



RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio
agendamentoservicos.digital

Objeto investigado	agendamentoservicos.digital — site que vende "guias educativos" sobre o passaporte brasileiro (gTLD .digital)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	28/07/2026 (RDAP, DNS, HTTP/TLS, geolocalização, bundle JS e chunks do front-end)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do código do front-end
Achado central	Domínio com nome de serviço de agendamento que cobra por Pix modalidades de "processamento" definidas por critérios da Polícia Federal, serviço que é gratuito e não pode ser vendido
Classificação	RISCO MÉDIO
Emissão do laudo	28/07/2026 às 03:58

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **agendamentoservicos.digital**, 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 e sem envio de dados pessoais ou 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 de página única (SPA React/Vite) intitulada "Guia de Passaporte no Brasil", hospedada em **Amazon S3 + CloudFront**, que se apresenta como "plataforma privada de consultoria educacional sobre documentação brasileira". O site exhibe, de forma destacada e repetida, avisos de que **não é órgão público, não representa a Polícia Federal, não realiza agendamento, intermediação, emissão ou entrega** de passaporte, e de que "todo o processo de passaporte pode ser realizado gratuitamente pelo cidadão". Esses avisos existem, são explícitos e pesam a favor do site.

O problema está na **distância entre esses avisos e o que o produto efetivamente vende**. Primeiro, o próprio nome do domínio — **agendamentoservicos.digital** — captura quem procura agendar um serviço público, exatamente aquilo que o site declara não fazer. Segundo, e mais relevante: o checkout não vende um e-book por um preço só; vende **três modalidades de "processamento"** — Normal, **Emergência** e **Urgência** — com **preços diferentes** e descritas com os **critérios oficiais da própria Polícia Federal** ("Prazo padrão de processamento pela Polícia Federal"; "viagem inadiável em até 45 dias... saúde, tratamento médico no exterior"; "viagem inadiável em até 15 dias... doença grave ou morte de familiar"). A prioridade de emissão de passaporte é concedida gratuitamente pela PF mediante justificativa documental — **não é um produto que possa ser vendido por terceiro**, e o site declara não intermediar nada. Terceiro, a tela de pagamento diz textualmente: **"Pague [valor] via Pix para iniciar seu processo de passaporte"**, e o campo que guarda o preço no código se chama **valor_taxa** — vocabulário de taxa pública, não de material didático.

O domínio foi **registrado em 27/12/2025** (cerca de sete meses antes da coleta), com **titular oculto** no RDAP e validade de um ano. A infraestrutura é profissional (AWS, Route 53, certificado da Amazon, Google Analytics, backend Supabase e cobrança por gateway brasileiro), e o site tem termos de uso, política de privacidade e política de proteção de dados — não se trata de uma loja descartável. O risco ao consumidor não é o de não receber nada, e sim o de **pagar por um serviço gratuito** acreditando estar contratando prioridade ou agendamento junto à Polícia Federal.

CLASSIFICAÇÃO DE RISCO

RISCO MÉDIO

Leitura: o site declara vender apenas material educativo, mas estrutura a compra como se fosse uma taxa de processamento de passaporte com níveis de prioridade da Polícia Federal. Quem paga tende a acreditar que comprou celeridade ou agendamento — o que o próprio site afirma não fornecer. Antes de pagar, consulte **gov.br/pf**, onde o agendamento e a prioridade são gratuitos (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 (Identity Digital / .digital — registrador GoDaddy)	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 e dos chunks JS	app_index.js · chunk_*.js
Certificado TLS	openssl s_client / x509	tls_cert.txt
Geolocalização do IP	ipinfo.io · PTR reverso	ipinfo.json

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

Domínio	agendamentoservicos.digital (gTLD .digital — Identity Digital)
Registro	27/12/2025 · expira 27/12/2026 (validade de 1 ano)
Idade na coleta	~7 meses
Titular	Oculto (RDAP expõe apenas o registrador)
Registrador	GoDaddy.com, LLC
Servidores de nome	ns-392.awsdns-49.com · ns-924.awsdns-51.net · ns-1186.awsdns-20.org · ns-1949.awsdns-51.co.uk (Amazon Route 53)
DNS — A	3.174.83.4 · .26 · .74 · .129 (Amazon CloudFront) · sem AAAA · sem TXT
DNS — MX	inbound-smtp.sa-east-1.amazonaws.com (recebimento de e-mail via Amazon SES)
www	CNAME para db1gv4llxx4kh.cloudfront.net
Hospedagem	AS16509 Amazon.com — Amazon S3 (origem) + CloudFront, ponto de presença GRU3 (São Paulo/BR)
PTR reverso	server-3-174-83-4.gru3.r.cloudfront.net
Servidor web	Server: AmazonS3 · Via: CloudFront · x-cache: Hit from cloudfront
Certificado TLS	CN=*.agendamentoservicos.digital · emissor Amazon RSA 2048 M04 · válido 27/12/2025–25/01/2027
Analytics	Google Analytics 4 — G-GMX4D88XG4 (com allow_ad_personalization_signals)

