RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Verificação de legitimidade e de risco do domínio

marabraz.com.br

Objeto investigado	marabraz.com.br
Natureza	Verificação de legitimidade do domínio e checagem de indicadores de fraude
Data da coleta	19/05/2026 — aprox. 14:10 a 14:25 UTC (11:10–11:25 BRT)
Métodos	OSINT passivo · RDAP · DNS · cabeçalhos HTTP · TLS · Certificate Transparency · contexto público
Situação do site	Indisponível na data da coleta — servidor de origem fora do ar (erro Cloudflare 521/530)
Emissão do laudo	19/05/2026 às 11:42

1. Sumário Executivo

Este relatório documenta a investigação técnica do domínio **marabraz.com.br**, associado à rede varejista brasileira "Marabraz" (móveis, colchões, eletrodomésticos e itens para o lar). A coleta de evidências foi realizada em 19/05/2026 por meio de técnicas de OSINT (inteligência de fontes abertas) e análise forense passiva, sem qualquer interação intrusiva com a infraestrutura-alvo.

A investigação **não identificou indicadores de fraude**. Ao contrário, os dados convergem para a caracterização de um **domínio corporativo legítimo e de longa data**: registrado em **2004** (mais de 21 anos), em nome de **pessoa jurídica com CNPJ regularmente divulgado**, com infraestrutura de e-mail corporativa consolidada e um extenso histórico público de certificados digitais compatível com uma operação de comércio eletrônico estabelecida. Tecnicamente, este é o endereço institucional da própria rede Marabraz — e não uma imitação dela.

Registram-se, contudo, dois **pontos de atenção** de natureza operacional e comercial, que não são indícios de fraude: (i) na data da coleta o **site estava fora do ar** — o servidor de origem não respondia, gerando erro técnico; e (ii) é fato público que a empresa Marabraz encontra-se em **recuperação judicial**, processo de reorganização financeira que pode afetar prazos de entrega e pós-venda.

CLASSIFICAÇÃO DE RISCO	BAIXO RISCO — DOMÍNIO LEGÍTIMO

A classificação "baixo risco" refere-se à **autenticidade do domínio** — verificada na Seção 9. Ela não constitui recomendação de compra: o consumidor deve considerar separadamente os pontos de atenção comerciais descritos na Seção 8. Reforça-se a cautela de digitar o endereço diretamente e desconfiar de variações de nome divulgadas por terceiros.

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, 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, Certificate Transparency).

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`
Cabeçalhos HTTP	curl — requisição HTTPS, HTTP/80 e subdomínio www	`headers_https.txt` · `headers_http80.txt` · `headers_www.txt`
Resposta servida	Captura do corpo retornado pelo servidor	`corpo.html` · `corpo_www.html`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Histórico de certificados	Certificate Transparency (crt.sh)	`crtsh.json`
Geolocalização de IPs	ipinfo.io · ip-api.com (CDN e servidores de e-mail)	`ipinfo_cf.json` · `ipapi_cf.json` · `ipapi_origem.json` · `ipapi_spf.txt`
Contexto do titular	Notícias e bases públicas	`contexto_publico.txt`

Leitura técnica. Como o site estava indisponível na data da coleta (Seção 5), não foi possível observar diretamente o conteúdo das páginas; a verificação apoia-se nos dados de registro, de DNS, de certificados e em fontes públicas. Essa limitação está explicitada ao longo do laudo. Todos os artefatos estão na subpasta **evidencias/** e seus hashes constam do Anexo A. O fuso de referência é

UTC; conversões para Brasília (BRT, UTC–3) são indicadas quando aplicável.

3. Identificação do Domínio (RDAP)

Os dados a seguir foram obtidos junto ao **Registro.br** (operador do TLD `.br`) pelo protocolo RDAP. Diferentemente de domínios genéricos, o `.com.br` **divulga publicamente o titular**, o que permite a verificação direta da pessoa jurídica responsável.

