RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, forense e de risco do domínio

stsuper.com.br

Objeto investigado	stsuper.com.br (domínio .br recém-registrado)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	06/06/2026 (RDAP, DNS, transparência de certificados e arquivo histórico)
Métodos	OSINT passivo · RDAP · DNS · crt.sh · Wayback Machine
Estado na coleta	Domínio SEM site ativo (não resolve para IP)
Emissão do laudo	06/06/2026 às 02:34

1. Sumário Executivo

Este relatório documenta a investigação técnica do domínio **stsuper.com.br**, submetido a análise como sítio potencialmente suspeito. A coleta foi realizada em **06/06/2026** por meio de técnicas de OSINT (inteligência de fontes abertas) e análise passiva, sem qualquer interação intrusiva com a infraestrutura-alvo.

O achado central, e que condiciona todo o laudo, é que **o domínio não possui site ativo no momento da coleta**. Embora esteja registrado e delegado a servidores de nome da UOL, a zona **não publica qualquer registro de endereço (A/AAAA)**: o domínio não resolve para nenhum IP, não há serviço HTTP/HTTPS no ar, não existe certificado TLS emitido (verificado por transparência de certificados — crt.sh) e não há qualquer captura histórica no Internet Archive (Wayback Machine). Em consequência, **não houve conteúdo, código de pagamento, JavaScript ou imagens a analisar** — não por limitação de método, mas por inexistência de alvo público.

Por outro lado, o registro **.br** revela uma identidade não anônima: o domínio foi registrado em **02/06/2026** (quatro dias antes da coleta) por meio do registrador **UOLHOST**, em nome de uma **pessoa física identificada** — Ronaldo Ceurim Martins —, com CPF parcialmente exibido pelo Registro.br (redação automática por privacidade) e e-mail de contato em provedor UOL. Trata-se, portanto, de um **domínio recém-adquirido e ainda não colocado no ar**.

CLASSIFICAÇÃO DE RISCO	NÃO DETERMINADO — SITE INATIVO

Leitura: **não é possível classificar a loja como fraudulenta nem como legítima**, porque não há serviço no ar para avaliar. O único indicador de fraude objetivamente presente é a **idade mínima do domínio (quatro dias)**; os demais — pagamento só por PIX, falsa escassez, avaliações fabricadas, placeholders de template etc. — **não são avaliáveis** na ausência de conteúdo. Recomenda-se **não realizar pagamentos** enquanto não houver site público verificável e **reavaliar o domínio caso ele entre no ar** (ver Seções 9 a 11).

2. Metodologia e Cadeia de Custódia

A investigação seguiu o princípio da **preservação probatória**: todas as respostas de rede e de bases públicas 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 do Registro.br, DNS, a base de transparência de certificados crt.sh e o arquivo histórico Wayback Machine).

Registra-se uma **condição de coleta**: o resolvedor DNS local da estação estava indisponível (timeout); por isso as consultas de DNS foram realizadas por meio dos resolvedores públicos **1.1.1.1** (Cloudflare) e **8.8.8.8** (Google) e junto aos servidores autoritativos da UOL. Os serviços crt.sh e Wayback apresentaram instabilidade momentânea, tendo as consultas sido repetidas até a obtenção de resposta conclusiva.

Etapa	Técnica / ferramenta	Evidência preservada
Registro do domínio	RDAP — Registro.br (.br)	`rdap_raw.json`
Infraestrutura DNS	Consultas dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_records.txt`
Certificados TLS emitidos	Transparência de certificados (crt.sh)	`crtsh.json`
Histórico do site	Internet Archive (Wayback Machine — CDX)	`wayback_cdx.json`
Condições e ausências	Registro das tentativas de HTTP/TLS/IP (sem alvo)	`coleta_notas.txt`

Todos os artefatos estão na subpasta **evidencias/** e seus hashes constam do Anexo A (Manifesto de Integridade). O fuso 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 o nome do titular, o que permitiu a identificação direta do responsável — ainda que o número do documento (CPF) seja exibido de forma parcialmente redigida por força da legislação de proteção de dados.

