RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, forense e de risco do domínio

stampit.com.br

Objeto investigado	stampit.com.br ("Stamp It" — vestuário com estampas)
Natureza	Verificação de legitimidade e de risco ao consumidor (loja virtual)
Data da coleta	03–04/06/2026 (RDAP, DNS, HTTP, TLS, geolocalização e arquivo histórico)
Métodos	OSINT passivo · RDAP · DNS · cabeçalhos HTTP · TLS · CNPJ · Wayback Machine
Emissão do laudo	04/06/2026 às 16:41

1. Sumário Executivo

Este relatório documenta a investigação técnica do sítio eletrônico **https://stampit.com.br**, loja virtual apresentada ao público como "**Stamp It**", marca brasileira de vestuário e calçados com estampas (camisetas, botas, tênis e acessórios). A coleta de evidências foi realizada em 03–04/06/2026 por meio de técnicas de OSINT (inteligência de fontes abertas) e análise forense passiva, sem qualquer interação intrusiva com a infraestrutura-alvo.

Diferentemente do padrão de "loja-fantasma" descartável, a análise encontrou uma **identidade empresarial real e verificável**: o domínio existe há mais de seis anos (registrado em 2019), está vinculado a um **CNPJ ativo na Receita Federal** (3BET Comércio de Confecções do Vestuário Ltda, Franca/SP), cujo sócio-administrador coincide com o titular do domínio; o site opera sobre a plataforma **Shopify**, com checkout intermediado e regulado, e-mail corporativo Google Workspace e atendimento por WhatsApp com DDD compatível com a sede da empresa. **Os indicadores clássicos de fraude estão, em sua maioria, ausentes.**

O risco identificado é de outra natureza, **operacional e de continuidade**: na data da coleta a loja encontra-se **inativa**. O servidor Shopify responde com **HTTP 402 (Payment Required)** — estado em que a plataforma congela a loja por pendência de assinatura — e a página pública exibe o aviso padrão "Esta loja não está disponível no momento". O último conteúdo capturado antes do congelamento (02/06/2026) era um "AVISO IMPORTANTE" informando **pausa temporária das vendas por reestruturação interna**, ainda assim coletando e-mails de visitantes. Esse cenário expõe a risco, sobretudo, **consumidores com pedidos em aberto** (pagos e ainda não entregues) e quem pretenda comprar agora.

CLASSIFICAÇÃO DE RISCO	RISCO MODERADO

Leitura: trata-se de comerciante **real e identificável**, e não de uma fachada anônima. O risco preponderante é a **loja estar fora do ar / com vendas pausadas**, com possível impacto a pedidos já pagos. Recomenda-se cautela com pagamentos e atenção a eventuais cobranças fora do checkout oficial da Shopify (ver Seções 9 a 11).

2. Metodologia e Cadeia de Custódia

A investigação seguiu o princípio da **preservação probatória**: todas as respostas de rede foram salvas em arquivo no momento da coleta e tiveram seu resumo criptográfico (hash SHA-256) calculado, permitindo a verificação de integridade a qualquer tempo. Nenhuma técnica intrusiva, de exploração de vulnerabilidade ou de engenharia reversa de servidor foi empregada — apenas requisições equivalentes às de um visitante comum e consultas a bases públicas (RDAP, DNS, Receita Federal via BrasilAPI e o arquivo histórico Wayback Machine).

Etapa	Técnica / ferramenta	Evidência preservada
Registro do domínio	RDAP — Registro.br (.br)	`rdap_raw.json`
Pessoa jurídica	Consulta de CNPJ (BrasilAPI / Receita)	`cnpj_brasilapi.json`
Infraestrutura DNS	Consultas dig (A, AAAA, NS, MX, TXT, SOA)	`dns_records.txt`
Cabeçalhos / corpo HTTP	curl — HTTPS (443) e HTTP (80)	`headers_https.txt · corpo_https.html`
Certificado TLS	openssl s_client / x509	`ssl_cert.txt · ssl_raw.txt`
Geolocalização do IP	ipinfo.io e ip-api.com	`ipinfo_*.json · ipapi_*.json`

Histórico do site	Internet Archive (Wayback Machine)	`wayback_2025-10-07_*` · `wayback_2026-06-02_*`

Todos os artefatos estão na subpasta **evidencias/** e seus hashes constam do Anexo A (Manifesto de Integridade). O fuso horário de referência é UTC; conversões para o horário de Brasília (BRT, UTC−3) são indicadas quando aplicável.

