios (art. 135, CTN), com "prazo final para regularização: hoje". Trata-se de **encenação de autoridade fiscal**: nenhum órgão público brasileiro cobra taxas de abertura de empresa por meio de um site .com privado, com Pix a beneficiário não identificado e prazo de 15 minutos.

Os sinais técnicos confirmam a leitura. O domínio foi **registrado em 07/08/2026** - **três dias** antes da coleta -, com **titular oculto**, validade de apenas 1 ano, e a página era um aplicativo React/TanStack publicado na plataforma de desenvolvimento assistido por IA **Lovable** (PTR `lovable-app-cd-1-4.p.l5e.io`), atrás da Cloudflare. Não há CNPJ, razão social, endereço, telefone, e-mail nem páginas legais do responsável: **não existe no site qualquer entidade localizável** por tras da cobrança. A geração do código Pix ocorre no servidor, por chamada RPC, de modo que o beneficiário final não é exposto ao visitante.

Em **reverificação no dia 11/08/2026**, o endereço deixou de entregar a página de cobrança e passou a responder com um **aviso de remoção da própria plataforma** - "Website Takedown Notice - Lovable Trust & Safety" -, o que indica que a hospedagem retirou o conteúdo do ar após a coleta.

Ponto relevante ao destinatário: a personalização da fatura com a **razão social correta de uma empresa recém-aberta** é o vetor que torna a fraude convincente - dados de constituição de empresas são públicos, e listas de CNPJs novos são rotineiramente exploradas para envio de cobranças falsas. Receber uma cobrança com o próprio nome não a torna legítima.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: uma página anônima, criada três dias antes, que se passa por órgão público, emite fatura nominal com ameaças de protesto e bloqueio judicial e exige Pix em 15 minutos, oferece **risco elevado**. Recomenda-se **não pagar 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. O DNS foi consultado via resolvedor público 1.1.1.1; o conteúdo, os cabeçalhos e o bundle JavaScript foram obtidos por requisição HTTPS de visitante comum. Nenhum formulário foi preenchido e nenhum dado pessoal foi enviado. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada

Registro do domínio	RDAP (Verisign / .com - registrador Name.com)	`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_home.html` · `headers_home.txt`
Página de cobrança	curl HTTPS da rota de pagamento	`corpo_pagamento.html`
Aplicação (front-end)	Download do bundle JS e dos chunks de rota	`bundle_js.txt` · `js_pagamento.txt` · `js_rpc.txt`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · PTR reverso	`geoip.json`
Estado posterior	Reverificação HTTPS em 11/08/2026	`live_takedown_2026-08-11.html`

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

Domínio	pagamentomunicipal.com (gTLD .com - Verisign)
Registro	**07/08/2026** · expira 07/08/2027 (validade de 1 ano)
Idade na coleta	**3 dias** - domínio recém-criado
Titular	**Oculto** (o RDAP expõe apenas o registrador)
Registrador	Name.com, Inc. (IANA 625) · abuse@name.com
Status	clientTransferProhibited
Servidores de nome	ns1hwy / ns2fln / ns3fqs / ns4jnz.name.com
DNS - A	185.158.133.1 · sem AAAA · **sem MX** · **sem TXT**
Hospedagem	AS13335 Cloudflare, Inc. · deploy na plataforma **Lovable**
PTR reverso	`lovable-app-cd-1-4.p.l5e.io` - infraestrutura Lovable
Servidor web	Server: cloudflare · cabeçalho `x-deployment-id` · script `/~flock.js`
Certificado TLS	CN=pagamentomunicipal.com · emissor Google Trust Services WE1 (DV) · válido 08/08/2026-06/11/2026
Emissão do TLS	**um dia após** o registro do domínio
Estado em 11/08/2026	**Removido pela plataforma** - responde "Website Takedown Notice - Lovable Trust & Safety"