Domínio	marabraz.com.br
Status	active
Data de registro	27/10/2004 19:11:35 UTC
Última alteração	12/08/2025 10:52:41 UTC
Data de expiração	27/10/2026 19:11:35 UTC
Idade do domínio	**~21 anos e 7 meses** — domínio antigo e consolidado
Titular / Registrant	BLUE GROUP PARTICIPAÇÕES E COMÉRCIO ELETRÔNICO LTDA
Identificador do titular	CNPJ 20.857.131/0001-05 (divulgado no RDAP)
Contato administrativo	Blue Group — gestaoti@bgdigital.com.br
Contato técnico	MARABRAZ COMERCIAL LTDA — dominios@marabraz.com.br
DNSSEC	Não assinado (delegationSigned: false)
Servidores de nome	mitch.ns.cloudflare.com · nia.ns.cloudflare.com

Leitura técnica. O registro tem mais de duas décadas — o oposto do perfil de domínio descartável associado a fraudes. O titular é uma **pessoa jurídica com CNPJ aberto e verificável** na Receita Federal, e o contato técnico é a própria "Marabraz Comercial Ltda", com e-mail no domínio investigado. A titularidade em nome de uma empresa do grupo voltada a "participações e comércio eletrônico", tendo a Marabraz como contato técnico, é estrutura societária comum em grupos varejistas (separação entre a operação de loja e o braço digital) e, por si, não constitui irregularidade. A ausência de DNSSEC é uma escolha de configuração de baixa relevância para fins de fraude.

4. Infraestrutura de DNS

A zona DNS é operada pela **Cloudflare**, e o domínio dispõe de infraestrutura de e-mail corporativa própria — característica que distingue uma operação empresarial real de um site improvisado.

Registro	Valor	Observação
A	`172.67.162.50 · 104.21.90.226`	IPs da Cloudflare — site servido através do proxy/CDN
AAAA	`2606:4700:3035::… (dois endereços)`	IPv6 da Cloudflare — suporte a IPv6 presente
NS	`mitch.ns.cloudflare.com / nia.ns.cloudflare.com`	DNS gerenciado pela Cloudflare
MX	`mailhost.marabraz.com.br / mailhost2.marabraz.com.br`	Servidores de e-mail próprios — operação corporativa
TXT / SPF	`v=spf1 … include:outlook · amazonses · auinmeio … -all`	Política de e-mail elaborada (Microsoft 365, Amazon SES)
SOA	`cloudflare — serial 2401769661`	—
www	`A → mesmos IPs Cloudflare do apex`	Subdomínio configurado

Leitura técnica. A presença de registros **MX** apontando para servidores próprios (`mailhost.marabraz.com.br`) e de um registro **SPF** detalhado — que autoriza, entre outros, o Microsoft 365 (`spf.protection.outlook.com`), o Amazon SES e uma plataforma de e-mail marketing — é típica de uma empresa estabelecida, com TI estruturada. Sites fraudulentos normalmente não mantêm e-mail corporativo. Os servidores de e-mail estão fisicamente no Brasil (ver Seção 5).

5. Hospedagem, Geolocalização e Disponibilidade

Endereços do site (registro A)	172.67.162.50 · 104.21.90.226 — Cloudflare, Inc. (AS13335)
Modo de operação	Site servido através do proxy/CDN da Cloudflare (origem protegida)
Servidores de e-mail (Brasil)	mailhost → 187.62.219.231 (São Paulo) · mailhost2 → 201.28.203.202 (São Paulo)
IP adicional autorizado no SPF	142.0.66.108 — TOTVS S.A. (Campinas/SP)
Situação na coleta — apex	HTTP 521 — "Web server is down" (origem não respondeu)
Situação na coleta — www	HTTP 530 / erro 1016 — "Origin DNS error"
Certificado / servidor de borda	Cloudflare (ver Seção 6)

Sobre a geolocalização. Os endereços do site pertencem à **Cloudflare**, rede de distribuição de conteúdo (CDN) de alcance global cujos IPs são **anycast** — anunciados a partir de várias localidades ao mesmo tempo. Por isso, a "localização" do IP (apontada por bases de geolocalização ora nos EUA, ora no Canadá) **não indica** a localização da empresa. O dado geográfico relevante é outro: os **servidores de e-mail e os IPs autorizados no SPF estão no Brasil** (São Paulo e Campinas), em provedores nacionais (Fibrion, Telefônica/Vivo) e na TOTVS — coerente com uma empresa brasileira. Não há, portanto, a incompatibilidade geográfica que caracteriza hospedagens "offshore" suspeitas.

