



RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

drogariacarvalho.com

Objeto investigado	drogariacarvalho.com - loja online de beleza, perfumaria, higiene e suplementos ("Drogaria Carvalho")
Natureza	Verificação de vínculo com a empresa declarada e de risco ao consumidor
Data da coleta	23/10/2026 (RDAP, DNS, HTTP/TLS, geolocalização, base pública de CNPJ, scripts da aplicação)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · validação de CNPJ · análise do HTML e dos scripts
Achado central	Domínio de 49 dias , com titular oculto, que se apresenta como a loja online de uma drogaria real de Arcos/MG, ativa desde 1966 - CNPJ, razão social e endereço conferem com a Receita, mas nenhum vínculo técnico entre a empresa e o site foi demonstrado, e o e-mail de atendimento está em domínio sem servidor de e-mail
Classificação	RISCO MÉDIO
Emissão do laudo	23/10/2026 as 04:31

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **drogariacarvalho.com**, realizada em **23/10/2026** 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, sem cadastro, sem compra e sem envio de dados pessoais. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

O domínio **está no ar** e entrega uma loja virtual bem acabada - "Drogaria Carvalho - Beleza, higiene e cuidados pessoais online" - com catálogo de perfumes importados (Xerjoff, Montblanc, Calvin Klein, Armaf), dermocosméticos, fraldas, suplementos e itens pet, preços com parcelamento em até 12x no cartão e desconto de 5% no **Pix**. Não foram encontrados medicamentos no catálogo exibido. A aplicação é um SPA em React/Vite com funções de servidor e base de dados **Supabase**, servido por nginx em um servidor da GoDaddy em Phoenix (EUA).

Todas as páginas legais identificam o responsável: **DROGARIA E PERFUMARIA CARVALHO LTDA**, CNPJ **16.966.996/0001-24**, Avenida Getúlio Vargas, 115, Centro, Arcos/MG, CEP 35588-000, com WhatsApp **(37) 98385-1129** e e-mail atendimento@drogariacarvalho.com. O CNPJ passa no módulo 11 e, na base pública da Receita Federal, corresponde a essa mesma razão social, **ATIVA**, com início de atividade em **16/08/1966**, no mesmo logradouro, número e CEP, e CNAE de comércio varejista de produtos farmacêuticos. O DDD 37 do telefone também é da região de Arcos. Ou seja: a identidade declarada **existe e é coerente**.

O que falta é o **vínculo demonstrável** entre essa empresa e o site. O domínio foi registrado em **04/09/2026** - 49 dias antes da coleta - na GoDaddy, com **titular oculto** no RDAP e validade de um ano; não existe drogariacarvalho.com.br (RDAP 404 no Registro.br), que permitiria comparar o titular com o CNPJ. A base pública da Receita não traz telefone nem e-mail da empresa com que se possa cruzar os contatos do site. E o e-mail de atendimento divulgado em todas as páginas está num domínio **sem registro MX**: o domínio tem apenas um TXT de verificação do serviço de envio Brevo - ou seja, está preparado para **enviar** mensagens, mas não para **receber**. Mensagens de clientes a esse endereço tendem a não ser entregues.

Esse conjunto - empresa real e antiga, de cidade pequena, cujos dados aparecem integralmente em um domínio novo e anônimo, com catálogo de perfumaria importada de alto valor - é o mesmo padrão de **apropriação de identidade** documentado em outras lojas do Observatório. Aqui, porém, a evidência não permite afirmá-lo: não há recebedor de Pix divergente apurado, nem outra marca declarada, nem dado falso. Por isso a classificação é de **risco médio**, com a recomendação de confirmar o vínculo diretamente com a empresa antes de comprar.

CLASSIFICAÇÃO DE RISCO

RISCO MÉDIO

Leitura: os dados societários exibidos **são reais e coerentes** com a Receita Federal, mas o site não demonstra pertencer à empresa - domínio de 49 dias, titular oculto, nenhum .com.br e e-mail de atendimento que não recebe mensagens. Antes de comprar, confirme com a drogaria, por um canal obtido de forma independente, que a loja online é dela (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 resolvidor público 1.1.1.1; o conteúdo, os cabeçalhos e o bundle JavaScript foram obtidos por requisição HTTPS de visitante comum. Nenhum formulário foi preenchido e nenhum dado pessoal foi enviado. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (rdap.org / registro do gTLD / Registro.br)	rdap_raw.json

DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME) via 1.1.1.1	dns_records.txt
Conteúdo / cabeçalhos	curl HTTPS (visitante comum), home, páginas legais e scripts	corpo_home.html · headers_home.txt · bundle_js.txt
Certificado TLS	openssl s_client / x509	tls_cert.txt
Geolocalização do IP	ipinfo.io · PTR reverso	geoip.json
CNPJ declarado	Validação por módulo 11 · base pública BrasilAPI/Receita	cnpj_publico_*.json
Consolidação	Extração de fatos e hashes SHA-256	hash_manifest.txt

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

Domínio	drogariacarvalho.com (gTLD .com - registro Verisign)
Registro	04/09/2026 · expira 04/09/2027 (validade de 1 ano)
Idade na coleta	49 dias
Titular	Oculto no RDAP (o registro expõe apenas o registrador)
Registrador	GoDaddy.com, LLC (IANA 146) · abuse@godaddy.com
Servidores de nome	ns71.domaincontrol.com · ns72.domaincontrol.com (GoDaddy)
DNS - A	208.109.39.234 · sem AAAA · sem MX
DNS - TXT	brevo-code:a4640ea3 . . . (verificação do serviço de envio Brevo)
Hospedagem	AS398101 GoDaddy.com, LLC · Phoenix/EUA · PTR 234.39.109.208.host.secureserver.net
Servidor web	nginx/1.18.0 (Ubuntu)
Aplicação	React/Vite com funções de servidor (/__serverFn/) · Supabase · Microsoft Clarity · pixel do TikTok
Certificado TLS	CN=drogariacarvalho.com · Let's Encrypt YR2 (DV) · válido 23/09/2026-22/12/2026
Domínio .com.br	drogariacarvalho.com.br não registrado (Registro.br, RDAP 404)
CNPJ declarado	16.966.996/0001-24 - válido · DROGARIA E PERFUMARIA CARVALHO LTDA · ATIVA · início 16/08/1966 · Av. Getúlio Vargas, 115, Arcos/MG · CNAE: comércio varejista de produtos farmacêuticos

Leitura técnica. Registro recente, titular oculto e certificado DV gratuito são compatíveis tanto com uma empresa estreando no comércio eletrônico quanto com um terceiro usando a identidade dela; isoladamente, não decidem a questão. O que pesaria a favor da empresa - um .com.br em nome do CNPJ, um e-mail que funcione, um contato da Receita que coincida com o do site - não foi encontrado. Não se imputa conduta a GoDaddy, Supabase, Brevo ou Let's Encrypt, meros provedores de registro, hospedagem, dados, e-mail e certificado.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

A loja tem busca, categorias (Beleza, Beleza Premium, Cuidados Diários, Pet, Suplementos, Mamãe & Bebê, Vitaminas), carrinho, conta de cliente, "Meus pedidos" e rastreio. A página de formas de pagamento informa que, no Pix, "um QR Code PIX e um código copia e cola são gerados na hora" e que a confirmação é automática; o cartão é anunciado em até 12x. A cobrança é criada no servidor (funções /_serverFn/), sem identificação de gateway no código público. Como a coleta foi passiva, nenhum pedido foi criado e nenhum código Pix foi obtido; o **recebedor do pagamento não foi apurado**.

Aspecto	Constatação
Tipo de site	Loja online de beleza, perfumaria importada, higiene, suplementos e pet
Identificação do responsável	Presente em todas as páginas - DROGARIA E PERFUMARIA CARVALHO LTDA, CNPJ 16.966.996/0001-24
CNPJ na base pública	ATIVA , início em 1966, mesmo endereço e CEP do site, CNAE farmacêutico
Vínculo empresa x domínio	Não demonstrado - titular oculto, sem .com.br, sem contato na Receita para cruzar
E-mail divulgado	atendimento@drogariacarvalho.com - domínio sem MX (só TXT de envio Brevo)
Telefone divulgado	(37) 98385-1129 - DDD compatível com Arcos/MG; não verificável em base pública
Catálogo	Perfumaria importada de alto valor (até R\$ 1.099,00), dermocosméticos, fraldas, suplementos; sem medicamentos
Páginas legais	Quem somos, termos, privacidade, trocas, entrega, cookies - presentes e coerentes entre si
Meio de pagamento	Pix (5% de desconto) e cartão em até 12x - recebedor não apurado
Rastreadores	Microsoft Clarity e pixel do TikTok

