



RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

kerasysbrasil.com

Objeto investigado	kerasysbrasil.com - loja virtual que se apresenta como a operação brasileira da marca coreana de cosméticos capilares Kerasys
Natureza	Verificação da identidade do responsável e de risco ao consumidor
Data da coleta	12/09/2026 (RDAP, DNS, HTTP/TLS, geolocalização, base pública de CNPJ)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · validação de CNPJ · análise do HTML e das páginas legais
Achado central	A loja declara duas empresas diferentes como responsável - uma nas páginas legais e outra injetada por JavaScript no rodapé -, sua política de privacidade se refere a outra loja (kerassys.com, domínio gêmeo que serve página idêntica) e nenhuma delas tem atividade de comércio de cosméticos
Classificação	RISCO MÉDIO
Emissão do laudo	12/09/2026 as 00:53

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **kerasysbrasil.com**, realizada em **12/09/2026** 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 WordPress/WooCommerce bem acabada, em português, dedicada a shampoos, condicionadores, máscaras e kits da marca coreana **Kerasys**, com cupom de primeira compra, frete grátis acima de R\$ 99,90, selo "Produto Original Made in Korea" e **desconto de 5% no Pix**. Os preços de kit vão de R\$ 239,90 a R\$ 299,00, com descontos anunciados de 25% a 40%.

Ao contrário das lojas-fantasma, esta **nomeia um responsável verificável** - e é justamente aí que aparece a inconsistência. As páginas legais (Fale Conosco, Política de Privacidade, Trocas e Devoluções) identificam a operadora como **P. DALBEN MORAIS SERVICOS DE T.I LTDA, CNPJ 58.148.688/0001-31**, à Rua Dom José de Barros, 51, sala 73-I, República, São Paulo/SP. O CNPJ é válido, está **ATIVO** na base pública da Receita Federal desde 19/11/2024 e o endereço confere **exatamente**, inclusive a sala. A atividade registrada, porém, é **"desenvolvimento e licenciamento de programas de computador customizáveis"** - não comércio varejista de cosméticos -, e o capital social é de R\$ 10.000,00.

O rodapé exibido ao visitante, entretanto, nomeia **outra empresa**. Um trecho de JavaScript embutido na própria página insere, ao carregar, a linha **"Rmr Hub de Educação LTDA - CNPJ 60.774.416/0001-99 · Rua Sétimo Patelli, 85, Centro, Campo Limpo Paulista/SP"**. Esse segundo CNPJ também é válido e ativo, aberto em 12/05/2025, mas sua atividade registrada é **"ensino de idiomas"**. O visitante, portanto, vê no rodapé uma escola de idiomas e, nas páginas legais, uma empresa de tecnologia - nenhuma das duas com atividade de cosméticos, e sem qualquer relação explicada entre si.

Há ainda um terceiro sinal de reaproveitamento: a Política de Privacidade afirma textualmente que a empresa é "responsável pela loja **kerassys.com**" - domínio distinto, com dois "s". Esse domínio existe, está no ar atrás da Cloudflare e serve **exatamente a mesma página** ("Pagina Inicial - Kerasys Brasil"). Ou seja, o mesmo conteúdo é publicado em pelo menos dois endereços, e o texto legal de um deles ficou apontando para o outro. O tema do site também carrega o nome **trussadi**, de outra loja - modelo reutilizado. Por fim, nada na coleta indica autorização ou distribuição oficial da marca Kerasys, que pertence a fabricante coreano; o site não declara ser distribuidor autorizado nem cita contrato algum.

