

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

lojalunnacosmeticos.com

Objeto investigado	lojalunnacosmeticos.com - loja de perfumes importados, skincare e maquiagem de grifes
Natureza	Verificação de legitimidade da loja, da empresa declarada e do fluxo de pagamento
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	Domínio de **18 dias** que vende Dior, Lancôme, Kérastase e MAC com “até 70% OFF” + cupom de 12% + 15% no Pix, sob um CNPJ de “promoção de vendas” aberto em agosto de 2026 numa cidade de 4 mil habitantes
Classificação	**RISCO ALTO**
Emissão do laudo	18/11/2026 as 00:54

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **lojalunnacosmeticos.com**, 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).

O site, em Next.js atrás da Cloudflare, oferece 169 marcas de perfumaria e cosmética — Dior, Guerlain, Carolina Herrera, Lancôme, Kérastase, MAC — "originais, lacrados e com nota fiscal", com **até 70% de desconto**, cupom LUNNA12 (12% na primeira compra), 15% adicionais no Pix e frete grátis sem valor mínimo.

O rodapé identifica LUNNA COSMETICOS LTDA, CNPJ 68.838.162/0001-37, em Água Santa/RS — dados que conferem com a Receita. A empresa foi aberta em 27/08/2026, como microempresa de capital R$ 20 mil, com CNAE de **promoção de vendas**; o domínio foi registrado em 30/10/2026, 18 dias antes da coleta.

O checkout usa o formulário tokenizado do Mercado Pago para cartão (os dados do cartão não passam pelo servidor da loja) e PayPal, além de Pix. Quando o cartão é recusado, a resposta do servidor pode trazer uma "oferta", e as mensagens de erro orientam a "pagar no Pix para concluir o pedido".

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: o checkout de cartão é tecnicamente correto, mas os descontos acumulados sobre perfumes de grife (até 70% + 12% + 15%) são incompatíveis com produto original com nota fiscal, e a empresa é recém-aberta, com atividade que não é de comércio de cosméticos (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	lojalunnacosmeticos.com

Registro	30/10/2026 · expira 30/10/2027 · **18 dias** antes da coleta
Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)
Registrador	Internet Domain Service BS Corp · abuse@internet.bs
Servidores de nome	asa.ns.cloudflare.com · carter.ns.cloudflare.com
DNS - A	172.67.139.172 · 104.21.26.245 · MX: route2.mx.cloudflare.net, route3.mx.cloudflare.net
Hospedagem	AS13335 Cloudflare, Inc. · San Francisco/US · cabeçalho `server: cloudflare`
Certificado TLS	Let's Encrypt (YE2) · emitido em 30/10/2026 · válido até 28/01/2027
CNPJ exibido	68.838.162/0001-37 · LUNNA COSMETICOS LTDA · aberta em **27/08/2026** · Água Santa/RS · CNAE principal **“promoção de vendas”** · microempresa, capital R$ 20 mil · sócia única
lunnacosmeticos.com.br	Não registrado (Registro.br)

Leitura: domínio de 18 dias, titular oculto, registrador Internet.bs; DNS e e-mail na Cloudflare, verificação Brevo e Google no TXT — infraestrutura montada de uma vez, na mesma janela da abertura da empresa.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Aplicação Next.js (Turbopack) atrás da Cloudflare, com rotas próprias de conta, carrinho, cupom, brinde, PayPal (`/api/paypal/criar`) e Mercado Pago (`/api/mercadopago/criar`). A página de checkout e seus scripts foram baixados como visitante; nenhum pedido foi gerado.

Aspecto	Constatação
Pagamento	Pix (15% de desconto), cartão via formulário tokenizado do Mercado Pago, PayPal
Recusa do cartão	Estado “recusado” pode vir com uma “oferta”; mensagens orientam a pagar no Pix
Preços	“Até 70% OFF + 12% com LUNNA12”, 15% no Pix, brinde a partir de R$ 199
Identidade	LUNNA COSMETICOS LTDA · CNPJ 68.838.162/0001-37 · Rua Achyles Panisson, 512, Água Santa/RS · (54) 2888-0757
Telemetria do cartão	Cada etapa do formulário de cartão é reportada a `/api/cartao/evento` (sem os dados do cartão)

Leitura: o ponto de atenção não é o processamento do cartão, mas o incentivo a migrar para o Pix (desconto de 15% e mensagens pós-recusa), meio sem contestação.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Domínio de 18 dias, titular oculto	`rdap_raw.json`	ALTA
2	CNPJ aberto em 27/08/2026, CNAE “promoção de vendas”, capital R$ 20 mil	`cnpj_publico_68838162000137.json`	MEDIA
3	Descontos acumulados de até ~80% sobre perfumes e cosméticos de grife “originais com nota”	`corpo_home.html`	ALTA
4	Incentivo ao Pix após recusa do cartão	`bundle_checkout.txt`	MEDIA
5	Revenda de 169 marcas de luxo sem indicação de distribuidor autorizado	`corpo_home.html`	MEDIA

Síntese: cinco indicadores, dois de severidade alta. O conjunto — loja de dias, empresa recém-aberta e preços impossíveis para produto de grife original — é típico de loja não confiável.

6. Conclusão Técnica e Recomendações

A lojalunnacosmeticos.com tem empresa formalmente identificada e checkout de cartão tecnicamente adequado, mas o domínio tem 18 dias, a empresa foi aberta em agosto de 2026 com atividade de promoção de vendas e capital mínimo, e os preços anunciados são incompatíveis com perfumes de grife originais. Classificação técnica: **RISCO ALTO**.

Recomendações ao consumidor / solicitante

- Perfume de grife com 70% de desconto é forte indício de produto falsificado ou inexistente; compre em revendedores autorizados pelas marcas.
- 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@internet.bs).

- 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
bundle_checkout.txt (160763 bytes)	b464cacf981424e169ddc2fa54f001750cd8b46b38128075e073ed316e5c26d3
bundle_js.txt (433559 bytes)	97682464e9002c7c3ac48d27c2fe16483514792035a1a90ba7eede59e4a5c786
bundle_next_all.txt (780363 bytes)	54c4a118b5f5c91a5c4338cc0ea4e6000b5ee9545f2798e760550ed2fd20d2f5
cnpj_publico_68838162000137.json (1806 bytes)	681cf9c9397727f82ef57de317aca9492f7792d1abe71feddf2ae384071f404a
corpo_checkout.html (98444 bytes)	37d9ffa12b2d9a670415883bc5555e8d80e69f0c4226bb461ace8f7a1dd34218
corpo_home.html (508281 bytes)	73fd1073bcc9d2a075719170a4ded5e12405d9a34cbde35d8a863ebcbaf9c65f
dns_records.txt (690 bytes)	a960ad329abe36987b45b70a2fa04b17e9e805bf79c2f565f8047387c9fe1bfb
geoip.json (289 bytes)	ac2959802a66b0adfa16c4ca7abce43836e1ac410bab993730aed75d2903746a
headers_home.txt (1293 bytes)	a9f2b50ef093781c428d4995507bfbaca57255197951712c3575813e87c97e0d
rdap_lunnacosmeticos.com.br.json (645 bytes)	be1ee28c62ca8ffe0701a26dabd2d0fd93cbe02862b73e7778e546170debbd35
rdap_raw.json (2668 bytes)	a5e352153367f62a8eade9e0f177fc6241daba88ad7caa7a4d4a7f97e062c4ed
tls_cert.txt (308 bytes)	b13e3e739d2de804cb9e43a6a048cd9d8e7a4ff1426a41f30235e7f0fdb950db

- Fim do relatório -