Disponibilidade — site fora do ar. Na data da coleta, as requisições ao site não retornaram páginas: o domínio principal respondeu com **HTTP 521** e o subdomínio `www` com **HTTP 530 (erro 1016)**. São códigos gerados pela **própria Cloudflare** quando ela está no ar, mas **não consegue obter resposta do servidor de origem** da empresa (servidor desligado, em manutenção, ou com falha de DNS interno). O conteúdo do site, portanto, não pôde ser inspecionado.

Leitura técnica. Os erros 521/530 são **falhas de disponibilidade do servidor de origem**, e não sinais de fraude — qualquer site legítimo pode apresentá-los durante uma indisponibilidade. Combinados, porém, com o contexto empresarial descrito na Seção 8, merecem registro como ponto de atenção operacional. Não se imputa qualquer conduta à Cloudflare, à TOTVS ou às operadoras citadas — são provedores de infraestrutura; descreve-se apenas o fato observado.

6. Certificado TLS / HTTPS e Histórico Público

Ainda que o servidor de origem estivesse indisponível, a camada de borda da Cloudflare apresenta um certificado TLS válido. Foram também consultados os registros públicos de Certificate Transparency (crt.sh).

Titular (Subject)	CN = marabraz.com.br
Emissor (Issuer)	Google Trust Services — autoridade "WE1" (C=US)
Natureza	Certificado de borda gerenciado pela Cloudflare (SSL Universal)
Válido de	05/04/2026 20:01:17 UTC
Válido até	04/07/2026 21:00:56 UTC
Número de série	60B471048FBEFFD1135494B579E78CAD

A consulta ao Certificate Transparency retornou um **histórico extenso** — centenas de certificados emitidos ao longo de vários anos para o domínio e seus subdomínios. Esse histórico é, em si, uma forte evidência de operação contínua e legítima:

Elemento do histórico	Leitura
Centenas de certificados emitidos ao longo de anos (Let's Encrypt e Google Trust Services em rotação)	Padrão de renovação automática contínua — operação de longa duração, não descartável.
Subdomínio correio.marabraz.com.br	Servidor de webmail corporativo.
Subdomínios e.allin / img.allin.marabraz.com.br	Integração com plataforma de e-mail marketing ("All iN").
Certificados-curinga *.marabraz.com.br (DigiCert, GlobalSign)	Uso de autoridades comerciais pagas — investimento típico de empresa estabelecida.
Presença do domínio em certificado da plataforma VTEX	O comércio eletrônico opera sobre a VTEX, plataforma corporativa de e-commerce.

Leitura técnica. O certificado vigente é válido e a conexão HTTPS é legítima. Mais relevante que o certificado isolado é o **histórico**: a emissão contínua de certificados por vários anos, para subdomínios de webmail, e-mail marketing e e-commerce, e o uso da plataforma VTEX são incompatíveis com uma operação fraudulenta de curta duração e coerentes com uma rede varejista de verdade.

7. Análise de Conteúdo — Limitação da Coleta

A metodologia prevê a captura e a análise do conteúdo das páginas (textos, imagens, JavaScript, fluxo de checkout). **Nesta investigação esse exame não foi possível**: por estar o servidor de origem fora do ar (Seção 5), o site não serviu HTML, imagens nem scripts. Não há, igualmente, captura de tela de checkout a analisar — e o solicitante informou não haver pagamento via PIX a examinar neste caso.

Registra-se, assim, que os elementos normalmente avaliados em sites suspeitos — contador regressivo, falsa escassez, avaliações fabricadas, placeholders de template, geolocalização simulada, CNPJ mascarado — **não puderam ser observados nem positiva nem negativamente**. A verificação da Seção 9 baseia-se, portanto, nos dados de registro, DNS, certificados e contexto público, e não na inspeção do conteúdo ao vivo.

