RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, forense e de risco de fraude do domínio

cpxcapitalltda.com

Objeto investigado	cpxcapitalltda.com — apresenta-se como "Cpx Capital LTDA" (suposto operador de câmbio)
Natureza	Verificação de legitimidade / suspeita de fraude financeira (câmbio / FX / renegociação de dívida)
Estado do alvo	Atualmente em parking GoDaddy (página /lander com AdSense for Domains). Identidades comerciais anteriores reconstruídas por OSINT.
Data da coleta	21/05/2026 — 05:15 a 05:55 UTC (02:15–02:55 BRT)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · Certificate Transparency · urlscan.io (5 capturas históricas)
Emissão do laudo	21/05/2026 às 02:55

1. Sumário Executivo

Este relatório documenta a investigação técnica do domínio **cpxcapitalltda.com**, cuja denominação ("Capital LTDA") sugere uma pessoa jurídica brasileira atuante no setor financeiro. A coleta foi realizada em 21/05/2026 por meio de técnicas de OSINT (inteligência de fontes abertas) e análise forense passiva.

Na data da coleta, o domínio responde com a **página padrão de domain parking da GoDaddy** (`LANDER_SYSTEM=PW`, cookie `lander_type=parkweb`) — monetizando o domínio inativo via Google AdSense for Domains. Porém, a reconstrução do histórico do domínio a partir de Certificate Transparency e capturas preservadas pelo urlscan.io demonstra que, entre outubro e dezembro de 2025, ele **serviu ativamente dois sites distintos** com identidades comerciais incompatíveis entre si:

Período	Identidade exibida no site	Indícios visuais
08/10/2025	**"Cpx Capital LTDA"** — suposto operador de câmbio	Background com gráfico de notas de dólar; serviços de "Câmbio Comercial / Câmbio Financeiro"; telefone +55 (11) 3522-7002; e-mail `atendimento@cpxcapitalltda.com`.
13–14/12/2025	**Mockup com marca "ATIVOS S.A." + selo "Recovery"** — propaganda de renegociação de dívidas	Texto: "Negocie sua dívida com até 99% de desconto" / "Sua vida financeira não pode parar". Marcas reconhecíveis (Ativos S.A. — subsidiária do Banco do Brasil; Recovery do Brasil S.A.).
Atual (21/05/2026)	Página de parking da GoDaddy	Sem identidade comercial; monetização passiva via AdSense.

CLASSIFICAÇÃO DE RISCO **ALTO RISCO DE FRAUDE FINANCEIRA**

A coexistência de uma operação anunciada de **câmbio** com a inserção, dois meses depois, de elementos visuais de **marcas reais de recuperação de crédito** (Ativos S.A., Recovery), aliada à titularidade redigida por privacidade, ao prazo mínimo de registro (1 ano) e à reversão atual para parking, compõe o perfil de uma **infraestrutura de fraude descartável e adaptável**. Nenhum operador de câmbio autorizado pelo Banco Central usaria um nome de domínio anonimamente registrado em registrar norte-americano. Recomenda-se enfaticamente **não realizar pagamentos, transferências, ou compartilhar dados pessoais** em qualquer reativação futura deste domínio.

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 valor de resumo criptográfico (hash SHA-256) calculado. Nenhuma técnica intrusiva foi empregada — apenas requisições equivalentes às de um visitante comum e consultas a bases públicas (RDAP, DNS, Certificate Transparency e capturas históricas preservadas em urlscan.io).

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP — Verisign (operador .com)	`rdap_verisign.json`
Infraestrutura DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns.txt`
Cabeçalhos HTTP (root)	curl — HTTPS e HTTP/80	`headers_https.txt`, `headers_http80.txt`
Conteúdo servido (root + lander)	Captura do HTML servido	`corpo_https.html`, `corpo_http80.html`, `corpo_lander.html`, `headers_lander.txt`
Certificado TLS atual	openssl s_client / x509	`tls_cert_summary.txt`, `tls_handshake.txt`