Leitura técnica. A loja é tecnicamente sólida e as páginas legais são consistentes, o que a afasta do modelo de página descartável. O ponto de atenção é a **origem**: uma drogaria de cidade pequena, aberta há quase 60 anos e sem presença online anterior localizada, aparece com loja nova, em domínio anônimo hospedado nos EUA, vendendo perfumaria importada de alto valor. Isso pode ser uma expansão legítima - ou o uso, por terceiro, de dados societários públicos para dar credibilidade a uma loja. A coleta não permite distinguir as duas hipóteses; ela apenas registra que **nenhum elemento técnico liga o site à empresa** e que o canal de e-mail divulgado não recebe mensagens. A coleta foi passiva: nenhuma compra foi feita e nenhum dado pessoal foi enviado.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Dados de empresa real (CNPJ, razão social, endereço) em domínio novo e anônimo, sem vínculo técnico demonstrado	rdap_raw.json · cnpj_publico_16966996000124.json	MEDIA
2	E-mail de atendimento em domínio sem MX - mensagens tendem a não ser entregues	dns_records.txt · dns_extra.txt	MEDIA
3	Domínio registrado 49 dias antes da coleta, com titular oculto e validade de 1 ano	rdap_raw.json	MEDIA
4	Ausência de domínio .com.br que permitiria conferir o titular com o CNPJ	rdap_drogariacarvalho_com_br.txt	BAIXA
5	Catálogo de perfumaria importada de alto valor, destoante do CNAE e do porte declarado	corpo_home.html	BAIXA
6	Hospedagem fora do Brasil (GoDaddy, Phoenix/EUA) e certificado DV gratuito	geoip.json · tls_cert.txt	BAIXA

Síntese: **nenhum indicador de severidade ALTA**; 3 MEDIA e 3 BAIXA. Fatores a favor: CNPJ válido, ativo e coerente com o endereço; páginas legais completas; DDD compatível com a cidade declarada.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em **23/10/2026**, conclui-se que **drogariacarvalho.com** apresenta **risco médio ao consumidor**. O site se identifica como a loja online da DROGARIA E PERFUMARIA CARVALHO LTDA, CNPJ 16.966.996/0001-24 - empresa real, ativa desde 1966 em Arcos/MG, no endereço declarado -, mas **o vínculo entre essa empresa e o domínio não foi demonstrado**: o domínio tem 49 dias, titular oculto, não há .com.br da marca e o e-mail de atendimento está em domínio que não recebe mensagens. Não foram constatados dados falsos, recebedor de Pix divergente nem cobrança abusiva. O laudo não afirma que a empresa real tenha qualquer participação no site, nem que não tenha: registra que a ligação não está comprovada e recomenda confirmá-la diretamente antes de pagar.

Recomendações ao consumidor / solicitante

- **Confirmar com a drogaria, por canal obtido de forma independente** (ligação para a loja física em Arcos/MG, perfil oficial verificado), que drogariacarvalho.com é dela.
- No pagamento via Pix, conferir se o **nome do recebedor** exibido pelo banco é DROGARIA E PERFUMARIA CARVALHO LTDA; se for outro, não pagar.
- Preferir **cartão de crédito**, que permite contestação, a Pix enquanto o vínculo não estiver confirmado.
- Não depender do e-mail divulgado para pós-venda: o domínio não recebe mensagens.
- Guardar prints do pedido, valor, prazo e comprovante de pagamento.

Recomendações de mitigação / denúncia

- À empresa cujo CNPJ é exibido: se a loja for sua, configurar MX no domínio (ou publicar um e-mail funcional) e registrar o .com.br em nome do CNPJ; se não for, registrar boletim de ocorrência por uso indevido de dados e notificar o registrador (abuse@godaddy.com).
- Em caso de prejuízo, acionar o banco pelo **MED** (Mecanismo Especial de Devolução) do Pix e registrar reclamação no consumidor.gov.br.
- Preservar este relatório e as evidências (pasta evidencias/, com hashes SHA-256) para consulta futura.

*Ressalva metodológica: este laudo baseia-se em fontes abertas e reflete o estado do endereço na data indicada (coleta em 23/10/2026). A classificação expressa um **juízo técnico de risco** e não substitui decisão de autoridade policial, administrativa, regulatória ou judicial. A verificação do CNPJ confirma a existência e a situação cadastral da empresa declarada, não que ela opere este site; o laudo não afirma que a empresa real tenha participação nele. Não se imputa conduta ilícita aos provedores de infraestrutura citados (GoDaddy, Supabase, Brevo, Let's Encrypt).*

Anexo A - Manifesto de Integridade (SHA-256)

