

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

nurela.com.br

Objeto investigado	nurela.com.br - loja Shopify de utilidades domésticas, Natal, jardim e acessórios automotivos
Natureza	Verificação de identificação do fornecedor e das condições de venda
Data da coleta	17/11/2026 (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	Loja de 104 dias registrada por pessoa física, sem CNPJ, com rodapé de modelo (“Minha Loja”), selos de “Loja Verificada” que apenas apontam para páginas genéricas e dois números de WhatsApp diferentes
Classificação	**RISCO MÉDIO**
Emissão do laudo	18/11/2026 as 00:54

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **nurela.com.br**, realizada em **17/11/2026** 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, na Shopify e atrás de desafio anti-robô (lida com navegador headless), vende um sortimento típico de dropshipping — escada telescópica, sapateira de bambu, árvore e luzes de Natal, capas impermeáveis, descascador elétrico — com “Queima de estoque”, frete grátis e preço menor no Pix.

O domínio .com.br está em nome de uma pessoa física (CPF mascarado no RDAP), e o site não exibe CNPJ. O rodapé mantém o texto do modelo de tema, “© 2025 Minha Loja”, e o bloco “Loja Verificada” reúne selos do Reclame Aqui, Google e SSL que levam a páginas genéricas desses serviços — não a uma verificação da loja.

O atendimento informa o e-mail nurelaoficial@gmail.com e dois WhatsApp diferentes: (19) 99120-1347 no rodapé e (19) 97829-2314 na página de contato.

CLASSIFICAÇÃO DE RISCO	RISCO MÉDIO

Leitura: não há captura indevida de dados demonstrada, mas o fornecedor não é identificado, os selos de confiança não verificam nada e o modelo de loja não foi personalizado (Seções 4 e 5).

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	nurela.com.br
Registro	05/08/2026 · expira 05/08/2027 · **104 dias** antes da coleta
Titular	**Pessoa física** (CPF parcialmente mascarado no RDAP: ***.871.811-**) · contato nurelaoficial@gmail.com

Registrador	HSTDOMAINS · nurelaoficial@gmail.com
Servidores de nome	aurora.dns-parking.com · nebula.dns-parking.com
DNS - A	23.227.38.65 · sem MX
Hospedagem	AS13335 Cloudflare, Inc. · Ottawa/CA · PTR/hostname `myshopify.com` · cabeçalho `server: cloudflare`
Certificado TLS	Let's Encrypt (YE2) · emitido em 03/10/2026 · válido até 01/01/2027
Loja Shopify	`s8e0m0-qw.myshopify.com` · moeda BRL · checkout via Zedy/Yampi
CNPJ	**Nenhum** exibido; rodapé “© 2025 Minha Loja”

Leitura: domínio de 104 dias em nome de pessoa física (registrador HSTDOMAINS/Hostinger, DNS parking da Hostinger), site servido pela Shopify, sem MX — o e-mail é Gmail.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Loja Shopify com tema de dropshipping, checkout por app Zedy (`app.zedy.com.br`) com integração Yampi e analytics hospedado no Render. Páginas de contato e reembolso foram baixadas.

Aspecto	Constatação
Pagamento	Cartão em até 12x e Pix (desconto de ~5%)
Fornecedor	Sem CNPJ; domínio em nome de pessoa física; e-mail Gmail
Selos	“Loja Verificada” com links para páginas genéricas do Reclame Aqui, Google e SSLShopper
Contato	Dois WhatsApp distintos: (19) 99120-1347 e (19) 97829-2314

Leitura: selos estáticos que apontam para a página inicial de um serviço não comprovam reputação; a reputação real deve ser buscada pelo próprio comprador no Reclame Aqui.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Nenhum CNPJ; domínio em nome de pessoa física	`rdap_raw.json` · `corpo_home_chrome.html`	ALTA
2	Selos de “Loja Verificada” sem verificação real	`corpo_home_chrome.html`	MEDIA
3	Rodapé de modelo “© 2025 Minha Loja”	`corpo_home_chrome.html`	MEDIA
4	Dois números de WhatsApp diferentes e e-mail Gmail	`corpo_policies_contact_information.html`	BAIXA

Síntese: quatro indicadores, um de severidade alta (fornecedor não identificado).

6. Conclusão Técnica e Recomendações

A nurela.com.br é uma loja Shopify de dropshipping operada em nome de pessoa física, sem CNPJ, com selos de confiança decorativos e modelo não personalizado. Classificação técnica: **RISCO MÉDIO**.

Recomendações ao consumidor / solicitante

- Desconfie de selos “Loja Verificada” que apenas levam à página inicial do serviço; pesquise a loja diretamente no Reclame Aqui.
- 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 (nurelaoficial@gmail.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 17/11/2026; 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
corpo_home_chrome.html (1065350 bytes)	14f3ed3146b356e3ff65cce61164882e8734683cc41698cae3b00ee69a73757a
corpo_home.html (8713 bytes)	68a87cd55d48b7e0b304cd601fd0fc99f20c1ea87fad87dfb9a300c71a3f67a7
corpo_policies_contact_information.html (353717 bytes)	f0950425c4bcc9c8c63c3c1274b5096c565d514f13e613738d62aa2b3b080266
corpo_policies_refund_policy.html (358024 bytes)	5b41c24c5ecd29271e25938128a5eec924a04125759c74860fecd6d98d2c37eb
dns_records.txt (322 bytes)	8e69eba1aa6b2eebff3877003595c9aecb4187c2c517bd141ff4fb0c90df988b
geoip.json (301 bytes)	53d8288d3aac6ca6e14e847315b68482ba7f9fa2631f7cda25cfaa26d705e83c
headers_home.txt (1781 bytes)	f5bdc57365e9491af13f5f81d774d0476a748878390d7d9dc96a186b46964924
rdap_raw.json (4049 bytes)	9976d59ff4db381946e051eba278803e08a001037b81b73acc167d7d72071e5e
tls_cert.txt (298 bytes)	88e647eb83899dbd47befd34851aee9f08636cb2943057b7917e50c5d616b317

- Fim do relatório -