Leitura técnica. A infraestrutura é **madura e legítima**: AWS (S3 + CloudFront + Route 53 + SES), certificado emitido pela própria Amazon, CDN com presença no Brasil e mensuração por GA4. Isso distingue este caso de lojas descartáveis: há investimento e continuidade operacional. O único ponto de atenção no registro é o **titular oculto** — hoje padrão de mercado, mas que, somado a um nome de domínio que sugere serviço público de agendamento, dificulta identificar o responsável. Não se imputa conduta à GoDaddy nem à Amazon (AWS), meros provedores de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site é uma SPA React/Vite com rotas /guias, /primeira-via, /renovacao, /pagamento/:orderId, /pagamento-sucesso/:orderId, além de área autenticada (/login, /dashboard, /admin). O back-end é Supabase e a cobrança por Pix é gerada pela função pagoume-pix-generator; os pedidos guardam um campo witetec_transaction_id, indicando o uso dos intermediários de pagamento PagoU.me/WiteTec. O usuário informa CPF, nome, e-mail, telefone, profissão e endereço completo (preenchido via ViaCEP) antes de pagar.

O ponto central da análise está na tela de escolha da modalidade, reproduzida abaixo a partir do código do front-end.

Modalidade oferecida	Descrição exibida ao cliente (texto do próprio site)
Processamento Normal	"Prazo padrão de processamento pela Polícia Federal" – preço base (valor_taxa)
Processamento Emergência	"Processamento acelerado para casos específicos." Requisitos: "Viagem inadiável em até 45 dias, desde que vinculada a: saúde (tratamento médico no exterior)..." – preço majorado
Processamento Urgência	"Máxima prioridade no processamento." Requisitos: "Viagem inadiável em até 15 dias... Exclusivamente para casos gravíssimos, como: doença grave ou morte de familiar" – preço majorado
Tela de pagamento	"Pague [valor] via Pix para iniciar seu processo de passaporte"
Campo do preço no código	valor_taxa (e valor_final após a escolha da modalidade)

Aspecto	Constatação
Tipo de serviço	Venda de "guias educativos" sobre passaporte (primeira via, renovação, perdido/roubado, infantil)
Tecnologia	SPA React/Vite em Amazon S3 + CloudFront · back-end Supabase · Google Analytics 4
Meio de pagamento	Pix, gerado por função pagoume-pix-generator (PagoU.me) · campo witetec_transaction_id (WiteTec)
Dados coletados	CPF, nome, e-mail, telefone, profissão, CEP, endereço, número, complemento, bairro, cidade (ViaCEP)
Avisos exibidos	Presentes e explícitos: "empresa privada... não possui vínculo com a Polícia Federal"; "Vendemos apenas material educativo"; "Todo o processo de passaporte pode ser realizado gratuitamente pelo cidadão"
Nome do domínio	"agendamentoservicos" — sugere agendamento de serviço público, atividade que o site declara não exercer
Modalidades vendidas	Normal / Emergência / Urgência com preços distintos , descritas pelos critérios oficiais de prioridade da Polícia Federal
Linguagem do checkout	"Pague ... via Pix para iniciar seu processo de passaporte " e campo valor_taxa — vocabulário de taxa pública
Identidade empresarial	Não publicada no site: não há CNPJ, razão social nem endereço nas páginas coletadas

Leitura técnica. Há uma **contradição interna** entre o discurso e o produto. O site afirma não intermediar nem acelerar nada, mas o carrinho oferece **níveis de prioridade de processamento** com preços diferentes, descritos com os critérios que a Polícia Federal usa para conceder — **gratuitamente e mediante comprovação** — atendimento prioritário. Material educativo não tem "prazo de processamento pela Polícia Federal", e um terceiro não tem como entregar celeridade em um processo estatal. Some-se o nome do domínio, orientado a quem busca agendamento, e a frase da tela de pagamento, e o resultado é um fluxo em que o consumidor **pode razoavelmente concluir que está pagando uma taxa oficial ou comprando prioridade** — quando, segundo o próprio site, está comprando apenas um texto informativo. A ausência de CNPJ e razão social nas páginas coletadas agrava a dificuldade de identificar o fornecedor. Não se imputa conduta aos intermediários de pagamento (PagoU.me/WiteTec) nem aos provedores de

infraestrutura citados.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Venda de modalidades "Emergência"/"Urgência" descritas pelos critérios de prioridade da Polícia Federal — celeridade que um particular não pode entregar	chunk_Pagamento-CL2iBVgY.js	ALTA
2	Tela de pagamento afirma "Pague ... via Pix para iniciar seu processo de passaporte" e nomeia o preço como valor_taxa, contradizendo o aviso de que só se vende material educativo	chunk_Pagamento-CL2iBVgY.js	ALTA
3	Nome do domínio ("agendamentoservicos") direcionado a quem busca agendar serviço público — atividade que o site declara não exercer	rdap_raw.json · corpo.html	MÉDIA
4	Coleta de CPF e endereço completo antes do pagamento, para um produto que seria apenas informativo	chunk_PrimeiraVia-DXWwkZVX.js	MÉDIA
5	Nenhum CNPJ, razão social ou endereço do fornecedor nas páginas coletadas	corpo.html · chunk_Footer-C_6oK5Tw.js	MÉDIA
6	Titular do domínio oculto no RDAP	rdap_raw.json	BAIXA
7	Registro recente (~7 meses) com validade de apenas 1 ano	rdap_raw.json	BAIXA