Geolocalização dos IPs	ipinfo.io, ip-api.com, PTR	`geo_ips.txt`
Histórico TLS	crt.sh (Certificate Transparency)	`crtsh.json`
Capturas históricas	urlscan.io (5 scans em 2025-10 a 2025-12)	`urlscan_search.json`, `urlscan_*.html`, `imagens/urlscan_*.png`
Snapshots de arquivamento	Internet Archive (Wayback) — CDX e Available APIs	`wayback_cdx.json`, `wayback_available.json`
Verificação de marcas concorrentes	Acesso direto a ativos.com.br, ativossa.com.br, recovery.com.br	`ativos_real_root.html`, `ativossa_real_root.html`, `recovery_real_root.html`
Reconstrução cronológica	Síntese dos eventos extraídos das fontes acima	`cronologia.txt`

Todos os artefatos estão na pasta **evidencias/** (mídias em **imagens/**) e seus hashes constam do Anexo A. Fuso de referência: UTC; conversões para BRT (UTC–3) são indicadas quando aplicável.

3. Identificação do Domínio (RDAP)

Os dados a seguir foram obtidos junto ao operador do registro do TLD **.com** (Verisign) pelo protocolo RDAP. Sob política da ICANN para gTLDs, os dados do titular ("registrant") são **redigidos por privacidade**, impedindo a identificação direta do responsável a partir do RDAP público.

Domínio	CPXCAPITALLTDA.COM
Handle Verisign	3026712203_DOMAIN_COM-VRSN
Data de registro	07/10/2025 16:57:52 UTC — **~7 meses na data da coleta**
Data de expiração	07/10/2026 — período mínimo de 1 ano
Última alteração	28/01/2026 20:20:27 UTC — coincide com novo certificado TLS (Seção 6)
Status EPP	client delete prohibited · client renew prohibited · client transfer prohibited · client update prohibited
Significado	Travas defensivas padrão aplicadas pelo registrar GoDaddy a todos os seus domínios — **não são**, neste caso, sanções por abuso. Não há "client hold".
Registrar	**GoDaddy.com, LLC** — IANA Registrar ID 146 (Scottsdale, Arizona, EUA)
Contato de abuso do registrar	abuse@godaddy.com · +1-480-624-2505
Servidores de nome	NS03.DOMAINCONTROL.COM · NS04.DOMAINCONTROL.COM (GoDaddy)
Titular (Registrant)	Redigido por política de privacidade (gTLD ICANN)
DNSSEC	Não assinado (delegationSigned: false)

Leitura técnica. O domínio foi registrado pelo prazo mínimo (1 ano), em registrar internacional e sob proteção de privacidade. O nome inclui o sufixo "ltda" (Sociedade Limitada) — forma jurídica brasileira — mas a contratação foi feita em registrar dos EUA com pagamento internacional em dólar. Não há razão operacional para uma pessoa jurídica brasileira de câmbio (regulada pelo Banco Central) registrar seu domínio sob anonimato em GoDaddy.com: empresas legítimas costumam usar o TLD `.com.br` (que exige CNPJ visível) ou o `.com` com WHOIS público.

4. Infraestrutura de DNS

Registro	Valor	Observação
A	`3.33.130.190 · 15.197.148.33`	Endereços anycast AWS Global Accelerator usados pela hospedagem GoDaddy.
AAAA	— (ausente)	Sem IPv6.
NS	`ns03.domaincontrol.com · ns04.domaincontrol.com`	DNS gerenciado pela GoDaddy (domaincontrol.com).
MX	`0 smtp.secureserver.net · 10 mailstore1.secureserver.net`	E-mail também na infraestrutura GoDaddy/Secure Server — **caixa "atendimento@" anunciada no site capturado pode ter sido operacional**.
TXT (SPF)	`v=spf1 include:secureserver.net -all`	SPF restritivo, autoriza apenas a infraestrutura GoDaddy a enviar pelo domínio.
SOA	`ns03.domaincontrol.com · dns.jomax.net · serial 2026050402`	Última atualização da zona em 04/05/2026 — DNS continua ativo.
www	`CNAME → cpxcapitalltda.com`	Apex e www unificados.

Leitura técnica. Toda a pilha (DNS, web, e-mail) opera nas infraestruturas GoDaddy — configuração típica de cliente que contratou o "Websites + Marketing" (W+M), construtor visual de sites da GoDaddy. A SOA foi reatualizada em 04/05/2026, o que indica

gerenciamento ativo da zona ainda em 2026 (apesar de o conteúdo ter caído para parking). O domínio dispõe de MX próprio: a caixa `atendimento@cpxcapitalltda.com` exibida em outubro provavelmente foi efetivamente operacional naquele período.