3. Identificação do Domínio (RDAP)

Os dados a seguir foram obtidos junto ao **Registro.br** (NIC.br), operador do TLD **.br**, pelo protocolo RDAP. Diferentemente de TLDs estrangeiros, o Registro.br divulga publicamente os dados do titular, o que permitiu a identificação direta do responsável.

Domínio	stampit.com.br
Data de registro	26/12/2019 21:47:01 UTC
Última alteração	31/10/2025 16:57:26 UTC
Data de expiração	26/12/2026 21:47:01 UTC
Idade do domínio	**~6 anos e 5 meses** — domínio antigo e renovado (não recente)
Titular / Registrant	Renato de Pina Ramos
CNPJ do titular	21.775.785/0001-44
Contatos (adm./téc.)	Renato de Pina Ramos · renato.nuvens@gmail.com
Registrador (Registrar)	GoDaddy
DNSSEC	Não assinado (delegationSigned: false)
Servidores de nome	carrera.ns.cloudflare.com · vicente.ns.cloudflare.com
Status	active

Leitura técnica. A antiguidade do domínio (mais de seis anos, com renovação registrada em out/2025 e validade até dez/2026) é um **fator de legitimidade**: contraria frontalmente o perfil de domínio descartável de poucas semanas usado em golpes. O titular não está redigido por privacidade — é uma pessoa jurídica identificada (CNPJ 21.775.785/0001-44), detalhada na Seção 3.1. A delegação aponta para servidores de nome da Cloudflare, o que é coerente com a hospedagem analisada na Seção 5.

3.1. Pessoa jurídica vinculada (CNPJ)

A consulta ao CNPJ informado no registro retornou empresa **ativa** na Receita Federal, cujo sócio-administrador é a mesma pessoa indicada como titular do domínio — uma correspondência que reforça a autenticidade da identidade comercial:

Razão social	3BET COMÉRCIO DE CONFECÇÕES DO VESTUÁRIO LTDA
Nome fantasia	PLIIM
CNPJ	21.775.785/0001-44 (matriz)
Situação cadastral	**ATIVA** (sem motivo de baixa)
Início de atividade	29/01/2015
Atividade (CNAE)	4781-4/00 — Comércio varejista de artigos do vestuário e acessórios
Natureza / porte	Sociedade Empresária Limitada · Microempresa
Capital social	R$ 99.800,00
Endereço	Rua Belém, 1181 — Jardim Brasilândia, Franca/SP, CEP 14402-272
Sócio-administrador	Renato de Pina Ramos (entrada em 09/09/2019)

Telefone informado	(16) 9423-4966

Leitura técnica. O ramo registrado (varejo de vestuário) é coerente com o produto anunciado no site. A sede em **Franca/SP** — tradicional polo calçadista — alinha-se ao DDD 16 do WhatsApp de atendimento (Seção 7) e à oferta de calçados estampados. A convergência entre titular do domínio, sócio-administrador e ramo de atividade constitui um conjunto consistente de **fatores de legitimidade**. Ressalva: a existência de CNPJ ativo comprova a constituição da empresa, mas não, por si só, a regularidade da operação comercial atual nem a quitação de pedidos pendentes.

4. Infraestrutura de DNS

A zona DNS é gerenciada pela **Cloudflare**, e os registros de endereço apontam para a faixa anycast da própria Cloudflare — ou seja, o site utiliza o proxy/CDN da Cloudflare, que oculta o servidor de origem (adiante identificado como Shopify). O domínio possui e-mail corporativo provido pelo **Google Workspace**.

