RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

amazingbrasil.com

Objeto investigado	amazingbrasil.com — loja online que se anuncia "Distribuidor Autorizado Dyson no Brasil" (gTLD .com)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	25/07/2026 (RDAP, DNS, HTTP/TLS, geolocalização, bundle JS, base pública de CNPJ, BR Code do Pix)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do app · decodificação EMV do Pix
Achado central	Loja recém-criada em domínio anônimo que usa a marca Dyson e a identidade de uma empresa real, com Pix a recebedor genérico
Classificação	**RISCO ALTO**
Emissão do laudo	25/07/2026 às 01:45

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **amazingbrasil.com**, realizada em **25/07/2026** por técnicas de OSINT (inteligência de fontes abertas) e análise passiva — requisições equivalentes às de um visitante comum e consultas a bases públicas, sem qualquer interação intrusiva. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

O domínio **está no ar** e entrega uma **loja online em português** intitulada "Amazing Brasil — Distribuidor Autorizado Dyson no Brasil", que oferece produtos **Dyson** (aspiradores, secadores, modeladores Airwrap e purificadores) com pagamento por **Pix**. É uma aplicação de página única (SPA React/Vite) hospedada na plataforma de desenvolvimento **Replit** (IP da Google Cloud; registro DNS `replit-verify`), e as próprias metatags canônicas do site apontam para um **segundo domínio**, `dyson.clubvenda.com.br` — ou seja, o mesmo site é espelhado em endereços distintos, ambos recém-registrados.

O conjunto de sinais é o de uma **loja de alto risco**: o domínio foi **registrado em 17/06/2026** (cerca de cinco semanas antes da coleta), por meio de um **registrador offshore** (Fewmoretaps OÜ / Trustname.com, Estônia) e com **titular oculto**, o que é incompatível com a imagem de uma importadora estabelecida. O site apresenta a identidade de uma **empresa real** — "Amazing Brasil Comércio, Importação e Exportação de Produtos Eletrônicos Ltda", CNPJ 21.940.636/0001-93, ativa desde 2015 —, mas nada no registro do domínio, na hospedagem ou no fluxo de pagamento vincula essa empresa ao site: o **recebedor do Pix**, decodificado do código "copia e cola", é **"VENDASVERIFICADAS"**, um nome genérico intermediado pelo agregador `a55scd.com.br` — e **não** a loja anunciada. O código do checkout ainda expõe cobrança de **Pix fracionado** ("part") e rotas administrativas de forçar avanço de pedido.

Ponto relevante ao consumidor: a alegação de "distribuidor autorizado Dyson" **não é comprovável** no site, os produtos premium ofertados são a isca típica de lojas fraudulentas, e o dinheiro pago por Pix vai para um **recebedor genérico** que não é a empresa nomeada. Não há garantia de entrega nem responsável localizável por trás do domínio.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: uma loja que recebe dinheiro por Pix e coleta dados pessoais (CPF, endereço) **sem vincular quem a opera à empresa que anuncia**, com o pagamento indo a um recebedor genérico, oferece **risco elevado**. Recomenda-se **não comprar, não pagar e não fornecer dados** (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 resolvedor público 1.1.1.1; o conteúdo, os cabeçalhos e o bundle JavaScript foram obtidos por requisição HTTPS de visitante comum. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (Verisign / .com — registrador Trustname)	`rdap_raw.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS (visitante)	`corpo.html · headers_https.txt`
Aplicação (front-end)	Download do bundle JS	`app_index.js`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · PTR reverso	`ipinfo_amazingbrasil.json`

Identidade declarada	Base pública de CNPJ (Receita Federal)	`cnpj_publico.json`
Pagamento (Pix)	Decodificação EMV/BR Code do "copia e cola"	`pix_copiaecola.txt`
Intermediário do Pix	RDAP .br (a55scd.com.br)	`rdap_a55scd.json`
Domínio espelho	RDAP .br (clubvenda.com.br)	`rdap_clubvenda.json`

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

Domínio	amazingbrasil.com (gTLD .com — Verisign)
Registro	**17/06/2026** · expira 17/06/2027 (validade de 1 ano)
Idade na coleta	**~5 semanas** — domínio recente
Titular	**Oculto** (RDAP expõe apenas o registrador)
Registrador	Fewmoretaps OÜ d/b/a Trustname.com (Estônia) — registrador offshore
Servidores de nome	ares / zeus.trustname.com · DNS operado por anycastdns.cz (Gransy)
DNS — A	34.111.179.208 · sem AAAA · **sem MX** · TXT `replit-verify=…`
www	CNAME para o próprio domínio
Hospedagem	AS396982 Google LLC (Kansas City/US) — infraestrutura da plataforma **Replit**
PTR reverso	208.179.111.34.bc.googleusercontent.com (Google Cloud)
Servidor web	Server: Google Frontend · Via: 1.1 google (deploy Replit)
Certificado TLS	CN=amazingbrasil.com · emissor Let's Encrypt (DV) · válido 17/06/2026–15/09/2026
Emissão do TLS	no **mesmo dia** do registro do domínio (17/06/2026)
Domínio espelho	canonical/og:url do site apontam para dyson.clubvenda.com.br (registrado 28/06/2026, Cloudflare)