CLASSIFICAÇÃO DE RISCO

RISCO MÉDIO

Leitura: a loja **nomeia responsáveis reais e verificáveis**, o que a distingue de uma loja-fantasma, mas nomeia **dois diferentes** - uma empresa de T.I. nas páginas legais e uma escola de idiomas no rodapé -, sua política de privacidade se refere a **outra loja** e nenhuma das empresas declaradas tem atividade de cosméticos. Risco **médio**: recomenda-se exigir esclarecimento sobre quem é o vendedor e preferir cartão ao Pix (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 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)	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 e páginas legais	corpo_home.html · headers_home.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	kerasysbrasil.com (gTLD .com - registro Verisign)
Registro	24/06/2026 · expira 24/06/2027 · última alteração 22/07/2026
Idade na coleta	cerca de 2 meses e meio
Titular	Oculto no RDAP (o registro expõe apenas o registrador)
Registrador	GoDaddy.com, LLC (IANA 146) · abuse@godaddy.com
Status	clientDeleteProhibited · clientRenewProhibited · clientTransferProhibited · clientUpdateProhibited
Servidores de nome	fiona.ns.cloudflare.com · oswald.ns.cloudflare.com
DNS	A 172.67.190.86 / 104.21.76.62 (Cloudflare) · AAAA presentes · MX Mailgun · SPF v=spf1 include:mailgun.org ~all
Hospedagem	AS13335 Cloudflare (proxy) - origem não exposta
Servidor web	Server: cloudflare
Certificado TLS	CN=kerasysbrasil.com · emissor Google Trust Services WE1 (DV) · válido 22/07/2026-20/10/2026
Plataforma	WordPress 7.0 + WooCommerce 10.8.1 · tema flatsome com child trussadi · plugins fluid-checkout, kerasys-pixel-manager, woocommerce-extra-checkout-fields-for-brazil
CNPJ nas páginas legais	58.148.688/0001-31 - válido · P. DALBEN MORAIS SERVICOS DE T.I LTDA, ATIVA desde 19/11/2024 · endereço confere · CNAE: desenvolvimento de software · capital R\$ 10.000
CNPJ injetado no rodapé	60.774.416/0001-99 - válido · RMR HUB DE EDUCACAO LTDA, ATIVA desde 12/05/2025, Campo Limpo Paulista/SP · CNAE: ensino de idiomas
Domínio gêmeo	kerassys.com - no ar atrás da Cloudflare, serve página idêntica ; citado como "a loja" na política de privacidade

Leitura técnica. A infraestrutura é **madura para o padrão de lojas descartáveis**: DNS na Cloudflare, e-mail transacional via Mailgun com SPF configurado, WordPress e WooCommerce em versões atuais e plugins brasileiros de checkout (campos de CPF, simulador de parcelas). Isso indica uma operação com alguma continuidade, não um site montado para durar uma semana. O que destoa é a **identificação do responsável**: dois CNPJs distintos, ambos válidos e ativos, mas nenhum com atividade de comércio de cosméticos, e um deles inserido por script apenas no rodapé. O certificado DV gratuito comprova apenas o controle do domínio, **não a identidade de qualquer entidade**. Não se imputa conduta a GoDaddy, Cloudflare ou Mailgun, meros provedores de registro, rede e e-mail.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site é uma **loja WooCommerce** em português com catálogo organizado por linha (Shampoo, Kits, Condicionador, Tratamento, Finalizadores), avaliações exibidas nos produtos, cupom "PRIMEIRACOMPRA" de 10%, barra de progresso de frete grátis e brinde. O checkout usa o plugin `fluid-checkout` com os campos brasileiros (`woocommerce-extra-checkout-fields-for-brazil`), o que significa coleta de **nome, CPF, e-mail, telefone e endereço** antes do pagamento, conforme a própria política de privacidade descreve. O site anuncia **5% de desconto no Pix** com "pagamento aprovado na hora", e a política de trocas informa que o reembolso é feito **"pelo mesmo meio de pagamento (PIX)"**. Na coleta, com carrinho vazio, o intermediário de pagamento não foi exposto; não houve compra nem envio de dados.

Aspecto	Constatação
Tipo de site	Loja online de cosméticos capilares da marca coreana Kerasys, voltada ao público brasileiro
Responsável nas páginas legais	P. DALBEN MORAIS SERVICOS DE T.I LTDA - CNPJ 58.148.688/0001-31, São Paulo/SP, endereço confere na base pública
Responsável no rodapé	Rmr Hub de Educação LTDA - CNPJ 60.774.416/0001-99, Campo Limpo Paulista/SP - empresa diferente , inserida por JavaScript
Atividade registrada de ambas	Nenhuma é de comércio de cosméticos - uma é de desenvolvimento de software, a outra de ensino de idiomas
Política de privacidade	Afirma ser responsável pela loja kerassys.com - outro domínio, com dois "s"
Domínio gêmeo	<code>kerassys.com</code> está no ar e serve a mesma página ("Pagina Inicial - Kerasys Brasil")
Tema do site	Child theme <code>trussadi</code> sobre <code>Flatsome</code> - modelo reaproveitado de outra loja
Marca	Kerasys - marca de fabricante coreano; o site não declara ser distribuidor autorizado nem cita contrato
Dados coletados	Nome, CPF, e-mail, telefone e endereço no checkout, conforme a própria política de privacidade
Meio de pagamento	5% de desconto no Pix ; reembolso previsto "pelo mesmo meio de pagamento (PIX)"
Canal de contato	E-mail <code>contato@kerassysbrasil.com</code> (domínio com MX Mailgun ativo) e WhatsApp +55 (17) 92004-4380
Infraestrutura	Cloudflare + Mailgun + WordPress/WooCommerce atualizados - operação com continuidade, não descartável

