



RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

drogariafirmeforte.com

Objeto investigado	drogariafirmeforte.com - domínio cujo nome remete a drogaria/farmácia (gTLD .com)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	02/09/2026 (RDAP, DNS, HTTP/TLS, geolocalização, arquivo web)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · consulta ao Internet Archive
Achado central	O domínio está registrado e com TLS válido, mas não entrega conteúdo : responde HTTP 503 "Site Currently Unavailable" . Sem conteúdo, não é possível avaliar a loja - o laudo documenta apenas a infraestrutura
Classificação	INCONCLUSIVO - SITE FORA DO AR
Emissão do laudo	02/09/2026 as 22:14

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **drogariafirmeforte.com**, realizada em **02/09/2026** por técnicas de OSINT (inteligência de fontes abertas) e análise passiva - requisições equivalentes às de um visitante comum e consultas a bases públicas, sem cadastro, sem envio de dados pessoais e sem qualquer compra ou pagamento. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

O domínio não entregou conteúdo durante a coleta. Duas requisições HTTPS, a segunda com cabeçalhos completos de navegador, retornaram **HTTP 503** com a página padrão de erro do servidor, intitulada "Site Currently Unavailable" (título interno 400_401_403_bgr). O código 503 indica **serviço indisponível** - o servidor existe e responde, mas a aplicação por trás dele não está sendo servida. Não é um domínio expirado nem uma página removida por provedor: é um site **que não está no ar no momento da coleta**.

Em consequência, este laudo não classifica o risco da loja. Não há como avaliar catálogo, preços, identificação do fornecedor, meios de pagamento, páginas legais ou fluxo de compra - nada disso foi servido. Qualquer afirmação sobre a conduta do site seria especulação, e este documento se abstém de fazê-la. A classificação registrada é **INCONCLUSIVA por indisponibilidade**.

A consulta ao **Internet Archive (Wayback Machine)** não retornou **nenhuma captura** do domínio. Assim, também não é possível analisar conteúdo histórico. Registre-se que a ausência de capturas é, por si, um dado: sites com tráfego relevante e alguma longevidade costumam ser arquivados ao menos uma vez.

O que é possível documentar é a infraestrutura, e ela tem uma particularidade digna de registro. O perfil técnico de **drogariafirmeforte.com** é **o mesmo de perfumariavaidosa.com**, também deste lote: **mesmo registrador** (Tucows Domains Inc.), **mesmos servidores de nome** (NS1/NS2.SITEGROUND.NET), **mesmo bloco de hospedagem** (Google Cloud, faixa 34.174.x, Dallas), **mesmo conjunto de MX** (mx10/mx20/mx30.antispam.mailspamprotection.com) e **mesmo padrão de SPF** (<domínio>.spf.auto.dnssmarthost.net). Trata-se do perfil padrão de contas de hospedagem compartilhada da SiteGround, o que significa que a coincidência **não demonstra, por si, vínculo entre os operadores** - milhares de clientes independentes compartilham essa mesma configuração. O fato é registrado por completude, sem inferência.

CLASSIFICAÇÃO DE RISCO

INCONCLUSIVO - SITE FORA DO AR

Leitura: o domínio existe, tem certificado válido e servidor ativo, mas **não entrega conteúdo** (HTTP 503) e **não possui capturas no Internet Archive**. Sem conteúdo, não há objeto a avaliar: a classificação é **inconclusiva**, e recomenda-se **nova coleta caso o site volte ao ar** (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 resolvidor 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 Tucows)	rdap_raw.json
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME) via 1.1.1.1	dns_records.txt
Conteúdo (1ª tentativa)	curl HTTPS simples - HTTP 503	corpo_home.html · headers_home.txt

Conteúdo (2ª tentativa)	curl HTTPS com cabeçalhos de navegador - HTTP 503	corpo_retry.html · headers_retry.txt
Conteúdo histórico	API do Internet Archive (Wayback Machine) - sem capturas	consulta registrada neste laudo
Certificado TLS	openssl s_client / x509	tls_cert.txt
Geolocalização do IP	ipinfo.io · PTR reverso	geoip.json

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

Domínio	drogariafirmeforte.com (gTLD .com - Verisign)
Registro	09/05/2026 · expira 09/05/2027 (validade de 1 ano)
Idade na coleta	Cerca de 4 meses
Titular	Oculto (o RDAP expõe apenas o registrador)
Registrador	Tucows Domains Inc. (IANA 69) · domainabuse@tucows.com
Status	clientTransferProhibited · clientUpdateProhibited
Servidores de nome	ns1.siteground.net · ns2.siteground.net
DNS - A	34.174.77.32 · sem AAAA
DNS - MX	mx10 / mx20 / mx30.antispam.mailspamprotection.com (SiteGround)
DNS - TXT	SPF próprio e verificação Google configurados
Hospedagem	AS396982 Google LLC (infraestrutura SiteGround) · Dallas/EUA
PTR reverso	32.77.174.34.bc.googleusercontent.com
Servidor web	Server: nginx
Certificado TLS	CN=*.drogariafirmeforte.com · emissor Let's Encrypt YR2 (DV) · válido 25/08/2026-23/11/2026
Estado do conteúdo	HTTP 503 - "Site Currently Unavailable" nas duas tentativas
Internet Archive	Nenhuma captura registrada para o domínio