Leitura técnica. Registro recente, validade de 1 ano, titular oculto e registrador offshore compõem um perfil de **baixa rastreabilidade do responsável**. A hospedagem em uma plataforma de desenvolvimento (Replit, sobre Google Cloud) e a ausência de e-mail próprio (sem MX) não condizem com uma importadora estabelecida. O certificado DV gratuito comprova apenas o controle do domínio, **não a identidade de qualquer empresa**. Não se imputa conduta ao registrador, à Google (Cloud) nem ao Replit, meros provedores de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site é uma **loja online** (SPA React/Vite) que se anuncia como "Distribuidor Autorizado Dyson no Brasil" e vende produtos Dyson com pagamento por **Pix**. O checkout é próprio do site (rotas `/api/pix/create`, `/api/create-pix-part`, `/api/pix/status`, `/api/check-payment` e rotas `/api/admin/*` como `generate-part` e `force-advance`), com QR gerado por api.qrserver.com e busca de endereço via ViaCEP. O código "copia e cola" do Pix fornecido foi decodificado (padrão EMV/BR Code):

Campo (EMV)	Valor decodificado
26 · GUI	`br.gov.bcb.pix`
26 · URL do payload	`qrcode.a55scd.com.br/v1/3eefbf21-4062-492d-88da-d69ead73ee7b`
59 · Nome do recebedor	`VENDASVERIFICADAS (genérico — não é "Amazing Brasil")`
60 · Cidade	`SAOPAULO`
53 / 58 · Moeda / País	`986 (BRL) / BR`
62 · Identificador (txid)	`***`
Intermediário (RDAP .br)	`a55scd.com.br → SELECT CREDIT SCMEPP LTDA (CNPJ 45.756.448/0001-78), Cloudflare`

Aspecto	Constatação
Tipo de serviço	Loja online de produtos Dyson (aspiradores, secadores, Airwrap, purificadores)
Tecnologia	SPA React/Vite hospedada no Replit (Google Cloud) · espelhada em dyson.clubvenda.com.br
Meio de pagamento	Pix, inclusive **fracionado** ("part") via checkout próprio
Recebedor do Pix	**"VENDASVERIFICADAS"** — não corresponde à loja anunciada
Intermediário	a55scd.com.br (SELECT CREDIT SCMEPP — instituição de pagamento) · agregador que oculta o beneficiário final
Dados coletados	CPF, nome, contato e endereço (ViaCEP) no fluxo de compra
Identidade declarada	CNPJ 21.940.636/0001-93 — empresa **real** "Amazing Brasil … Ltda", ativa desde 2015 (São Paulo). DV do CNPJ válido
Vínculo empresa↔site	**Não demonstrado** — domínio novo/anônimo e recebedor genérico não ligam a empresa ao site
Marca de terceiro	Uso da marca "Dyson" e alegação de "distribuidor autorizado" sem comprovação no site

Leitura técnica. O fluxo financeiro é real: o usuário paga por Pix e informa CPF e endereço. O risco está na **dissociação entre quem anuncia e quem recebe**: a loja invoca a identidade de uma empresa real e a marca Dyson, mas o Pix vai a um **recebedor genérico** intermediado por um agregador, ocultando o beneficiário final; e a cobrança de Pix "em partes", com rotas administrativas de forçar avanço de pedido, é padrão de manipulação do status da compra. A existência de um **domínio espelho** recém-criado reforça a hipótese de rotação de endereços. Não se imputa conduta à empresa real cuja identidade aparece no site (que pode ser vítima de apropriação), nem ao intermediário de pagamento (a55/SELECT CREDIT), provedor regulado.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Recebedor do Pix genérico ("VENDASVERIFICADAS") via agregador — não é a loja anunciada	`pix_copiaecola.txt` · `rdap_a55scd.json`	ALTA
2	Uso da marca Dyson e alegação de "distribuidor autorizado" sem comprovação	`corpo.html` · `app_index.js`	ALTA