5. Hospedagem e Geolocalização do Servidor

IPs A	3.33.130.190 · 15.197.148.33 (anycast)
Sistema autônomo	AS16509 — Amazon.com, Inc.
Tipo	AWS Global Accelerator (anycast global; cliente final: GoDaddy)
Hostname (PTR comum)	a2aa9ff50de748dbe.awsglobalaccelerator.com
Plataforma inferida	GoDaddy Websites + Marketing (construtor visual) — confirmada pelo redirecionamento atual `/lander` ("LANDER_SYSTEM=PW") e pelo cookie `lander_type=parkweb`
Servidor web	openresty (na rota /lander); na raiz, resposta minimalista 114 bytes com redirect JavaScript
Países detectados	EUA (ipinfo: Seattle) · CA (ip-api: Montreal) — Anycast: a localização efetiva depende do nó AWS mais próximo do consumidor; para o Brasil, tende a roteamento via São Paulo (sa-east-1) ou Rio (sa-east-2).

Postura quanto a provedores de infraestrutura. AWS e GoDaddy são provedores estabelecidos amplamente utilizados por clientes legítimos. O fato de o domínio ter operado sobre essa infraestrutura não imputa, isoladamente, conduta ilícita aos provedores. O registro factual é: o domínio foi contratado na GoDaddy e hospedado em sua plataforma W+M, com fronting AWS Global Accelerator.

6. Certificado TLS / HTTPS e Histórico via Certificate Transparency

6.1. Certificado vigente no momento da coleta

Titular (Subject)	CN = cpxcapitalltda.com
Emissor (Issuer)	C=US · O=GoDaddy.com, Inc. · OU=http://certs.godaddy.com/repository/ · CN=Go Daddy Secure Certificate Authority - G2
Tipo de validação	DV — Domain Validation (GoDaddy automatizado, padrão da plataforma W+M)
Válido de	28/01/2026 20:51:55 UTC
Válido até	14/08/2026 20:51:55 UTC
Número de série	47359CC7B0C4144C
Fingerprint SHA-256	CF:45:5F:0B:11:5F:F4:E9:EC:28:68:E0:42:31:C6:90:19:F6:F0:9A:E7:42:90:BC:59:44:6B:93:98:BA:93:7A

6.2. Histórico de emissões (crt.sh)

A consulta a Certificate Transparency revelou um **padrão atípico de cinco emissões em ~6 meses**, todas pela autoridade GoDaddy CA G2 — sugerindo intervenções recorrentes de configuração:

#	Emitido em (UTC)	Válido até	Contexto
1	`07/10/2025 17:20`	`05/01/2026`	~23 min após o registro do domínio — ativação inicial do site.
2	`07/12/2025 10:38`	`07/03/2026`	Renovação automática (~60 dias após emissão #1).
3	`28/01/2026 20:51`	`14/08/2026`	Novo cert (válido por ~6,5 meses) — coincide com "last changed" no RDAP. Provável troca de plano/configuração.
4	`29/01/2026 13:33`	`29/04/2026`	Outro cert ~17h depois do #3 — possível republicação do site.

5	31/03/2026 03:38	29/06/2026	Última renovação registrada no CT.

Leitura técnica. O certificado em uso é legítimo do ponto de vista criptográfico, mas é um DV gratuito (incluso no plano GoDaddy W+M) que **não atesta identidade da empresa**. A multiplicidade de emissões em curto intervalo, particularmente as emissões #3 e #4 separadas por menos de 24h, é compatível com troca/reedição de conteúdo do site — corroborando a transformação observada nas capturas urlscan entre outubro e dezembro de 2025.

7. Análise do Conteúdo da Página

7.1. Estado atual (21/05/2026) — parking GoDaddy

A requisição HTTP/HTTPS ao endereço raiz retorna um documento mínimo (114 bytes) que apenas redireciona para `/lander` via JavaScript. A rota `/lander` é o aplicativo SPA de parking da GoDaddy ("parkweb"), monetizando o domínio com anúncios contextuais via **Google AdSense for Domains** (script `caf.js`).

Cookies emitidos pelo /lander confirmam o sistema: `traffic_target=gd`, `lander_type=parkweb`, `country=BR` (a geo-detecção identificou o solicitante como Brasil).