Síntese: 2 indicadores de severidade ALTA, 3 MÉDIA e 2 BAIXA. Ao contrário dos demais casos deste lote, **foram constatados fatores de legitimidade**: infraestrutura AWS consolidada, avisos legais explícitos e destacados, termos de uso, política de privacidade e de proteção de dados, e sete meses de operação. O risco identificado é de **publicidade enganosa e cobrança por serviço gratuito**, não de fraude de pagamento ou captura de credenciais.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 28/07/2026, conclui-se que **agendamentoservicos.digital** é um site **comercialmente operante e tecnicamente sólido**, que exhibe avisos legais corretos sobre não ter vínculo com a Polícia Federal e vender apenas material educativo — mas cujo **funil de compra contradiz esses avisos**: vende, por Pix, três modalidades de "processamento" com preços distintos, descritas pelos critérios oficiais de prioridade da PF, sob a frase "pague para iniciar seu processo de passaporte", em um domínio chamado "agendamentoservicos". Classifica-se o caso como **RISCO MÉDIO** ao consumidor: o risco predominante é **pagar por um serviço que o Estado presta gratuitamente**, ou acreditar ter contratado prioridade ou agendamento que o próprio fornecedor declara não prestar.

Recomendações ao consumidor / solicitante

- **Antes de pagar, consulte os canais oficiais**: o agendamento do passaporte é feito gratuitamente em gov.br/pf, e a taxa oficial (GRU) é paga diretamente à União.
- Saiba que **prioridade de emissão não se compra**: a Polícia Federal concede atendimento emergencial ou urgente **sem custo adicional**, mediante comprovação documental do motivo (saúde, morte de familiar, viagem inadiável). Nenhum site privado pode acelerar esse trâmite.
- Se ainda assim optar por comprar material informativo, **exija a identificação do fornecedor** (CNPJ, razão social e endereço) e guarde o comprovante e o print da oferta.
- Se já houve pagamento e você entendeu estar contratando agendamento ou prioridade: peça o estorno ao fornecedor, acione o banco e o mecanismo **MED** do Pix, e registre reclamação em **consumidor.gov.br** e no Procon.

Recomendações de mitigação / denúncia

- Reportar a oferta ao **Procon** e à **Senacon** como possível publicidade enganosa (arts. 30, 31, 37 e 39 do Código de Defesa do Consumidor), instruindo com este laudo.
- Comunicar a **Polícia Federal** sobre a venda de "modalidades de processamento" descritas com seus critérios oficiais de prioridade, para avaliação quanto ao uso indevido da referência institucional.
- 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. Nenhuma compra foi realizada e nenhum dado pessoal foi enviado ao site; os valores e o fluxo descritos foram lidos no código público do front-end. 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 (GoDaddy, Amazon/AWS, Supabase) nem aos intermediários de pagamento citados.

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	8aed0994d59b756de5c64db96b8ac569f726e4655383afe9350faa836bda2cc9
chunk_client.js	89e3ad04d63104fdf8f84209c0473838a5e9c93a3107a032cd9353ee994413cf
chunk_EbookBonusSection-BAYYq2it.js	30ff927451109478e6a2bf4e7b84cd503ed3eb5456eeabae7b9b97b57b277493
chunk_Footer-C_6oK5Tw.js	3cb3cd50f16c1f55d8a10b7c8b3969af6cfcda6309d525bd64a02feda2643cd2
chunk_Pagamento-CL2iBVgY.js	8923cddb8f3800ec796bc41fd8278252f733a434d68da854b3cf6e7c8c19fc44
chunk_PrimeiraVia-DXWwkZVX.js	95c02935e5066859db60fc2f629ec4df7e4c514f74d56d4f12d61601e3a6ce78
chunk_ProcessingTypeAndTerms-Ch7eAkd3.js	9b5f1b5d44fbc7c2ea3deef7e4d21a483d4aea6c76080f0e5df3bf2f85ae5eb1
corpo.html	240c4d3083334de2f3fd1dc199c021638954e16707fbef86e70cc85376764927
dns_records.txt	b1b5eedb9d1df11ab835981123a1b26d9fe2aec1b2bf0cec2dd3ba969f23a010
headers_https.txt	7d868c107f1d0ebb14cbb3d8688f25209448256fc266368ff7a99851029f39d
ipinfo.json	e65ac9f7013c717245136a87d4b50d1586e029128a7e9ce9481b27982404bf23
rdap_raw.json	71452b49271ed7bcec15774f3a9c80873b2b94d80e86629be4e0513dd6e12e4a
tls_cert.txt	5815352a1fa35d3b9cbb2a062877fbdfe1f3198075dc6c3d5b84dbca0866c150

— Fim do relatório —