

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

floricultura-rosas.com

Objeto investigado	floricultura-rosas.com - floricultura on-line “Floricultura Rosas”
Natureza	Verificação de identificação do vendedor e do mecanismo de “parceiro local”
Data da coleta	28/11/2026 (RDAP, DNS, HTTP/TLS, geolocalização, bases públicas, análise do código da página)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do HTML e dos scripts
Achado central	O site busca o nome de uma **floricultura real da cidade do visitante** e o exibe como “parceiro encontrado”, sem CNPJ nem qualquer vínculo demonstrado com essa empresa
Classificação	**RISCO ALTO**
Emissão do laudo	28/11/2026 as 01:05

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **floricultura-rosas.com**, realizada em **28/11/2026** por técnicas de OSINT (inteligência de fontes abertas) e análise passiva — requisições equivalentes às de um visitante comum e consultas a bases públicas, sem cadastro, sem compra e sem envio de dados pessoais. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

A loja vende buquês, orquídeas e cestas com chocolates, com “Restam apenas 5 unidades”, avaliações “há 7 min” e “mais de 3.000 pedidos entregues” — num domínio registrado em 18/08/2026, 102 dias antes da coleta, com titular oculto.

Ao abrir a página, um script descobre a cidade do visitante (pelo cabeçalho da Cloudflare, pelo serviço ipapi.co ou pelo GPS do navegador) e consulta `/api/florist` com a busca “florist in <cidade>, <estado>, Brasil”. O primeiro nome de floricultura retornado é exibido numa janela “**Parceiro Encontrado!** Encontramos uma floricultura parceira disponível para entrega rápida em sua região”. O código filtra nomes indesejados, mas não há lista de parceiros: o nome é o de qualquer floricultura que exista na cidade.

A loja se identifica apenas como “Floricultura Rosas”, sem CNPJ, endereço ou telefone; o contato é um e-mail. Há outro site com o mesmo nome (`floriculturarosas.site`), analisado em laudo próprio, sem recurso técnico em comum.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: o visitante passa a acreditar que comprará de uma floricultura conhecida da sua cidade, cujo nome foi apenas copiado de uma busca automática — indício de apropriação de identidade de terceiros.

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. 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 · rdap_*.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME) via 1.1.1.1	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS (visitante comum) e navegador headless; home, páginas legais e scripts	`corpo_*.html · headers_home.txt · bundle*.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	floricultura-rosas.com
Registro	18/08/2026 · expira 18/08/2027 · **102 dias** antes da coleta

Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)
Registrador	Realtime Register B.V. · rtr-security-threats@realtimeregister.com
Servidores de nome	hunts.ns.cloudflare.com · yolanda.ns.cloudflare.com
DNS - A	172.67.153.220 · 104.21.72.186 · sem MX
Hospedagem	AS13335 Cloudflare, Inc. · San Francisco/US · cabeçalho `server: cloudflare`
Certificado TLS	Google Trust Services (WE1) · emitido em 16/10/2026 · válido até 14/01/2027
Geolocalização	Script na home detecta a cidade (Cloudflare, ipapi.co ou GPS) e consulta `/api/florist?q=florist in <cidade>` para exibir “Parceiro Encontrado!” com o nome de uma floricultura local
Identificação	“Nome da empresa: Floricultura Rosas” — sem CNPJ, endereço ou telefone

Leitura: domínio de 102 dias, titular oculto, registrador Realtime Register, atrás da Cloudflare.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Site estático (Bootstrap, Swiper) com funções de servidor na Cloudflare para geolocalização, busca de floricultura e contato; checkout próprio com Pix.

Aspecto	Constatação
“Parceiro” local	Nome de floricultura real obtido por busca automática
Prova social	Avaliações “há 7 min” e “mais de 3.000 pedidos” num domínio de 3 meses
Escassez	“Restam apenas N unidades” em todos os itens
Identificação	Sem CNPJ, endereço ou telefone

Leitura: a sensação de proximidade e de urgência é fabricada pela própria página.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Nome de floricultura real da cidade exibido como “parceiro”, sem vínculo	`corpo_home.html`	ALTA
2	Nenhum CNPJ, endereço ou telefone	`corpo_sobre-nos.html`	ALTA
3	Prova social e escassez incompatíveis com domínio de 102 dias	`corpo_home.html`	MEDIA
4	Titular do domínio oculto	`rdap_raw.json`	BAIXA

Síntese: quatro indicadores, dois de severidade alta.