7.2. Identidade #1 — "Cpx Capital LTDA" (08/10/2025)

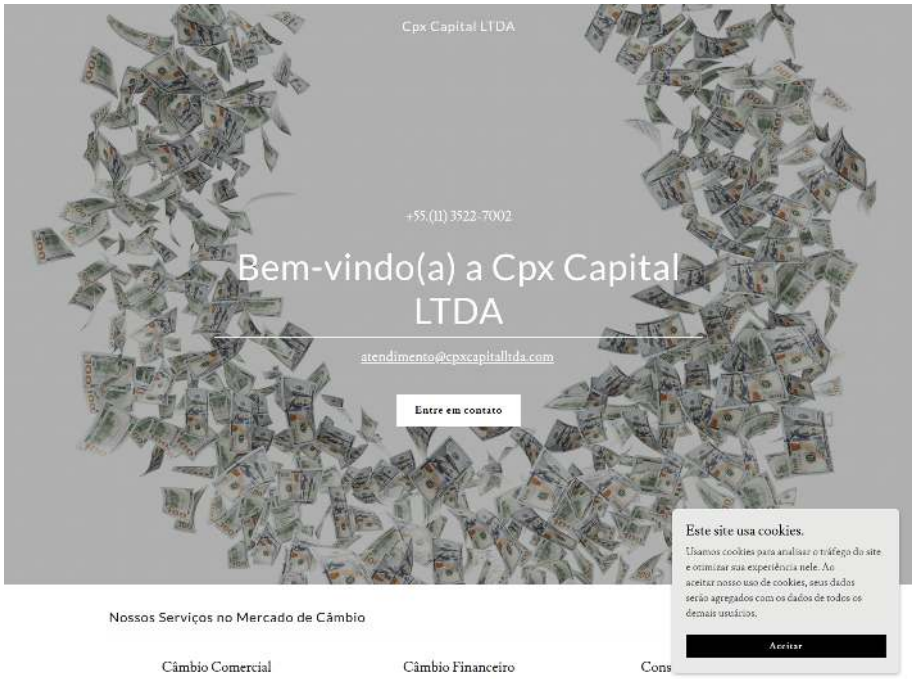

Figura 1 — Captura urlscan UUID 0199c3cf, 08/10/2025 12:32 UTC. Site apresentado como agência de câmbio "Cpx Capital LTDA", com background de notas de dólar.

Conteúdo observado na captura: marca **"Cpx Capital LTDA"**; saudação "Bem-vindo(a) a Cpx Capital LTDA"; telefone **+55 (11) 3522-7002**; e-mail **atendimento@cpxcapitalltda.com**; secção "Nossos Serviços no Mercado de Câmbio" com itens "Câmbio Comercial", "Câmbio Financeiro" e "Cons[ultoria]" (truncado). O background visual é o clichê visual recorrente em fraudes de FX/investimentos: gráfico circular de notas de dólar dos EUA.

7.3. Identidade #2 — Mockup "Ativos S.A. / Recovery" (13–14/12/2025)

Figura 2 — Captura urlscan UUID 019b15f3, 13/12/2025 04:23 UTC. Mesma URL (cpxcapitalltda.com), porém exibindo agora propaganda de renegociação de dívida com mockup de aplicativo "ATIVOS S.A." e selo "Recovery".

Cerca de dois meses após a primeira identidade, o site passou a exibir conteúdo completamente diferente: **"Negocie sua dívida com até 99% de desconto"** / **"Sua vida financeira não pode parar"**. A imagem central é um mockup de celular cujo aplicativo, na própria tela, ostenta a marca **"ATIVOS S.A."** e, ao pé, o selo **"Recovery"**. A inserção de marcas registradas reais nesse mockup é especialmente relevante:

Marca exibida	Empresa real correspondente
"ATIVOS S.A."	**Ativos S.A. Securitizadora de Créditos Financeiros** — subsidiária do **Banco do Brasil**, domínio oficial `ativossa.com.br` (redireciona a `portal.ativosbb.com.br`).
"Recovery"	**Recovery do Brasil S.A.** — gestora de carteiras de dívida; opera o domínio `recovery.com.br`.