Leitura técnica. Registro de três dias, validade de 1 ano, titular oculto e ausência total de e-mail próprio (sem MX) compõem um perfil de **baixa rastreabilidade do responsável**, incompatível com qualquer órgão da administração pública - que opera sob domínios `.gov.br`. O certificado DV gratuito comprova apenas o controle do domínio, **não a identidade de qualquer entidade**. A remoção posterior pela própria plataforma de hospedagem é um fato objetivo registrado nesta investigação. Não se imputa conduta ao registrador (Name.com), a Cloudflare nem a Lovable, meros provedores de infraestrutura - está última, aliás, agiu removendo o conteúdo.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site não é uma loja nem um serviço contratável: é uma **página de cobrança única**, implementada como aplicação React sobre o framework TanStack Start (funções de servidor identificadas no bundle como `TSS_SERVER_FUNCTION` / `createClientRpc`) e publicada pela plataforma Lovable. O visitante chega a uma "guia consolidada de taxas" já preenchida com o nome de sua empresa e segue para a rota de pagamento, que apresenta a fatura e o botão "COPIAR PIX" com expiração em 15 minutos.

Aspecto	Constatação
Tipo de página	Falso portal de administração pública municipal ("Portal do Contribuinte")
Tecnologia	SPA React / TanStack Start publicada na plataforma Lovable, atrás da Cloudflare
Cobrança	**R$ 112,00** em sete rubricas fiscais fictícias, emissão e vencimento no mesmo dia
Destinatário nominal	Fatura personalizada com a razão social "EDILENE PEREIRA AMORIM COMERCIO LTDA" e protocolo "ABE-1041.8827"
Meio de pagamento	**Pix** "cópia e cola", com contagem regressiva de **15 minutos**
Geração do código Pix	No **servidor**, por chamada RPC - o beneficiário final **não e exposto** ao visitante
Coerção	Seção de "Advertência Legal" com ameaça de Dívida Ativa, protesto, SERASA/SPC, BACENJUD/SISBAJUD, multa de 20% e art. 135 do CTN
Marca de terceiro	Logotipo do **gov.br** carregado do site oficial do governo federal - simulação de identidade estatal
Identificação do operador	**Inexistente** - sem CNPJ, razão social, endereço, telefone, e-mail ou páginas legais
Estado em 11/08/2026	Conteúdo **removido** pela plataforma de hospedagem (aviso de takedown)

Leitura técnica. O desenho da página reúne, de forma concentrada, os três elementos clássicos da cobrança fraudulenta: **autoridade simulada** (nome "Portal do Contribuinte", logotipo do gov.br, vocabulário fiscal correto), **personalização** (razão social e protocolo nominais, obtidos de dados públicos de constituição de empresas) e **urgência coercitiva** (vencimento no mesmo dia, Pix expirando em 15 minutos e ameaças de protesto e bloqueio judicial). O valor baixo - R$ 112,00 - é coerente com a estratégia de tornar o pagamento mais barato que a checagem. Como o código Pix é gerado no servidor, o beneficiário só seria conhecido no momento do pagamento; a coleta foi passiva e nenhum código foi gerado.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Simulação de órgão público ("Portal do Contribuinte") com logotipo do gov.br, fora do domínio .gov.br	`corpo_home.html`	ALTA
2	Cobrança de taxas fiscais inexistentes (R$ 112,00) por Pix a beneficiário não identificado	`corpo_pagamento.html`	ALTA
3	Ameaça de Dívida Ativa, protesto, SERASA/SPC e bloqueio BACENJUD/SISBAJUD para forçar o pagamento	`corpo_home.html`	ALTA
4	Domínio registrado 3 dias antes da coleta, titular oculto, validade de 1 ano	`rdap_raw.json`	ALTA
5	Fatura personalizada com razão social e protocolo de empresa recém-aberta	`corpo_home.html`	ALTA
6	Prazo artificial: vencimento no mesmo dia da emissão e Pix expirando em 15 minutos	`corpo_pagamento.html`	MEDIA
7	Nenhuma identificação do operador: sem CNPJ, endereço, telefone, e-mail ou páginas legais	`corpo_home.html` · `dns_records.txt`	MEDIA

8	Código Pix gerado no servidor por RPC - beneficiário final oculto ao visitante	`js_rpc.txt` · `js_pagamento.txt`	MEDIA
9	Publicação em plataforma de desenvolvimento (Lovable), sem infraestrutura institucional	`geoip.json` · `headers_home.txt`	BAIXA
10	TLS DV gratuito emitido um dia após o registro do domínio	`tls_cert.txt`	BAIXA