6. Conclusão Técnica e Recomendações

A floricultura-rosas.com não identifica o vendedor e usa o nome de floriculturas reais da cidade do visitante como se fossem parceiras. Classificação técnica: **RISCO ALTO**, com indício de apropriação de identidade — as floriculturas cujos nomes aparecem são possíveis vítimas, não responsáveis.

Recomendações ao consumidor / solicitante

- Se o site disser que uma floricultura da sua cidade é “parceira”, ligue para ela antes de pagar.
- Desconfie de preços muito abaixo do mercado combinados com desconto extra para pagamento via Pix.
- Antes de comprar, confira o CNPJ na Receita Federal e se o domínio do site pertence de fato à empresa (consulta RDAP / Registro.br).
- Prefira cartão de crédito, que permite contestação (chargeback); o Pix é instantâneo e de difícil reversão.

Recomendações de mitigação / denúncia

- Reportar o endereço ao Google Safe Browsing e ao canal de abuso do registrador (rtr-security-threats@realtimeregister.com).
- Vítimas que pagaram via Pix: acionar o banco imediatamente pedindo o MED (Mecanismo Especial de Devolução), registrar boletim de ocorrência e reclamação em consumidor.gov.br / Procon, anexando este laudo.

Ressalva: este laudo expressa **juízo técnico de risco** com base em evidências públicas coletadas passivamente em 28/11/2026; não é decisão judicial e não imputa crime a nenhuma pessoa física ou jurídica. Registradores, provedores de hospedagem/CDN, plataformas de loja e intermediários de pagamento são citados apenas como fatos técnicos, sem imputação de conduta. O titular do site pode usar estes achados para corrigir as inconsistências apontadas. Os fatos podem mudar após a coleta.

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 (390929 bytes)	274eebd4f715bc286b8a03b3f1920cf253140eaf5a172a44a3bd168e5e5e7d5f
corpo_contato.html (40795 bytes)	17d317c0250af7c77ac51beb53399ff000ad1da4301d88795514026c99ce15a3
corpo_contato_html.html (40795 bytes)	d551083d45c5be074d70b2e01123acdc83caac9a4b95f5aa88d888a61033dfee
corpo_faq.html (31726 bytes)	813faa98173c0805a428a0e86048c72411e24e80e68fc93d5c097844d710bb68
corpo_home.html (82546 bytes)	4bba1a119e817467ae696f3f2813fdd4210eed259eb8177e038ff13c17884295
corpo_pagamentos.html (31398 bytes)	558957ffba63f3da5693c2239666deb25be060cbfe0c3d252028a8080f79364d
corpo_sobre-nos.html (31803 bytes)	bf9272eca83f840e3135890fde1cca8d1e022fecefa969564a5d2f477a87da2a
corpo_termos_de_uso.html (31370 bytes)	ba7f04ecdf26330ceb07100ab23217ea14951428e9144c641aaf7324edbd100c
dns_records.txt (439 bytes)	7cfe9420dae88e27369039b6e8c7e0e3ddcb5b4dcdccda13012b1eee322ee440
geoip.json (289 bytes)	54b219f43503a37345d271a2ceb64295858eb335bf2a8240fb1acb6dc65cb17f
headers_home.txt (751 bytes)	ce795f431cc76b3b1de92e27cd89246552ad44be0a12c54b4de3abb0f614faaf
rdap_raw.json (2685 bytes)	4258bee8f0be69096e7a90537290d6006ef658553d68b033cabb250c371f7e7a
store-brand.js.txt (24818 bytes)	a099d91f588fbb62ead763d5e631b9049683b64f4ad78942f7af7d95612bdb5e
tls_cert.txt (311 bytes)	8fac100756cb4b6726546640156e4436186eaf43b97dcf87fff93b6783376d37

- Fim do relatório -