Leitura técnica. O domínio `cpxcapitalltda.com` não tem qualquer relação societária ou comercial publicamente verificável com Ativos S.A. (BB) ou Recovery do Brasil. O reaproveitamento desses elementos visuais — em um domínio anonimamente registrado — configura, em tese, **uso indevido de marca** e indício de operação fraudulenta de "renegociação de dívidas" (modalidade conhecida em que falsos "negociadores" cobram pagamentos sob promessa de quitar dívidas em nome do consumidor, sem nunca repassar os valores).

8. Análise do Fluxo de Pagamento

Não foi possível realizar análise direta do código JavaScript ou do fluxo de pagamento das duas identidades comerciais, pois o site não está mais ativo na coleta. A inspeção do JS atualmente servido (`/lander/main.be9a3b28.js`) confirma tratar-se exclusivamente do SPA de parking da GoDaddy, sem qualquer rotina de captação de pagamento ou de dados pessoais — apenas o carregamento do script `caf.js` de AdSense for Domains.

Em **operações de câmbio fraudulentas**, o esquema mais comum é a oferta de cotações de compra/venda de moeda estrangeira ligeiramente melhores que as oficiais; o consumidor é induzido a transferir reais (por TED ou PIX) para uma conta apresentada como "da Cpx Capital", após o que a moeda nunca é entregue. Em **operações falsas de renegociação de dívida**, o esquema padrão envolve a cobrança de boletos ou PIX a título de "taxa de regularização" / "quitação antecipada", sem que a dívida real seja paga.

Leitura técnica. Esta seção é mantida como **informativa**: não há dados capturados sobre o fluxo de pagamento específico deste domínio. Caso o solicitante possua prints da etapa de pagamento (comprovantes PIX/TED, e-mails de cobrança, contratos digitais),

recomenda-se aditar o laudo conforme o adendo descrito em `docs/prompt_investigacao.md` (decodificação EMV/BR Code do código PIX e identificação do recebedor real).

9. Indicadores de Fraude (IoF)

A tabela consolida os indicadores objetivamente identificáveis. Cada indicador é classificado pela sua severidade isolada; a **convergência** sustenta a classificação de risco.

#	Indicador	Evidência observada	Severidade
1	Domínio recém-registrado	07/10/2025 (~7 meses); prazo mínimo (1 ano)	ALTA
2	Titular redigido por privacidade em registrar estrangeiro	GoDaddy.com (Arizona/EUA); WHOIS/RDAP sem dados de pessoa jurídica	ALTA
3	Operação financeira anunciada (câmbio/FX) sem registro BCB visível	Domínio anonimato em .com — incompatível com operador de câmbio autorizado pelo Banco Central	ALTA
4	Duas identidades comerciais incompatíveis no mesmo domínio	Cpx Capital (out/2025) → "Ativos S.A. / Recovery" (dez/2025) — capturas urlscan	ALTA
5	Uso aparente de marcas reais ("Ativos S.A.", "Recovery") sem vínculo	Mockup das telas em capturas de dez/2025	ALTA
6	Padrão visual associado a fraudes financeiras	Background de notas de dólar (identidade #1)	MÉDIA
7	Certificado TLS DV gratuito, com reedições frequentes	5 emissões GoDaddy em ~6 meses; troca em 28-29/01 separada por <24h	MÉDIA
8	Site descontinuado e revertido para parking pago	Atual lander parkweb com AdSense for Domains	MÉDIA
9	Hospedagem em plataforma de site builder (W+M)	GoDaddy W+M sobre AWS Global Accelerator — montagem em minutos	BAIXA
10	DNSSEC desativado	delegationSigned: false	BAIXA
11	Ausência total de snapshots no Internet Archive	Wayback / archived_snapshots: {} — domínio passou despercebido pelos crawlers do IA	MÉDIA

Síntese: **5 indicadores de severidade ALTA**, 4 de severidade MÉDIA e 2 de severidade BAIXA. A convergência — em especial, a combinação de (a) operação financeira anunciada sem identidade real, (b) duas fachadas incompatíveis no mesmo endereço e (c) uso aparente de marcas de terceiros — é praticamente conclusiva para o perfil de domínio fraudulento adaptável.