3	Domínio recém-registrado (~5 sem.) em registrador offshore, com titular oculto	`rdap_raw.json`	ALTA
4	Checkout com Pix fracionado e rotas admin de forçar avanço de pedido	`app_index.js`	ALTA
5	Site é espelho de dyson.clubvenda.com.br (outro domínio novo) — rotação de endereços	`corpo.html` · `rdap_clubvenda.json`	MÉDIA
6	Hospedagem em plataforma de desenvolvimento (Replit), incompatível com importadora	`dns_records.txt` · `headers_https.txt`	MÉDIA
7	Identidade de empresa real (CNPJ 2015) em domínio novo/anônimo — sem vínculo demonstrado	`cnpj_publico.json` · `rdap_raw.json`	MÉDIA
8	Sem e-mail próprio (sem MX) apesar de anunciar atendimento@amazingbrasil.com	`dns_records.txt`	BAIXA
9	TLS DV gratuito emitido no dia do registro do domínio	`tls_cert.txt`	BAIXA

Síntese: 4 indicadores de severidade ALTA, 3 MÉDIA e 2 BAIXA. **Nenhum fator de legitimidade** (vínculo verificável entre a empresa nomeada e o site, recebedor coincidente, histórico do domínio) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 25/07/2026, conclui-se que **amazingbrasil.com** é uma **loja online de alto risco**: recém-criada em domínio anônimo (registrador offshore, titular oculto), hospedada em plataforma de desenvolvimento e espelhada em um segundo domínio novo, que usa a **marca Dyson** e a **identidade de uma empresa real** para vender produtos premium por Pix — sendo que o **recebedor do Pix é genérico** ("VENDASVERIFICADAS", via agregador) e não a loja anunciada, com cobrança fracionada e rotas de manipulação de pedido. Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não comprar, não pagar por Pix e não fornecer CPF, endereço ou dados pessoais** ao site.
- Desconfiar de ofertas de produtos Dyson com desconto anunciadas por redes sociais, WhatsApp ou anúncios pagos que conduzam a `amazingbrasil.com` ou `dyson.clubvenda.com.br`.
- Confirmar canais oficiais da Dyson e comprar apenas em revendedores comprovadamente autorizados.
- Se já houve pagamento: acionar o banco e o mecanismo **MED** do Pix, reunir comprovantes e registrar reclamação em **consumidor.gov.br** e Boletim de Ocorrência.

Recomendações de mitigação / denúncia

- Reportar o recebedor "VENDASVERIFICADAS" ao intermediário de pagamento (a55/SELECT CREDIT SCMEPP) e ao banco, e denunciar os domínios aos canais de abuse do registrador (Trustname), da Google/Replit (hospedagem) e da Cloudflare (domínio espelho), anexando este laudo.
- Comunicar o titular da marca **Dyson** sobre o uso não autorizado, e a empresa real cujo CNPJ aparece no site, que pode ser vítima de apropriação de identidade.
- Preservar este relatório e as evidências (pasta `evidencias/`, com hashes SHA-256) para eventual uso administrativo ou judicial.

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, administrativa ou judicial. Não se imputa conduta ilícita à empresa cuja identidade aparece no site, aos provedores de infraestrutura (Trustname, Google/Replit, Cloudflare) nem ao intermediário de pagamento citados.

Anexo A — Manifesto de Integridade (SHA-256)

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

Arquivo	SHA-256
app_index.js	17a704c122c479229c0eb5e25a0e84efb70bdd1e247450a8526a40f4ebff7026
cnpj_publico.json	5f6ec9f7bb28c0fa0d37c83f5649dbefc63670a203d78e97ef2bbd1754af465f
corpo.html	ccd930ac95ad621df322d57fc3062734761c7288f725a8e3b27b9047e27db86b
dns_records.txt	ebedbf64e3dc57a8164554206f7cf33838166a418e14a6b56a5c6c113d285bb0
hash_manifest.txt	32f598a9b21b81adb58c8f1bcc5ed9151fbcb09b582574fed421b400e7441332
headers_https.txt	18852f6f79dc64708b7f80de02c132bf9fa8ac506e2a8d408f955708a4f13604
ipinfo_amazingbrasil.json	3996c30237cb485d6d5b3c15bc0086162c2b3e76e903f8770685ffd8a6da10c9
pix_copiaecola.txt	43aa87afe308a5df37684c5b0b26d327b2d7564fe52f9708e247c22b23462b75
rdap_a55scd.json	3f9d91301117bf8be748137248448945948d2c4a21dd14d89b357efbfe3c15af
rdap_clubvenda.json	b5e40f71032a5187b07edca6be9c5852eb4f0c041cbdc654e2aabfe9fda0993a
rdap_raw.json	4847dcfb5dc5302ac81d3117890a70d613474c7c7411a9431d3871e35be03e98
tls_cert.txt	3d0e40c6c10e7f817780f61ac4290ce00ee724bd71f59fb680364503ef09b641

— Fim do relatório —