Domínio	stsuper.com.br
Data de registro	**02/06/2026 03:01:26 UTC**
Última alteração	02/06/2026 03:01:26 UTC
Data de expiração	02/06/2027 03:01:26 UTC
Idade do domínio	**~4 dias** na data da coleta — domínio recém-registrado
Titular / Registrant	RONALDO CEURIM MARTINS (pessoa física)
Documento (CPF)	***.884.773-** (redigido pelo Registro.br por privacidade)
Contatos (adm./téc.)	Ronaldo Ceurim Martins · ronaldoceurimmartins@uol.com.br
Handle do contato	ROCMA1009
Registrador (Registrar)	UOLHOST (provedor p22)
DNSSEC	Não assinado
Servidores de nome	ns1 · ns2 · ns3.dominios.uol.com.br
Status	active

Leitura técnica. A **idade mínima do domínio** — registrado há apenas quatro dias — é, isoladamente, o indicador de risco mais relevante deste caso: domínios de pouquíssimas semanas são frequentemente associados a operações efêmeras. Em sentido contrário, e como fator que **reduz** o anonimato, o titular é uma **pessoa física nominalmente identificada**, com contato em provedor conhecido (UOL) e via um registrador nacional estabelecido (UOLHOST) — perfil distinto do registro anônimo via privacidade em TLDs estrangeiros. Observa-se ainda que o registro está em nome de **pessoa física (CPF)**, e não de pessoa jurídica (CNPJ); a redação parcial do CPF é o comportamento padrão do Registro.br e **não** configura, por si, o indicador de "CNPJ mascarado/não verificável".

4. Infraestrutura de DNS

A zona está delegada aos servidores de nome da **UOL** (uolhost), mas **não publica registros de endereço**. As consultas A e AAAA retornam resposta sem respostas (apenas o registro SOA da zona), o que significa que o domínio **não aponta para nenhum servidor web**. Também não há registros MX (e-mail) nem TXT (SPF/verificações). É a configuração típica de um domínio **recém-registrado e ainda não publicado** (estacionado/em pré-lançamento).

Registro	Valor	Observação
A	`— (sem resposta)`	Domínio não resolve para IPv4
AAAA	`— (sem resposta)`	Sem IPv6
NS	`ns1 / ns2 / ns3.dominios.uol.com.br`	DNS gerenciado pela UOL (uolhost)
MX	`— (sem resposta)`	Sem e-mail configurado para o domínio
TXT / SPF	`— (sem resposta)`	Sem política de e-mail / verificações

SOA	`ns1.dominios.uol.com.br · admin.uolhost.com.br (serial 2026060500)`	Zona existe, porém vazia de hospedagem
CNAME www	`— (sem resposta)`	Sem subdomínio www publicado

Leitura técnica. A existência da zona (SOA presente, com serial datado de 05/06/2026) aliada à **ausência completa de registros de endereço, e-mail e verificação** indica que o titular adquiriu o domínio e o apontou para os servidores da UOL, mas **ainda não vinculou hospedagem nem publicou conteúdo**. Não se imputa qualquer conduta à UOL, mera provedora de registro e DNS. O fato relevante é objetivo: **no momento da coleta não havia site no ar**.

5. Hospedagem e Geolocalização

A etapa de geolocalização e identificação de hospedagem **não pôde ser realizada por inexistência de alvo**: como o domínio não resolve para nenhum endereço IP (Seção 4), não há servidor a localizar, nem PTR reverso, nem sistema autônomo (ASN) a consultar. Registra-se a ausência, e não uma limitação de método.

Endereço IP	— (o domínio não resolve)
Sistema autônomo (ASN)	Não aplicável (sem IP)
Geolocalização (ipinfo.io / ip-api.com)	Não aplicável (sem IP)
DNS reverso (PTR)	Não aplicável (sem IP)
Provedor de DNS/registro	UOL / UOLHOST (Brasil)

Leitura técnica. Não há, neste caso, "hospedagem offshore incompatível" a avaliar — simplesmente não existe hospedagem ativa. Qualquer conclusão sobre a infraestrutura de servir conteúdo dependerá de nova coleta caso o domínio venha a ser publicado.

6. Certificado TLS / HTTPS

Não foi possível negociar TLS diretamente (sem IP/serviço em escuta na porta 443). Como verificação complementar e independente, consultou-se a base pública de **Transparência de Certificados** (Certificate Transparency, via crt.sh), que indexa praticamente todos os certificados publicamente emitidos. O resultado foi **vazio**: **nenhum certificado jamais foi emitido** para stsuper.com.br (nem para subdomínios).