10. Conclusão Técnica

Com base nas evidências coletadas e preservadas em 21/05/2026, conclui-se que o domínio **cpxcapitalltda.com** apresenta **alto risco de fraude financeira**. O domínio foi registrado em 07/10/2025 sob proteção de privacidade em registrar estadunidense, ativado em minutos sobre a plataforma GoDaddy Websites + Marketing, e operado em **duas identidades comerciais distintas e inconsistentes** em apenas dois meses: primeiro como suposta agência de câmbio "Cpx Capital LTDA"; depois como propaganda de renegociação de dívidas com inserção de elementos visuais associados a marcas reais (Ativos S.A. / Recovery do Brasil), sem qualquer vínculo societário publicamente verificável com essas empresas. O domínio encontra-se, na data desta coleta, em estado de parking pago (GoDaddy + AdSense for Domains) — comportamento típico de infraestrutura mantida para reativação futura.

Nenhum operador de câmbio autorizado pelo Banco Central do Brasil utilizaria registro anônimo em registrar estrangeiro, e nenhuma operação legítima de recuperação de crédito utilizaria, em seu site institucional, mockups com marcas de terceiros sem licenciamento explícito. A análise do conteúdo, reconstruída por capturas preservadas pelo urlscan.io (cinco scans entre 08/10/2025 e 14/12/2025), é consistente com o padrão de **infraestrutura de fraude descartável e adaptável**, em que um mesmo domínio é reutilizado para

diferentes campanhas conforme a oportunidade.

Ressalva metodológica: este laudo baseia-se exclusivamente em fontes abertas. A classificação expressa um juízo técnico de risco e não substitui decisão de autoridade policial, judicial ou regulatória (Banco Central, CVM, Procon).

11. Recomendações

Para quem foi vítima ou potencial vítima

- **Não realizar pagamentos**, transferências TED/PIX ou compras de moeda estrangeira por meio deste domínio, mesmo que ele volte ao ar com nova interface ou nome.
- Caso já tenha sido feito pagamento PIX: acionar imediatamente o banco e solicitar o **Mecanismo Especial de Devolução (MED)** (prazo decadencial de 80 dias). Para TED, registrar contestação formal.
- Se houve transferência sob promessa de "renegociação de dívida": **desconfiar de qualquer cobrança** que não tenha sido feita pelo canal oficial do credor original. Empresas reais (Ativos S.A. / Recovery do Brasil) não cobram taxas antecipadas para "liberar" descontos.
- **Registrar Boletim de Ocorrência** e reunir todas as evidências (prints do anúncio que levou ao site, prints do site, comprovantes de pagamento, conversas de WhatsApp/e-mail).
- Denunciar no **consumidor.gov.br** indicando o domínio `cpxcapitalltda.com`. Para suspeita de operação de câmbio sem autorização, comunicar ao **Banco Central do Brasil** (canal Atende BC). Para uso indevido de marca, comunicar a **Ativos S.A. (BB)** e a **Recovery do Brasil**.

Para responsáveis técnicos / takedown

- Reportar abuso ao registrar **GoDaddy.com, LLC** (`abuse@godaddy.com`), anexando este laudo, as três capturas de tela e o histórico de Certificate Transparency. Solicitar a suspensão preventiva do domínio (similar ao client hold) caso seja reativado.
- Para os titulares das marcas (Ativos S.A. e Recovery do Brasil): considerar procedimento **UDRP** (Uniform Domain-Name Dispute-Resolution Policy) junto à WIPO para apreensão do nome de domínio, dado o evidente uso indevido das marcas.
- Solicitar ao Google a remoção do AdSense for Domains deste domínio — atualmente o esquema de parking gera receita publicitária diretamente para o titular anônimo, mesmo após o desligamento do conteúdo fraudulento.
- Monitorar reativações: configurar alertas em crt.sh para novos certificados emitidos para `cpxcapitalltda.com` e variantes léxicas (`cpx*`, `cpxcapital*`) — uma nova emissão TLS é o primeiro sinal técnico de reativação do site.

Anexo A — Manifesto de Integridade das Evidências

Os arquivos abaixo foram preservados nas pastas `evidencias/` e `imagens/` 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 `evidencias/hash_manifest.txt`.