Registro	Valor	Observação
A	`104.21.52.30 · 172.67.194.157`	Faixa anycast Cloudflare (proxy/CDN ativo)
AAAA	`2606:4700:3033::ac43:c29d · 2606:4700:3036::6815:341e`	IPv6 Cloudflare
NS	`carrera.ns.cloudflare.com / vicente.ns.cloudflare.com`	DNS gerenciado pela Cloudflare
MX	`aspmx.l.google.com (+ alt1/alt2/aspmx2/aspmx3)`	E-mail corporativo Google Workspace
TXT / SPF	`v=spf1 include:_spf.google.com ~all` + 2× `google-site-verification`	Política de e-mail definida; verificações Google
SOA	`carrera.ns.cloudflare.com (serial 2403699317)`	—
www	`104.21.52.30 · 172.67.194.157`	Mesmo destino do apex (Cloudflare)

Leitura técnica. A presença de registros MX do Google e de SPF configurado indica que o domínio opera **e-mail corporativo profissional** — outro fator de legitimidade, ausente em fraudes improvisadas. As duas entradas `google-site-verification` sugerem integração com serviços Google (Search Console / Workspace). O uso de Cloudflare como DNS e proxy é prática comum e idônea; aqui o proxy está efetivamente ativo, ao contrário de instalações que expõem o IP de origem.

5. Hospedagem e Geolocalização

A geolocalização do endereço IP atendido reflete a rede **anycast** da Cloudflare e, por trás dela, a plataforma de e-commerce **Shopify** (identificada pelos cabeçalhos HTTP). Por se tratar de anycast, diferentes bases de geolocalização retornam cidades distintas — o que é esperado e não indica, isoladamente, qualquer irregularidade.

Endereço IP (consultado)	104.21.52.30
Sistema autônomo	AS13335 — Cloudflare, Inc.
Geolocalização (ipinfo.io)	San Francisco / EUA — registro anycast
Geolocalização (ip-api.com)	Toronto / Canadá — registro anycast (hosting: true)
DNS reverso (PTR)	— (vazio; típico de IP anycast de borda)
Plataforma de origem	**Shopify** (cabeçalho `powered-by: Shopify`)
Loja Shopify interna	polo-stamp-it-port.myshopify.com
Moeda da loja	BRL — Real brasileiro

Plataforma idônea, não infraestrutura "offshore" suspeita. A combinação Cloudflare (CDN/DNS) + Shopify (e-commerce) é uma das mais difundidas no varejo on-line legítimo do mundo. A localização física dos data centers (EUA, via Shopify/GCP) é uma característica da plataforma SaaS e **não** equivale ao padrão de hospedagem em provedor de baixa reputação tipicamente associado a sites fraudulentos. O identificador interno `polo-stamp-it-port.myshopify.com` confirma a loja como instância Shopify da marca "Stamp It".

Leitura técnica. Não se imputa qualquer conduta à Cloudflare ou à Shopify — são provedores de infraestrutura e plataforma. O ponto relevante é que a hospedagem é **compatível** com um e-commerce brasileiro comum e operado por terceiros idôneos,

afastando o indicador de "hospedagem offshore incompatível".

6. Certificado TLS / HTTPS

Titular (Subject)	CN = stampit.com.br
Emissor (Issuer)	Let's Encrypt — autoridade "E7" (C=US)
Tipo de validação	DV — Domain Validation (validação apenas de domínio)
Válido de	12/04/2026 12:28:03 UTC
Válido até	11/07/2026 12:28:02 UTC
Número de série	062DD163F2323CDD354717140D976F00D436
Fingerprint SHA-256	C5:55:D2:A1:92:48:50:B6:D0:B2:DF:DB:20:5F:C7:B2: 98:DF:A3:83:F6:6E:47:B1:15:E3:69:8B:3C:3C:25:05

Leitura técnica. O certificado é válido e a conexão HTTPS é legítima do ponto de vista criptográfico. Trata-se de certificado **gratuito do tipo DV** (emitido automaticamente pela infraestrutura Cloudflare/Shopify via Let's Encrypt), que comprova o controle do domínio mas **não atesta a identidade jurídica** da empresa — observação válida tanto para sites legítimos quanto para fraudulentos. A porta 80 (HTTP) responde com redirecionamento 301 para HTTPS, comportamento adequado.