Leitura técnica. Este caso não se parece com uma loja-fantasma: há CNPJs reais, endereço que confere, e-mail em domínio com servidor configurado e infraestrutura mantida. O problema é de **quem responde pela venda**. O consumidor que lê o rodapé conclui que compra de uma escola de idiomas de Campo Limpo Paulista; quem lê a política de privacidade conclui que compra de uma empresa de software da República, em São Paulo, responsável por *outra* loja. Numa disputa de troca, garantia ou não entrega, essa divergência é material: define contra quem o consumidor reclama, em qual comarca e sob qual CNPJ. Some-se que **nenhuma das duas empresas tem atividade registrada de comércio de cosméticos** e que o reembolso previsto é apenas via Pix, meio sem contestação junto a administradora de cartão. Não há, por outro lado, nenhum indício de captura de credenciais, de cobrança de taxa antecipada ou de recebedor de Pix incompatível - por isso a classificação é **média**, e não alta. A coleta foi passiva: nenhuma compra foi feita e nenhum dado pessoal enviado.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Duas empresas diferentes declaradas como responsável - uma nas páginas legais, outra injetada por JavaScript no rodapé	<code>corpo_home.html</code> · <code>pg_politica-de-privacidade.html</code> · <code>pg_fale-conosco.html</code>	ALTA

2	Política de privacidade declara responsabilidade sobre outra loja (kerassys.com), domínio gêmeo que serve página idêntica	pg_politica-de-privacidade.html · corpo_kerassys_com.html	ALTA
3	Nenhuma das duas empresas declaradas tem atividade registrada de comércio de cosméticos	cnpj_publico_58148688000131.json · cnpj_publico_60774416000199.json	MEDIA
4	Titular do domínio oculto no RDAP, com validade de 1 ano	rdap_raw.json	MEDIA
5	Desconto de 5% no Pix e reembolso previsto exclusivamente por Pix - meio sem direito a contestação	corpo_home.html · pg_trocas-e-devolucoes.html	MEDIA
6	Uso da marca Kerasys sem declaração de distribuição autorizada ou de contrato com o fabricante	corpo_home.html	MEDIA
7	Tema child "trussardi" sobre Flatsome - modelo reaproveitado de outra loja	corpo_home.html	BAIXA
8	Coleta de CPF, telefone e endereço completo no checkout por operador cuja identidade diverge entre páginas	pg_politica-de-privacidade.html	BAIXA

Síntese: 2 indicadores de severidade ALTA, 4 MEDIA e 2 BAIXA. Foram constatados **fatores de legitimidade parciais**: CNPJs válidos e ativos, endereço conferido na base pública, e-mail em domínio com MX configurado, plataforma e plugins atualizados e páginas legais completas. O que falta é **coerência** entre as identidades declaradas.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em **12/09/2026**, conclui-se que **kerasysbrasil.com** apresenta **risco médio ao consumidor**. A loja é tecnicamente sólida e, diferentemente de lojas descartáveis, **identifica responsáveis reais**: as páginas legais apontam a P. DALBEN MORAIS SERVICOS DE T.I LTDA (CNPJ 58.148.688/0001-31), empresa ativa cujo endereço confere exatamente com a base pública. O problema é a **divergência de identidade**: um script insere no rodapé uma segunda empresa, a Rmr Hub de Educação LTDA (CNPJ 60.774.416/0001-99), de Campo Limpo Paulista, e a política de privacidade declara responsabilidade sobre **outra loja**, o domínio gêmeo **kerassys.com**, que serve página idêntica. Nenhuma das duas empresas tem atividade registrada de comércio de cosméticos, e o site não declara ser distribuidor autorizado da marca coreana que estampa. Não foram encontrados indícios de captura de credenciais, de taxa antecipada ou de recebedor de Pix incompatível - o risco aqui é de **indefinição de quem responde pela venda**, o que pesa numa troca, garantia ou não entrega. Recomenda-se exigir, por escrito e antes de pagar, qual CNPJ emitirá a nota fiscal, e preferir cartão ao Pix.