Leitura técnica. A infraestrutura é a de uma **conta de hospedagem compartilhada comum** (SiteGround sobre Google Cloud), com DNS, MX, SPF e certificado curinga corretamente configurados. Isso indica que o domínio foi **preparado para operar** - alguém configurou e-mail e TLS -, e não que esteja meramente estacionado. O certificado, aliás, foi **renovado em 25/08/2026**, oito dias antes da coleta, o que sugere que a conta de hospedagem **segue ativa** mesmo com a aplicação fora do ar. O quadro é compatível tanto com um site **temporariamente indisponível** (falha, manutenção, suspensão por consumo ou por pendência com o provedor) quanto com um site **ainda não publicado** ou **retirado do ar pelo próprio operador**. As evidências **não permitem escolher entre essas hipóteses**, e o laudo não o faz. Não se imputa conduta à Tucows, à SiteGround ou ao Google.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Não há plataforma, fluxo de pagamento ou coleta de dados a descrever: **o site não serviu conteúdo**. Esta seção registra, portanto, apenas o estado observado e o que ele permite e não permite concluir.

Elemento que se pretendia verificar	Situação
Catálogo e preços	Não avaliável - sem conteúdo servido
Identificação do fornecedor (CNPJ, endereço)	Não avaliável
Meios de pagamento	Não avaliável
Páginas legais	Não avaliável
Fluxo de compra e dados coletados	Não avaliável
Conteúdo histórico	Não avaliável - sem capturas no Internet Archive
Registro do domínio	Verificado - 09/05/2026, Tucows, titular oculto
DNS, MX, SPF e TLS	Verificados - configurados e ativos
Estado do serviço HTTP	HTTP 503 - indisponível

Aspecto	Constatação
Estado na coleta	Fora do ar - HTTP 503 "Site Currently Unavailable" em duas tentativas
Nome do domínio	Remete a drogaria / farmácia - setor sujeito a regulação sanitária e a autorização da ANVISA para comércio de medicamentos
Registro	09/05/2026, Tucows, titular oculto, validade de 1 ano
Infraestrutura	SiteGround sobre Google Cloud (Dallas), com MX, SPF e verificação Google configurados
Certificado TLS	Curinga válido, renovado em 25/08/2026 - conta de hospedagem aparentemente ativa
Internet Archive	Nenhuma captura do domínio
Perfil compartilhado	Mesma configuração padrão SiteGround de perfumariavaidosa.com - não indica vínculo entre operadores
Avaliação de risco da loja	Impossível - sem conteúdo, não há objeto a analisar

Leitura técnica. Este laudo é deliberadamente **curto em conclusões**, e isso é uma escolha metodológica, não uma limitação de esforço. Um domínio cujo nome sugere farmácia, com titular oculto e quatro meses de registro, é o tipo de alvo que uma análise apressada classificaria como suspeito por analogia com outros casos. **Não é o que se faz aqui.** Sem conteúdo servido e sem capturas históricas, **não existe evidência sobre a conduta do site** - nem a favor, nem contra. Afirmar risco alto seria inferir a partir do nome e do vizinho de hospedagem; afirmar risco baixo seria igualmente infundado.

Registre-se ainda que a coincidência de perfil de infraestrutura com **perfumariavaidosa.com** - avaliado neste mesmo lote como de risco baixo - **não transfere** classificação em nenhuma direção: a configuração observada (Tucows + SiteGround + Google Cloud + mailspprotection) é o **padrão de fábrica** de uma das maiores hospedagens compartilhadas do mundo, usada por um número enorme de clientes independentes entre si. Tratá-la como indício de vínculo seria erro elementar de análise. O correto é **reverificar o domínio quando e se voltar ao ar**.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
---	-----------	-----------	------

1	Site não entrega conteúdo: HTTP 503 "Site Currently Unavailable" em duas tentativas distintas	headers_home.txt · headers_retry.txt	MEDIA
2	Nenhuma captura no Internet Archive - sem histórico público verificável	consulta ao Wayback Machine	MEDIA
3	Titular oculto no RDAP, com registro de validade de 1 ano	rdap_raw.json	BAIXA
4	Nome de domínio remete a comércio de medicamentos, atividade sujeita a autorização sanitária	rdap_raw.json	BAIXA
5	Certificado TLS renovado 8 dias antes da coleta, indicando conta de hospedagem ainda ativa	tls_cert.txt	BAIXA