7. Análise do Conteúdo e do Estado Atual da Loja

Na data da coleta (04/06/2026), a página pública **não exibe a loja**: o servidor Shopify responde com **HTTP 402 (Payment Required)** e entrega a página padrão de loja indisponível ("Esta loja não está disponível no momento", com links da Shopify marcados `ExpiredDomainLink`). Esse estado é o **congelamento da loja por pendência de assinatura/cobrança** junto à própria Shopify — e não a remoção definitiva da conta.

O arquivo histórico (Wayback Machine) permite reconstruir o estado anterior do site em dois momentos:

Data (captura)	Estado observado
07/10/2025	**Loja ativa e vendendo.** Catálogo de camisetas de algodão e botas/coturnos com estampas (coleções "Bandas de Rock", "Boho"). Promoção progressiva ("2 itens R$70 OFF · 3 itens R$140 OFF · 4 itens R$210 OFF"). Bandeiras de cartão (ex.: American Express) e checkout Shopify. Nome da loja: "Stamp It".
02/06/2026	**Aviso de pausa.** Banner "AVISO IMPORTANTE": a marca informa "há mais de 5 anos" de atuação e comunica que as "vendas estão temporariamente pausadas" por "reestruturação interna" (processos, produção, atendimento e logística), convidando o visitante a deixar e-mail para avisos de retorno. Atendimento por WhatsApp (DDD 16).

O texto institucional ("há mais de 5 anos") é **consistente** com a idade do domínio (2019) e do CNPJ. A loja empregava pilha de marketing típica de varejo digital profissional — pixels de **Facebook/Meta, Google Ads/Analytics e Mailchimp** — coerente com operação que investe em tráfego pago.

7.1. Ponto de atenção — uso de marcas e obras de terceiros

Parte do catálogo histórico nomeia **marcas e obras protegidas** (p.ex. bandas e artistas como Pink Floyd, David Bowie, Gorillaz, Misfits, Bring Me The Horizon, além de obras de Van Gogh e Frida Kahlo) aplicadas a estampas. Sem comprovação de licenciamento, a comercialização desses produtos pode configurar **risco jurídico de propriedade intelectual** (direitos autorais/marcas). Registra-se como ponto de atenção — é fato observado, não prova de ilícito, e independe da questão de idoneidade frente ao consumidor.

Leitura técnica. O conteúdo capturado descreve um e-commerce de moda **genuíno e em operação até recentemente**, que entrou em estado de pausa/congelamento. Não foram observados os artifícios de engenharia social típicos de loja-fantasma (contador zerado, falsa escassez, avaliações fabricadas, placeholders de template não preenchidos, geolocalização simulada).

8. Fluxo de Pagamento

O site é uma loja **Shopify**; o pagamento ocorre no **checkout hospedado pela própria Shopify**, e não por scripts proprietários no domínio. A configuração da loja declara moeda **BRL** (`"paymentSettings":{"currencyCode":"BRL"}`) e o histórico exibia bandeiras de cartão de crédito (ex.: American Express) entre os meios aceitos.

Aspecto	Observação
Plataforma de checkout	Shopify Checkout (intermediação regulada da plataforma).
Endpoints proprietários .php	Não identificados — não há servidor de pagamento próprio no domínio.
Chave PIX estática no código	Não identificada no conteúdo coletado.
Meios de pagamento	Cartão (bandeiras exibidas) via Shopify; eventual PIX, quando ativo, ocorreria dentro do checkout Shopify.
Moeda	BRL (Real brasileiro).

Leitura técnica. O uso do checkout Shopify é um **fator de proteção ao consumidor**: pagamentos com cartão dispõem dos mecanismos de contestação/estorno (chargeback) da bandeira, e a plataforma interpõe controles antifraude. Isso contrasta diretamente com o padrão de "PIX direto, sem gateway" característico de falsas lojas. **Importante:** esta análise não recebeu captura de tela de pagamento (pasta `pix/`) para este caso; portanto não houve decodificação de código PIX "copia e cola". Caso, com a loja pausada, surja qualquer cobrança PIX **fora** do checkout oficial da Shopify (por DM, WhatsApp ou link avulso), ela deve ser tratada com forte desconfiança e verificada antes de qualquer pagamento.