Leitura técnica. Esta é uma limitação probatória decorrente da indisponibilidade do site, e não um achado. Caso o site volte ao ar, recomenda-se uma coleta complementar do conteúdo para fechamento da análise; até lá, a conclusão deste laudo restringe-se à **autenticidade e à titularidade do domínio**, que puderam ser plenamente verificadas.

8. Situação Empresarial e Pontos de Atenção ao Consumidor

A consulta a fontes públicas (notícias e bases jurídicas, preservadas em `contexto_publico.txt`) traz informações relevantes para o consumidor — de natureza estritamente **econômica e societária**, que não se confundem com fraude:

Ponto de atenção	Descrição
Recuperação judicial	É fato público que a Marabraz está em processo de recuperação judicial — instrumento legal de reorganização financeira de empresas em dificuldade. Não é falência: a empresa segue operando, mas o processo pode impactar prazos de entrega, trocas e atendimento de pós-venda.
Disputa societária	Há litígio sucessório envolvendo a família controladora, em discussão judicial desde 2024. Trata-se de questão interna de governança, sem efeito direto sobre a autenticidade do site.
Site indisponível	Na data da coleta o site estava fora do ar (Seção 5). A indisponibilidade pode ser temporária (manutenção/falha) — recomenda-se reavaliar antes de qualquer compra.

Leitura técnica. Estes pontos são **riscos comerciais**, não indícios de fraude. A distinção é importante: o domínio é autêntico e pertence à empresa que diz representar; o que o consumidor deve ponderar é a saúde financeira da empresa e a disponibilidade do serviço no momento da compra, preferindo meios de pagamento com proteção (cartão de crédito, com possibilidade de contestação) a pagamentos irreversíveis.

9. Verificação de Indicadores de Fraude

A tabela aplica, ponto a ponto, a lista de indicadores de fraude prevista na metodologia, registrando o resultado da verificação para o domínio investigado.

Indicador de fraude avaliado	Resultado da verificação	Situação
Domínio recém-registrado	Registrado em 2004 — mais de 21 anos	AUSENTE
Titular oculto / CNPJ não verificável	Titular é pessoa jurídica com CNPJ divulgado no RDAP	AUSENTE
Hospedagem offshore incompatível	CDN global (Cloudflare); e-mail e SPF em provedores no Brasil	AUSENTE
IP compartilhado com domínio de padrão idêntico	IPs anycast de CDN — não aplicável como indício	AUSENTE
Conteúdo de template não personalizado	Não observável — site fora do ar (ver Seção 7)	N/A
Contador regressivo / falsa escassez / avaliações fabricadas	Não observável — site fora do ar (ver Seção 7)	N/A
Pagamento exclusivo por PIX direto, sem gateway	Não observável — site fora do ar; sem checkout a examinar	N/A
Histórico de operação curto / descartável	Centenas de certificados ao longo de anos; e-commerce em VTEX	AUSENTE
Site fora do ar na data da coleta	Erro Cloudflare 521/530 — indisponibilidade do servidor de origem	ATENÇÃO
Saúde financeira do titular	Empresa em recuperação judicial (risco comercial, não fraude)	ATENÇÃO

Síntese: **nenhum indicador de fraude foi confirmado**. Cinco indicadores foram verificados e estão AUSENTES; três não puderam ser avaliados por estar o site fora do ar (assinalados N/A); e dois pontos foram marcados como ATENÇÃO — ambos de natureza operacional/comercial (indisponibilidade do site e recuperação judicial da empresa), sem relação com fraude.

10. Conclusão Técnica

Com base nas evidências coletadas e preservadas em 19/05/2026, conclui-se que o domínio **marabraz.com.br** é **legítimo e autêntico**: trata-se do endereço institucional da rede varejista Marabraz, e não de uma imitação. Sustentam essa conclusão o registro com mais de 21 anos, a titularidade em nome de pessoa jurídica com CNPJ publicamente verificável, a infraestrutura de e-mail corporativa, o uso da plataforma de e-commerce VTEX e um histórico de certificados digitais de vários anos. **Não foram identificados indicadores de fraude.**

A classificação atribuída é de **baixo risco quanto à autenticidade do domínio**. Esta conclusão convive com dois pontos de atenção que o consumidor deve ponderar — e que **não** são fraude: o site estava **fora do ar** na data da coleta, e a empresa encontra-se em **recuperação judicial**, o que pode afetar entregas e atendimento. Por estar o site indisponível, o conteúdo ao vivo (catálogo, preços, checkout) não pôde ser inspecionado — a conclusão restringe-se à camada de identidade e infraestrutura do domínio.