Negociação TLS direta	Não realizada — domínio sem IP/serviço em 443
Certificados em CT logs (crt.sh)	**0** (resposta vazia, HTTP 200)
Interpretação	Nenhuma emissão de certificado registrada — coerente com domínio nunca publicado

Leitura técnica. A ausência total de certificados na Transparência de Certificados é uma evidência **convergente** com o estado observado no DNS: o domínio nunca serviu HTTPS. Caso a loja entre no ar (p.ex. atrás de Cloudflare/Shopify ou hospedagem própria), espera-se o surgimento de um certificado DV — momento oportuno para reavaliação.

7. Análise do Conteúdo e do Estado Atual

Na data da coleta (06/06/2026), as requisições HTTPS (porta 443) e HTTP (porta 80) **não obtiveram qualquer resposta** (código de saída 000 do cliente), em decorrência direta da ausência de resolução DNS. Não houve, portanto, página, HTML, JavaScript, formulários ou imagens a coletar e analisar.

A consulta ao arquivo histórico (Internet Archive / Wayback Machine, via índice CDX) retornou **nenhuma captura** para o domínio — não há registro de qualquer conteúdo que tenha estado no ar em momento anterior. Isso reforça que o domínio é **novo e ainda não utilizado** para servir um site.

Verificação	Resultado
HTTP/HTTPS (visitante comum)	Sem resposta (código 000) — domínio não resolve
Conteúdo / HTML / JS	Inexistente na coleta — nada a analisar
Imagens / metadados (EXIF)	Não aplicável — sem imagens disponíveis
Capturas históricas (Wayback)	Nenhuma (resposta vazia)

Leitura técnica. Os artifícios de engenharia social típicos de loja-fantasma (contador regressivo zerado, falsa escassez, avaliações fabricadas, placeholders de template não preenchidos, geolocalização simulada) **não puderam ser observados nem descartados**: não há conteúdo público que os contenha ou os afaste. Este laudo, portanto, **não atesta** a inexistência desses artifícios em uma eventual versão futura do site.

8. Fluxo de Pagamento

Não há fluxo de pagamento a analisar: sem site ativo, não existem scripts de checkout, endpoints proprietários (`.php`), chaves PIX embutidas no código nem gateway identificável. Tampouco foi fornecida, para este caso, captura da tela de pagamento/checkout (pasta `pix/`) que permitisse decodificar um código PIX "copia e cola" (padrão EMV/BR Code).

Aspecto	Observação
Plataforma de checkout	Não identificável (sem site ativo).
Endpoints proprietários .php	Não aplicável — sem conteúdo coletado.
Chave PIX estática no código	Não aplicável — sem código a inspecionar.
Captura de pagamento (pix/)	Não fornecida para este caso.

Leitura técnica. Não é possível, no estado atual, afirmar nem afastar o padrão de "PIX direto, sem gateway" característico de falsas lojas. **Cautela essencial:** caso surja, por qualquer canal (site, anúncio, DM, WhatsApp ou link avulso) em nome de "stsuper", uma cobrança via PIX, ela deve ser tratada com forte desconfiança e verificada antes de qualquer pagamento — sobretudo considerando a idade mínima do domínio. Se uma captura de tela de pagamento for fornecida posteriormente, este laudo poderá ser complementado com a decodificação EMV/BR Code e a checagem do recebedor.

9. Indicadores de Risco e Fatores Observados

A tabela consolida os achados objetivos. Dada a **ausência de site ativo**, a maioria dos indicadores clássicos de fraude é **não avaliável**. Destaca-se um único indicador de risco efetivamente presente (idade mínima do domínio) e alguns fatores que **reduzem o anonimato** do responsável.

#	Indicador / fator	Evidência	Severidade
1	Domínio recém-registrado (~4 dias)	`RDAP — registro 02/06/2026`	MÉDIA
2	Domínio sem site ativo / não resolve	`DNS sem A/AAAA; HTTP 000`	MÉDIA
3	Nenhum certificado TLS jamais emitido	`crt.sh vazio`	BAIXA
4	Sem histórico no Internet Archive	`Wayback CDX vazio`	BAIXA
5	Registro sob CPF (pessoa física), não CNPJ	`RDAP — titular pessoa física`	BAIXA
6	Titular nominalmente identificado (reduz anonimato)	`RDAP — Ronaldo Ceurim Martins`	ATENUANTE
7	Registrador nacional estabelecido (UOLHOST)	`RDAP — provedor p22`	ATENUANTE
8	Pagamento só por PIX sem gateway	–	N/AVAL.
9	Falsa escassez / avaliações fabricadas / placeholders	–	N/AVAL.
10	Hospedagem offshore incompatível	–	N/AVAL.