9. Indicadores de Risco e Fatores de Legitimidade

A tabela consolida os achados objetivos. Ao contrário de uma loja-fantasma, predominam **fatores de legitimidade**; os indicadores de risco concentram-se na **continuidade operacional** (loja pausada/congelada) e em um ponto jurídico acessório (uso de marcas de terceiros).

#	Indicador / fator	Evidência	Severidade
1	Loja atualmente inacessível (congelada na Shopify)	`HTTP 402 + página "loja indisponível"`	MÉDIA
2	Última comunicação: "vendas pausadas / reestruturação"	`Wayback 02/06/2026`	MÉDIA
3	Coleta de e-mails durante a pausa (sem previsão de retorno)	`Banner de newsletter no aviso`	BAIXA
4	Uso de marcas/obras de terceiros sem licença aparente	`Catálogo (bandas/artistas)`	BAIXA
5	Domínio antigo e renovado (~6,5 anos)	`RDAP — registro 2019; validade 2026`	LEGÍTIMO
6	CNPJ ATIVO e coincidente com o titular do domínio	`3BET Confecções Ltda — Receita`	LEGÍTIMO
7	Ramo (vestuário) e sede (Franca/SP) compatíveis	`CNAE 4781-4 · DDD 16 do WhatsApp`	LEGÍTIMO
8	Checkout regulado (Shopify) com cartão/estorno	`powered-by Shopify · BRL`	LEGÍTIMO
9	E-mail corporativo profissional (Google Workspace)	`MX Google + SPF`	LEGÍTIMO
10	Infraestrutura idônea (Cloudflare + Shopify)	`DNS/HTTP`	LEGÍTIMO

Síntese: nenhum indicador de severidade ALTA; 2 de severidade MÉDIA (continuidade da loja), 2 de severidade BAIXA e **6 fatores objetivos de legitimidade**. O perfil é o de um comerciante real cuja loja está temporariamente fora do ar, e não o de uma operação fraudulenta.

10. Conclusão Técnica

Com base nas evidências coletadas e preservadas em 03–04/06/2026, conclui-se que o sítio **stampit.com.br** corresponde a uma **loja virtual de identidade real e verificável** — a marca "Stamp It", operada pela empresa 3BET Comércio de Confecções do Vestuário Ltda (CNPJ ativo, Franca/SP), sobre a plataforma Shopify. Os indicadores clássicos de fraude (domínio descartável, hospedagem offshore incompatível, PIX direto sem gateway, CNPJ mascarado, placeholders de template, falsa escassez e avaliações fabricadas) **não foram constatados**.

O risco efetivo é de **natureza operacional e de continuidade**: na data da coleta a loja está congelada pela Shopify (HTTP 402) e a última comunicação pública informava pausa das vendas por reestruturação. Esse cenário **expõe a risco principalmente os consumidores com pedidos pagos e não entregues**, além de frustrar quem pretenda comprar no momento. Classifica-se o caso como **RISCO MODERADO**, com a ressalva de que tal classificação reflete **incerteza de cumprimento/continuidade**, e não imputação de golpe. Em acréscimo, registra-se ponto de atenção jurídica quanto ao uso de marcas e obras de terceiros nas estampas.

Ressalva metodológica: este laudo baseia-se em fontes abertas e na análise do conteúdo público e histórico do site nas datas indicadas. A classificação expressa um juízo técnico de risco e não substitui decisão de autoridade policial ou judicial, nem a verificação direta da situação de eventuais pedidos junto à empresa.