Síntese: 5 indicadores de severidade ALTA, 3 MEDIA e 2 BAIXA. **Nenhum fator de legitimidade** (domínio institucional .gov.br, identificação do órgão, base legal verificável da cobrança, beneficiário identificado) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 10/08/2026, conclui-se que **pagamentomunicipal.com** era uma **página de cobrança fraudulenta de alto risco**: um falso "Portal do Contribuinte" municipal, publicado em domínio anônimo registrado três dias antes, que usava o logotipo do gov.br e o vocabulário fiscal brasileiro para emitir uma **fatura nominal de R$ 112,00 em taxas inexistentes**, exigia pagamento por **Pix em 15 minutos** e ameaçava o destinatário com Dívida Ativa, protesto, negativação e bloqueio judicial de bens. Não há, no site, qualquer entidade identificável responsável pela cobrança. Classifica-se o caso como **RISCO ALTO**. Registre-se que, em 11/08/2026, o conteúdo já havia sido **removido pela própria plataforma de hospedagem**.

Recomendações ao consumidor / solicitante

- **Não pagar o Pix e não fornecer qualquer dado** a página, ainda que a fatura traga a razão social correta da sua empresa.
- Lembrar que órgãos públicos brasileiros operam em domínios `.gov.br`; cobranças de abertura de empresa são pagas por guia (DARF/DAS/DAM) emitida no portal oficial, nunca por Pix em site `.com` com prazo de minutos.
- Conferir eventuais débitos diretamente na prefeitura do município, na Junta Comercial do estado e no portal **gov.br**, ou com o contador responsável pela abertura da empresa.
- Desconfiar de qualquer cobrança que chegue logo após a abertura do CNPJ: os dados de constituição são públicos e são usados para direcionar cobranças falsas.
- Se já houve pagamento: acionar o banco e o mecanismo **MED** do Pix, 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 (`abuse@name.com`) e da Cloudflare, e a plataforma Lovable, anexando este laudo - registrando que a plataforma já removeu o conteúdo em 11/08/2026.
- Comunicar o uso indevido da identidade visual do **gov.br** aos canais oficiais do Governo Federal, e a prefeitura eventualmente aludida.
- Se a empresa nomeada na fatura for a sua, comunicar o fato ao contador e à Junta Comercial, pois o vazamento útil aqui é a própria publicidade do registro empresarial.
- 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 nas datas indicadas (coleta em 10/08/2026, reverificação em 11/08/2026). 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 citados (Name.com, Cloudflare, Lovable). A empresa nomeada na fatura é apresentada como **destinatária** da cobrança, não como responsável por ela.*

Anexo A - Manifesto de Integridade (SHA-256)

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

Arquivo	SHA-256
bundle_js.txt	f4acbc666b9d72fea2bd0792ff472dcb6da0cc399c551476d4979eb4dcf8035b
corpo_home.html	a04e3b26d52fc297d8aa085c3c55305943f76989762d49cc9b6623e311434444
corpo_pagamento.html	2d2dcdd939d8548b9a49fb78b4e7b9d910f14df2986a7048bb3557cbcc256ef7
dns_records.txt	14f0f417961556ece74abdd614a7000e9076d6bd94b96cdec18e1d56f301fbb6
geoip.json	f3de4534eb304f6b11755d5092960c41b83eb6bcf64b805dc41d0f172d6870b3
hash_manifest.txt	6777b5fc0894a61a3b15d59b4166f1b733260d483863ba2208be0ab6b3398c84
headers_home.txt	fd5c845df9385287d6fd923b7823a7c08a29962dba5c369655037a01b2b537e7
js_pagamento.txt	ddd1a98a17af0f53efed46422bcaebacd6c5c1aac1fd6c2dcd762f81515265d7
js_rpc.txt	3629f72109d590b4da4e48d763a7e0a91e07059e78bc7617bd43125468a26323
live_takedown_2026-08-11.html	623ab286dfc7e4618efb77014a654499ef88da906d2d05990a4c40702f4b758f
live_takedown_headers.txt	14d0cee142abbec55c132a01f7d665ddcf7def793087f4a27cad015515f2d4d3
rdap_raw.json	df855c5407dce24367e2fe7c2e47d9ac9258f52ddb055988addcb11b0bcf02d9
tls_cert.txt	1a1bc928ee750af95abdecd65711fd56449236d099faf0d3cdb012acca807544

- Fim do relatório -