Síntese: nenhum indicador de severidade ALTA; 2 de severidade MÉDIA (novidade do domínio e ausência de site), 3 de severidade BAIXA, 2 fatores atenuantes (responsável identificado, registrador nacional) e 3 indicadores **não avaliáveis** por falta de conteúdo. O conjunto não permite afirmar fraude, mas também não oferece garantias de legitimidade comercial.

10. Conclusão Técnica

Com base nas evidências coletadas e preservadas em 06/06/2026, conclui-se que o domínio **stsuper.com.br** encontra-se em estado de **pré-publicação**: foi registrado há poucos dias (02/06/2026), via UOLHOST, em nome de uma pessoa física identificada, e está delegado aos servidores da UOL, porém **sem**

qualquer site, certificado ou histórico — não resolve para IP, não serve HTTP/HTTPS e nunca foi arquivado.

Por essa razão, **não é tecnicamente possível classificar o domínio como fraudulento nem como legítimo** no momento: não há serviço público a avaliar. Classifica-se o caso como **RISCO NÃO DETERMINADO (site inativo)**. O único indicador de fraude objetivamente presente é a **idade mínima do domínio**, mitigado pela **identificação nominal do responsável** e pelo uso de um **registrador nacional**. Os demais indicadores clássicos (PIX direto, falsa escassez, avaliações fabricadas, placeholders, hospedagem offshore) permanecem **não avaliáveis** até que haja conteúdo no ar.

*Ressalva metodológica: este laudo baseia-se em fontes abertas e reflete o estado do domínio na data indicada. A classificação expressa um juízo técnico de risco e não substitui decisão de autoridade policial ou judicial. Recomenda-se expressamente a **reavaliação** caso o domínio passe a hospedar um site, pois a presente conclusão poderá mudar substancialmente com o surgimento de conteúdo, certificado e fluxo de pagamento.*

11. Recomendações

Para o consumidor / solicitante

- **Não efetuar qualquer pagamento** a "stsuper" enquanto não existir um site público, no ar e verificável — no momento da coleta não há loja ativa.
- **Desconfiar de anúncios, links ou cobranças PIX** que circulem em nome de "stsuper" (redes sociais, mensageiros, e-mail), sobretudo por se tratar de domínio registrado há poucos dias.
- Caso o site entre no ar, **solicitar nova análise** antes de comprar: verificar identificação da empresa (CNPJ), meios de pagamento (preferir cartão, que permite estorno) e existência de gateway regulado.
- Guardar todos os comprovantes e prints de qualquer oferta recebida; em caso de prejuízo, registrar reclamação no **consumidor.gov.br**, acionar o **Procon** e, se houve pagamento via PIX, o **Mecanismo Especial de Devolução (MED)** junto ao banco.

Observações para diligência adicional

- **Monitorar a publicação do domínio**: o surgimento de registro A/AAAA, de certificado TLS (visível em crt.sh) ou da primeira captura no Wayback indicará que a loja entrou no ar e demandará reavaliação.
- O titular é uma **pessoa física identificada** (Ronaldo Ceurim Martins, contato em provedor UOL); essa informação consta do registro público e pode ser útil para eventual diligência formal por autoridade competente.
- Se for fornecida captura da **tela de pagamento/checkout** (pasta `pix/`), este laudo poderá ser complementado com a decodificação do código PIX (EMV/BR Code) e a verificação do recebedor.

Não se afirma, com base nas evidências, que se trate de fraude consumada — tampouco se atesta legitimidade. As cautelas acima visam proteger o consumidor diante da **incerteza própria de um domínio novo e ainda sem site**.

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
`rdap_raw.json`	`fbc84ee3f1f9fb4b7cb1d06f91d2c3a0892b344b74fe76e95f739e569ae131bf`
`dns_records.txt`	`400c3b9188cf063eb7c3af6400fb2f4dbea5513e14469dc6591ec615eee6a33f`
`crtsh.json`	`4f53cda18c2baa0c0354bb5f9a3ecbe5ed12ab4d8e11ba873c2f11161202b945`
`wayback_cdx.json`	`37517e5f3dc66819f61f5a7bb8ace1921282415f10551d2defa5c3eb0985b570`
`coleta_notas.txt`	`059dd476dc6843f8a6982776415fdb4c452b98fe388669e13a461eb1d5e1f4f9`

Coleta realizada em 06/06/2026 (RDAP/DNS, transparência de certificados crt.sh e índice CDX 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.