11. Recomendações

Para o consumidor / solicitante

- Se possui **pedido pago e não entregue**, reunir comprovantes (confirmação Shopify, e-mail, comprovante de pagamento) e contatar a empresa pelos canais oficiais (WhatsApp DDD 16 e e-mail divulgado).
- Pagamentos feitos com **cartão de crédito** podem ser contestados junto ao banco/bandeira (chargeback) caso o produto não seja entregue no prazo; pagamentos via **PIX**, acionar o banco e o **Mecanismo Especial de Devolução (MED)**.
- **Desconfiar de qualquer cobrança fora do checkout oficial da Shopify** — em especial chaves PIX ou links de pagamento enviados por DM/WhatsApp em nome da loja; confirmar antes de pagar.
- Antes de comprar, verificar se a loja **voltou ao ar** (deixou de responder com "loja indisponível") e preferir o pagamento com cartão, que oferece estorno.
- Em caso de prejuízo, registrar reclamação no **consumidor.gov.br** e, se necessário, Boletim de Ocorrência, além de acionar os órgãos de defesa do consumidor (Procon).

Observações para diligência adicional

- Confirmar diretamente com a empresa (CNPJ 21.775.785/0001-44) a **situação dos pedidos em aberto** e a previsão de retorno das vendas.
- Acompanhar a reativação (ou não) da loja Shopify; a permanência prolongada no estado "loja indisponível" eleva o risco de não cumprimento de pedidos pendentes.
- Quanto às estampas de marcas/obras de terceiros, eventual interessado (titulares de direitos) pode avaliar a regularidade do licenciamento — ponto jurídico autônomo, alheio à relação de consumo.

Não se recomenda, com base nas evidências, tratar a loja como fraude consumada. As cautelas acima visam proteger o consumidor diante da **incerteza de continuidade** identificada.

Anexo A — Manifesto de Integridade das Evidências

Os arquivos abaixo foram preservados na subpasta `evidencias/` e seus resumos criptográficos (SHA-256) foram calculados no momento da coleta. Qualquer alteração posterior de um arquivo modificará seu hash, permitindo a detecção. O manifesto também está salvo em texto em `evidencias/hash_manifest.txt`.

Arquivo	SHA-256
cnpj_brasilapi.json	55d6e49d075134abdb7e633f61b42fd4f413e425013e85fc4dce752fdf4309e2
corpo_http80.html	446a6087825fa73eadb045e5a2e9e2adf7df241b571228187728191d961dda1f
corpo_https.html	13a703af685815b3897c9ec4d23752d2416b4eb850e3f93909fa9daebcf30236
dns_records.txt	d70cc0cf4489e0924b090f1468f12fd6be8ce2275d0d877bc97371d63e2aac2c
headers_http80.txt	65f4bba13f67999edea7ab5de6e6e85916f7367b7ff4f239c279367d9c590ca4
headers_https.txt	9baac4e39e5e47280f2378a3934d95dac2f34872e9aca03cd834966dbe9c64fd
ipapi_104.21.52.30.json	3b06be401e79fb64e58dba02b76f9cb45696f18b93a81dc3e053c7cadba765c2
ipinfo_104.21.52.30.json	1fe1096c55a853d034e735d2f236a4d33c5f68a2af78aabfca71338dacbc2946
rdap_raw.json	2d33dd784d18c59b0497f48fd257e7cf98c8c20a24a34d2ff9cbda207890aa63
ssl_cert.txt	0aab170969bd7cb19ff1860bec5425dba16276fcbb40390c66d8c1a7e93e7c62
ssl_raw.txt	ec8fc6a9dc22c0d6139df63560d6e6a46213386eac6417e95d3f8f62a323e0af
wayback_2025-10-07_loja_ativa.html	e896da50551096b58fd9126582232e1b4e16691b1bebba4f0826d260eaf6f279
wayback_2026-06-02_aviso_pausa.html	63e59ed7a2bea40078b8fd9a1aeb4e672ce173ff087051ee60a0381c07796a45

Coleta realizada em 03–04/06/2026 (RDAP/DNS/HTTP/TLS, consulta de CNPJ e capturas do arquivo histórico Wayback Machine). Algoritmo de verificação: SHA-256. Comando sugerido: `sha256sum -c hash_manifest.txt` (executado dentro da pasta evidencias/).

— Fim do relatório —

Documento gerado por Dono do Site — OSINT & Investigação Digital · Relatório técnico baseado em dados públicos e análise de conteúdo aberto.