Síntese: **nenhum** indicador de severidade ALTA, 2 MEDIA e 3 BAIXA - e todos eles dizem respeito à **indisponibilidade e à opacidade** do domínio, não a qualquer conduta observada. **Nenhum juízo é emitido sobre a loja**, porque nenhuma loja foi servida.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em **02/09/2026**, conclui-se que **drogariafirmeforte.com não pôde ser avaliado**. O domínio está registrado desde **09/05/2026**, tem DNS, MX, SPF e certificado TLS curinga corretamente configurados - este último renovado oito dias antes da coleta -, mas **não entrega conteúdo**: responde **HTTP 503 "Site Currently Unavailable"** tanto a requisições simples quanto a requisições com cabeçalhos completos de navegador. O **Internet Archive não possui nenhuma captura** do domínio, de modo que também não há conteúdo histórico a examinar. Sem catálogo, sem identificação de fornecedor, sem meios de pagamento e sem páginas legais servidos, **não existe objeto sobre o qual emitir juízo de risco**. Registra-se a classificação **INCONCLUSIVA por indisponibilidade** e recomenda-se **nova coleta caso o site volte ao ar**. Este laudo **não afirma nem sugere** que o domínio seja fraudulento, tampouco que seja idôneo.

Recomendações ao consumidor / solicitante

- Se você chegou a este domínio por um anúncio, link ou mensagem, **não presuma que ele é confiável nem que é golpe**: no momento desta coleta ele simplesmente não estava no ar.
- Caso o site volte a funcionar, aplicar as verificações básicas antes de comprar: **procurar CNPJ, razão social e endereço** no rodapé ou nas páginas legais e conferir o CNPJ na consulta pública da Receita Federal.
- Tratando-se de nome que remete a **drogaria**, verificar adicionalmente se há **autorização sanitária** para o comércio: farmácias e drogarias que vendem medicamentos pela internet precisam de licenciamento e de registro junto à **ANVISA** e à vigilância sanitária local.
- Preferir **cartão de crédito** a Pix em qualquer loja sem histórico, e desconfiar de medicamentos vendidos sem exigência de receita quando ela for obrigatória.
- Se já houve pagamento a este domínio antes de ele sair do ar: acionar o banco (e o **MED** do Pix, se aplicável), reunir comprovantes e registrar reclamação em **consumidor.gov.br** e Boletim de Ocorrência.

Recomendações de mitigação / denúncia

- **Reverificar o domínio periodicamente**: caso volte ao ar, refazer a coleta completa (conteúdo, identificação do fornecedor, meios de pagamento e páginas legais) e emitir laudo conclusivo.
- Não utilizar este laudo como base para denúncia por fraude: **ele não documenta conduta alguma**, apenas a indisponibilidade do serviço.
- Se o domínio voltar ao ar oferecendo **medicamentos** sem licenciamento visível, comunicar à **ANVISA** e à vigilância sanitária local, além do Procon.
- Preservar este relatório e as evidências (pasta evidencias/, com hashes SHA-256) como registro do estado do domínio em 02/09/2026.

Ressalva metodológica: este laudo baseia-se em fontes abertas e reflete o estado do domínio na data indicada (coleta em 02/09/2026), quando o site **não entregava conteúdo. Nenhum juízo de risco é emitido sobre a loja**, porque não houve loja a observar; a classificação "inconclusivo" registra exatamente isso. **Não se afirma nem se sugere que o domínio seja fraudulento.** A coincidência de perfil de hospedagem com outro domínio deste lote decorre da configuração padrão de um grande provedor compartilhado e **não demonstra vínculo entre operadores.** Não se imputa conduta aos provedores citados (Tucows, SiteGround, Google).

Anexo A - Manifesto de Integridade (SHA-256)

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

Arquivo	SHA-256
corpo_home.html (73849 bytes)	35ecc4ed14e84a422921ac5a2702c2e75a4810e13e354b986dfed463e20eef73
dns_records.txt (623 bytes)	d18190c6a3d390aca951e0a80870583b8d4402e0152c3c3f4dbd0e24aaabdea4
geoip.json (301 bytes)	f0c9c9e072c036ec7850100ea4d4e0c05b03fc4af18b415008c1cd91cb7b5425
headers_home.txt (196 bytes)	e301b6bb112c42a176b6f12012f5950c654fb706c83708f5a3b5ca84e49f8dfc
rdap_raw.json (2680 bytes)	4241de94986f3835148063204602286ab0cd2bd90db034dc1edb7f079355165c
tls_cert.txt (309 bytes)	063d26d499d7c2acfc0340b4662a144ed39ca9a12f0292d716c5a7866ac537

- Fim do relatório -