Arquivo	SHA-256
evidencias/ativos_real_root.html	ec92a4de6bae52554e40aba82c7470536e11c1a6443a5c337eeb8a58e715298c
evidencias/ativossa_real_root.html	e1eef8b34e5329ad452b8303a4fb066319d1304ab8a70318c63dca3f3338cfef
evidencias/corpo_http80.html	6dc9c7fc93bb488bb0520a6c780a8d3c0fb5486a4711aca49b4c53fac7393023
evidencias/corpo_https.html	6dc9c7fc93bb488bb0520a6c780a8d3c0fb5486a4711aca49b4c53fac7393023
evidencias/corpo_lander.html	29efffb7c52fea1b45a616ec33a6d0b0ff171cb3c334b193ea5178975a31ee2f
evidencias/cronologia.txt	0232e918909d836b803bbddba583d0bd9acb7615a7d1e037d5dc3f7ac77d8760
evidencias/crtsh.json	dc888bce77fdb033bb4677aa0c27b09a6115fa52f8f4e5d622cc7651d95f96b7
evidencias/dns.txt	6d585984f562c35f89c7f837f6519153df70e93d795bf8f3f3f5c8f55657d5e6
evidencias/geo_ips.txt	a968afc3b62402a7344633ce4251fd42a9e368a1aa0b4669b25bc163202269c5
evidencias/hash_manifest.txt	4a6f412147c4d53908782b2c8af49ff87b7e5ac8bb7a612ad520fd3f0552bda6
evidencias/headers_http80.txt	e4269ba8382df59a639b64db70b2b77aacfebcf81e5d3b830519d8570b6e8b2d
evidencias/headers_https.txt	7407a11530754b36d9f7e9552c9ccc63fb33aabea538d4efb965d15aeb29d4ed
evidencias/headers_lander.txt	90650539984d70a928441ddf47ca5dd004f9bb4c3cdd7ae66a4ac07fc99ae460
evidencias/rdap_verisign.json	e3faefacddf14d0db7bd091bbb915f5b3283fc539b409074959016b8b468a1ce
evidencias/recovery_real_root.html	80a265bed528211aa708dcd58f7a95db36eeb7f873c6fe4ddab0b3a1dc0973a4
evidencias/tls_cert_summary.txt	7b765301c944e099d446eb74373f1268ec6f8f87bd20caf4feb3ec6cbc2a733b
evidencias/tls_handshake.txt	de65298583cc5b72cc2314031bf4058e25d0cea7c397579622d02298ec75a707
evidencias/urlscan_0199c3cf-2087-7074-997b-b3324c91ed6a.html	36364fb476f388afe990c8a693d94a893ba84bd80f3e87603cf24590b7bb6033
evidencias/urlscan_019b15f3-3384-7580-bab4-5272aa1b692a.html	f8ac7caedc180eb1ea87c67f1211bda0b4410ec301434fe7c17bd6abfc9b8dc3
evidencias/urlscan_019b1bd7-761c-73ad-a313-040f87b4312a.html	7bb516fdf0a356e181e34984211eee066bb512d5e7f41a581bf367dcc82595a7

evidencias/urlscan_result.json	86e91e6c8ac39ebad1fa2b5ad4b38073fbd5b832891acf93cedf409adc2e0a5d
evidencias/urlscan_search.json	b28ffe100f29aba0a9b142ce105472607eef922f8f24b339d837d38de64045b4
evidencias/wayback_available.json	afa757b45d464d97352721b827ec130763ebea90ff375e255a23bdec432dba57
evidencias/wayback_cdx.json	37517e5f3dc66819f61f5a7bb8ace1921282415f10551d2defa5c3eb0985b570
imagens/metadata_exiftool.txt	53467aff8b1c24b5c71d09fb909152c12d91dc5e9fe6006586c545e61ad88bb1
imagens/urlscan_0199c3cf-2087-7074-997b-b3324c91ed6a.png	dbd5ec13321d3965d6468e45a54b2e2eea1adad318e70b4159ef541252f71e1d
imagens/urlscan_019b15f3-3384-7580-bab4-5272aa1b692a.png	934289c5be1f99be12e4da073c0267b1f81b7077e4d224ecf42a906375b37749
imagens/urlscan_019b1bd7-761c-73ad-a313-040f87b4312a.png	bd185ff008be99ead8682229c701a099e2156c0be63d6c2f83ee3f0c017b0a78

Coleta principal realizada em 21/05/2026, ~05:15–05:55 UTC. Capturas urlscan.io referem-se a scans públicos preservados por terceiros entre 08/10/2025 e 14/12/2025. Algoritmo: SHA-256. Comando de verificação sugerido: `sha256sum -c hash_manifest.txt` (a partir do diretório raiz da investigação, após ajustar o cabeçalho do arquivo).

— Fim do relatório —

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