


# RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

## floriculturarosas.site

| | |
|---|---|
| **Objeto investigado** | floriculturarosas.site - floricultura on-line “Floricultura Rosas” |
| **Natureza** | Verificação de identificação do vendedor e das promessas de entrega |
| **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** | Floricultura sem CNPJ, endereço ou telefone que promete **entrega grátis em 1 hora** “em todo o Brasil”, criada em plataforma de geração de sites |
| **Classificação** | **RISCO MÉDIO** |
| **Emissão do laudo** | 28/11/2026 as 01:05 |

## 1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **floriculturarosas.site**, 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 oferece buquês a partir de R$ 60,00 (12 rosas) e cestas, com “Atendimento 24 horas” e “Entrega Grátis em 1 hora”, e se descreve como “entrega de flores em todo o Brasil”. O domínio foi registrado em 25/10/2025 na GoDaddy, com titular oculto, e o site foi gerado e publicado na plataforma Lovable.

Não há CNPJ, razão social, endereço nem telefone: o único contato é um e-mail do próprio domínio. Entrega em 1 hora em qualquer cidade do país exigiria uma rede de lojas que o site não identifica.

O nome “Floricultura Rosas” é o mesmo de `floricultura-rosas.com`, analisado em laudo próprio; os dois usam registradores, hospedagem e código diferentes, e não foi encontrado vínculo técnico entre eles.

**CLASSIFICAÇÃO DE RISCO** **RISCO MÉDIO**

Leitura: a promessa de entrega é incompatível com uma loja que não informa onde está nem quem é.

## 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** | floriculturarosas.site |
| **Registro** | 25/10/2025 · expira 25/10/2027 · **399 dias** antes da coleta |
| **Titular** | **Oculto** no RDAP (o registro expõe apenas o registrador) |
| **Registrador** | GoDaddy.com, LLC · abuse@godaddy.com, tho@godaddy.com |
| **Servidores de nome** | sergi.ns.cloudflare.com · zelda.ns.cloudflare.com |

| | |
|---|---|
| **DNS - A** | 185.158.133.1 · sem MX |
| **Hospedagem** | AS13335 Cloudflare, Inc. · San Francisco/US · PTR/hostname `lovable-app-cd-1-4.p.l5e.io` · cabeçalho `server: cloudflare` |
| **Certificado TLS** | Google Trust Services (WE1) · emitido em 31/10/2026 · válido até 29/01/2027 |
| **Hospedagem** | IP `185.158.133.1`, endereço de publicação da plataforma Lovable; script de eventos `__lovableEvents` na página |
| **Identificação** | Apenas `contato@floriculturarosas.site`; sem CNPJ, endereço ou telefone |

Leitura: domínio de 399 dias com titular oculto, registrado na GoDaddy e servido pela Lovable atrás da Cloudflare.

## 4. Plataforma, Fluxo de Pagamento e Dados Coletados

Aplicação React gerada na Lovable, com catálogo e carrinho.

| Aspecto | Constatação |
|---|---|
| Entrega | “Grátis em 1 hora”, “em todo o Brasil” |
| Preços | Buquê de 12 rosas por R$ 60,00 |
| Identificação | Só e-mail do domínio |
| Nome | Igual ao de outra loja sem vínculo técnico |

Leitura: sem identificação, o comprador não tem a quem recorrer se a entrega não acontecer.

## 5. Indicadores de Risco

| # | Indicador | Evidência | Sev. |
|---|---|---|---|
| 1 | Nenhum CNPJ, endereço ou telefone | `corpo_home.html` | ALTA |
| 2 | Entrega grátis em 1 hora em todo o país | `corpo_home.html` | MEDIA |
| 3 | Mesmo nome de outra floricultura on-line de alto risco | `corpo_home.html` | BAIXA |
| 4 | Titular do domínio oculto | `rdap_raw.json` | BAIXA |

Síntese: quatro indicadores, um de severidade alta.

## 6. Conclusão Técnica e Recomendações

A floriculturarosas.site não identifica o vendedor e faz uma promessa de entrega que não se sustenta sem lojas físicas declaradas. Classificação técnica: **RISCO MÉDIO**.

### Recomendações ao consumidor / solicitante

- Prefira floriculturas com endereço físico conferível na sua cidade.
- 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 (abuse@godaddy.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 (871814 bytes) | 6d6f87e0e26f8e3a3f64414a21c1fa4df19a11e8c6740558fd1408bda5dbaffd |
| corpo_home.html (76218 bytes) | 892eb4ea1663c048e14f816379a3706e8e98ec3c96576eb7d353dcec83df01c3 |
| dns_records.txt (370 bytes) | 960bff1b27072884857754cd3c14fb7d8fa7e146a7a5ba749c9b93955b960a87 |
| geoip.json (333 bytes) | 8c316e02ecf7a6652c0547faed6e32afe85bc5de6ecd42dcda1ab4739083ac95 |
| headers_home.txt (826 bytes) | c7c2f9e1d0421c1afdd8963d8df903525b71b114f6f05b1b1b8e29e88ad1271c |
| rdap_raw.json (5207 bytes) | 239d5fd3fae6e2233540d9decff324a5c8301382a365274f0474924891ed208e |
| tls_cert.txt (311 bytes) | 206382b22006171b66e392ce799233081decb51e6632fa652bac456a4c08da6f |

*- Fim do relatório -*