Ressalva metodológica: este laudo baseia-se em fontes abertas e, dada a indisponibilidade do site na data da coleta, não abrange a análise do conteúdo das páginas. A classificação expressa um juízo técnico de risco e não substitui decisão de autoridade policial ou judicial, nem constitui recomendação de compra ou aval à situação financeira da empresa.

11. Recomendações

Para o consumidor / solicitante

- Tratar **marabraz.com.br** como o domínio legítimo da rede Marabraz — mas **digitar o endereço diretamente** no navegador e desconfiar de links recebidos por mensagem, e-mail ou anúncios.
- Atenção a **domínios imitadores**: variações com letras a mais, hífens, outros TLDs (.com, .shop, .net) ou subdomínios enganosos não são o site oficial, ainda que copiem a marca.
- Antes de comprar, **verificar se o site voltou ao ar** e funciona normalmente; em caso de indisponibilidade persistente, buscar os canais oficiais de atendimento da empresa.
- Considerar que a empresa está em **recuperação judicial**: preferir **cartão de crédito** (que permite contestação) a pagamentos irreversíveis, e guardar todos os comprovantes e protocolos.
- Em caso de problema com pedido (atraso, não entrega), registrar reclamação em consumidor.gov.br e, se necessário, nos órgãos de defesa do consumidor (Procon).

Para responsáveis técnicos

- Não há ação de "takedown" a recomendar — o domínio é legítimo.
- Caso o site permaneça fora do ar, recomenda-se à empresa verificar a disponibilidade do servidor de origem por trás da Cloudflare (erros 521/530) e a configuração de DNS interno (erro 1016).
- Se o objetivo for a análise completa do conteúdo, realizar coleta complementar quando o site voltar ao ar.

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
contexto_publico.txt	c25acb8b6d1f553dcd8e1940afc7f30ceaacd3647fd79bb0f63c57c20c9b800f
corpo.html	19c6472b091707c76d91d6369280d6b9047a384a8fd2b160c28505fa3ad27089
corpo_www.html	62cb344a00a01e92ee1f31b253f3fa365ff05805bb03aa2f4e153c129ca729a7
crtsh.json	6a564ec5cadb1e4c0e1a219e71fc7a2110f13b143f05638b43b180aeef094533
dns_records.txt	df435823c0c4ebbe3d31128fddbbd1be6eae3f3aee914e323009378c265610b8
headers_http80.txt	445ffe7a86ce90719b83b531df9b3c1eee0bfca242e70fc17552ce4ac40dab1c
headers_https.txt	d276fda842da6afe53758c4d81be4315c6054fc0cb75aba0c9ad33849007e1ab
headers_www.txt	8e5268d88c90b66a5a6121939f743137a41f4709187ec2e047ded0964f24fa7d
ipapi_cf.json	645629c32023c0efe2e7bb74ed0800d9617f30819cb933e13f0e30efb6892e3d
ipapi_origem.json	15f44891c2d80f8ee58d5e57d47be7d11e54fa478538c47f3c71b44a0904315e
ipapi_spf.txt	b87766e9efec418d899a517da7311e5b2d5192f1e2f80ab8113fb374fe1e5a10
ipinfo_cf.json	459b9ad06dc47b58455cacca9e6ee7dcbaa276d26c526ae30b4b967bf7fd4ebc
rdap_raw.json	29f5b4b43612f81bcb6fa85a62788044dea5334dd480312052661a1908dbd0d0
tls_cert.txt	492fb4d66d21976e92856c50f45d244acb34a449e65f3f19d94210860de98c04

Coleta realizada em 19/05/2026, aprox. 14:10–14:25 UTC. Algoritmo de verificação: SHA-256. Comando sugerido: `sha256sum -c hash_manifest.txt` (a partir 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.