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

Arquivo	SHA-256
bundle_js.txt (477932 bytes)	a4130682897e21771650ad0a9749c0342bc659e2bedb196f9edf497ec8103eeb
chunks/carrinho-Cu1jWxnZ.js (5198 bytes)	8f1903a738e132558f0313093dcf030749a5c8fd58c87b38e7d1d65f5850e08b
chunks/formas-de-pagamento-vPhzPRAj.js (1157 bytes)	84d803a4c775bded37e5f5364835198e28031aa84cac2fb1eb8443903c9e3000
chunks/qr-code-B8IUShM2.js (639 bytes)	f9d0006be888d47a740b2cdb81c182defcd38ae742edd77308e272215a8fca8e

chunks/routes-CAVUmBae.js (12676 bytes)	9d133b6b32081df7047fad2740038dba8d85745eb23122079ddcc3be58c2692f
chunks/store-gu9Tmh5K.js (11879164 bytes)	f9ebb27a932c59fcfbc2d096dd7f64e62e0345a5f6d8912b79ada5e7c7bc3cd3
chunks/track-7ZBk8PRN.js (1490 bytes)	39baaf256e5ae76bc289633498597b4e9106b3614edc8af51b6dbc11a49e007b
cnpj_publico_16966996000124.json (3513 bytes)	f10f5ad6afdc7c025ccbb2a73520879877df70ca9e9cdeff040f932e07da8191
corpo_contato.html (41460 bytes)	0c2bd75923e8590339bd647738e08d6e9bd40a11a96e81f3343c21c007e79be3
corpo_contato_html.html (35903 bytes)	b826531666a3962ffec356bf416fdeff26788d00d050095301e8fb9c96c5d838
corpo_faq.html (35876 bytes)	ab5cf60fc9887acfd6af59c6f3e2a748f3c5f806a43dabdecea723365df46f77
corpo_home.html (244148 bytes)	8f4649bf49b2ef81ec9e710d6c836b905e9241de3c57d50dbb37ac4cf0cc9f86
corpo_politica_de_privacidade.html (40433 bytes)	43e695deef62bea1f6522fc5e1a55d5280f8b5d2d81419a4b5fc755c3c973c24
corpo_privacidade.html (35900 bytes)	6fb6ad8fec8b1cff98cea8dd65fcc3fc768fbd154e71558ecfece5f3b5b1d207
corpo_privacidade_html.html (35915 bytes)	e4ef3cae084b8569428ed30ab9ff9d7442ece25ecf262b110e72df0560666966
corpo_quem_somos.html (41730 bytes)	8aa3dda4b6082127f2019c7177aabb91d5090fd3ee42097236ed2dfc298292ae
corpo_sobre.html (35882 bytes)	ecd91642dd88b426d210b676646cec4de9d12384541b8ca8fee53a5a7c6c7d82
corpo_sobre_html.html (35897 bytes)	cab4722d6f3117de97642c545312aa96528aba30536d4cdc6b93170f197374f5
corpo_suporte.html (35888 bytes)	62b926d4f0a53175ac9131014573e722c4996932ce331961e02f9296a4f9037f
corpo_termos_de_uso.html (39970 bytes)	c999ebc0c0d2950bc80d33d868bf85edb464bbcb3d51b265b64b29b3280c87e8
corpo_termos.html (35885 bytes)	cfbdce7c627eb52aa89233422d61f6374260503f0a301bbbda4e72a491649515
corpo_termos_html.html (35900 bytes)	fd7a9501e41e528d45b677ad4d4f19d04662d87d7dac9c48fcc5cbb1deb2471a
dns_extra.txt (58 bytes)	36d494c61832e58c18b8850a075473c077863b5e3e4386fbfbf224336049535a0e
dns_records.txt (416 bytes)	9a28427976b30424964ff463dfd4a0f6fbff8bfffffe5e03ed5e6f2806a73889
geoip.json (312 bytes)	8b354f7c61816dbe354d5af4ba544cba0179405344964e45c23d8de019ff272b
headers_home.txt (147 bytes)	d4a87e92f7a77a544cb67bc4824f767ec74d437b86622382dbed818659f01033
rdap_drogariacarvalho_com_br.txt (121 bytes)	9a1dc58a718b9932e572644d77f291da51a800c1fa5f9c9ba32809531e5734dd
rdap_raw.json (2713 bytes)	b731e4676ec1748eab4e6ffda588fb79b91f0c30669a145cdb44c3df54a54c57
tls_cert.txt (305 bytes)	2096d1bba50ef694c1fc647e7a1621b4381e8aaa882b25df684b01e52d34fb3a

- Fim do relatório -