Recomendações ao consumidor / solicitante

- **Perguntar por escrito, antes de pagar, qual CNPJ emitirá a nota fiscal** - o rodapé e as páginas legais do site apontam empresas diferentes.
- Preferir **cartão de crédito** ao Pix: o desconto de 5% no Pix é pequeno diante da perda do direito de contestação junto à administradora, ainda mais porque a própria política de trocas prevê reembolso só por Pix.
- Guardar prints do produto, do preço, do prazo e de toda a conversa de atendimento antes de fechar o pedido.
- Ao receber, conferir se a nota fiscal traz um dos CNPJs divulgados e se o produto tem rotulagem de importação regular.
- Se houver problema: reclamar em **consumidor.gov.br** e no Procon citando os dois CNPJs constatados, e acionar o banco caso o pagamento tenha sido por cartão.

Recomendações de mitigação / denúncia

- Ao responsável pela loja: unificar a identificação societária - o rodapé injetado por JavaScript nomeia empresa diferente da que consta nas páginas legais.
- Corrigir a política de privacidade, que declara responsabilidade sobre kerassys.com, e esclarecer publicamente a relação entre os dois domínios.
- Publicar, se houver, a condição de distribuidor autorizado da marca Kerasys no Brasil, ou deixar claro tratar-se de revenda.
- Ao fabricante titular da marca **Kerasys**: avaliar as medidas de proteção de marca que entender cabíveis quanto ao uso do nome em kerasysbrasil.com e kerassys.com.
- 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 domínio na data indicada (coleta em 12/09/2026). A classificação expressa um **juízo técnico de risco** e não substitui decisão de autoridade policial, administrativa, regulatória ou judicial. A divergência entre os responsáveis declarados é um **fato constatado nas páginas**; este laudo não afirma que qualquer das empresas nomeadas tenha praticado ilícito, nem que a outra desconheça a operação. Não se imputa conduta ilícita aos provedores de infraestrutura citados (GoDaddy, Cloudflare, Mailgun) nem ao fabricante titular da marca Kerasys.*

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	275ff2d9025c357b801a12e1718ad0e0265f06308abe32acf6434492d5d361dc
cnpj_publico_58148688000131.json	c7cb6c9b403d0a9f36339b4e07aa4da77a826a86d1d3b679e67e157111c9b4b2
cnpj_publico_60774416000199.json	52a0f99c11fac95b8931f244e529f5e821b3aa0a7e6119906a3b934f1c83ca1d
corpo_carrinho.html	dd020721115f7a843ca436ea2bac166cffa5569e253e19d9360e3bd808f36ed
corpo_contato.html	932a96cc6fc91dfbed1548c09a06ce11a9f3028f3d392e3e40894eafaa831163
corpo_finalizar-compra.html	05d70f75355712604e2dd222e5a0724d14936bf6294f4b90c6116a5ce87ff20d
corpo_home.html	9db54137ede2180e0686ae6ce61039a2fd96234a287ed7d2028f44abe5a4f4dc
corpo_kerassys_com.html	f377664f123b8f29f5cf51566dee1df46cc65426d6271c0633232aee26343454
dns_records.txt	7568a081a31ec6692bd7161bbec4b598060f1ef88f3fa111809dc9fdbc01e53c
geoip.json	29feac9d570262b63310704b01716ba1df9f72d6c1f999875cb2eed15d343422
headers_home.txt	aee3d70656a4786a049e686a46640133f9ec9ea9008d4832ff0ac4b1dd650487
pg_contato.html	ee74b6b85ecf53214b663e5ef506e4e8602ade32d38cbf684c60b5eeb6320104
pg_fale-conosco.html	2f024f9ab2f4ff6774e23b3ea77c5951967f6a3b0a414599085fb8d7a23776af
pg_politica-de-privacidade.html	3bd395cc3eef741892727dadce1e103525900893ea1c5456977f81bb0e7c1f010
pg_trocas-e-devolucoes.html	b8e62df03e1b45ef7609a06b2eb5efcbf84d6adb787911b545b279a9c9179271
rdap_raw.json	78f285fdfb1bcb197ec403b458a7855cb70c05690a47347a24cbd027513d74b
tls_cert.txt	8237f595df81df34824d9dd18dc3dcbac2fdce9496673bdabfec6dfd38e23d48

- Fim do relatório -