



RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

lojasultrabrazil.com

Objeto investigado	lojasultrabrazil.com - loja virtual assinada como "Ultrafarma", com catálogo de dermocosméticos, fraldas, maquiagem e produtos de higiene
Natureza	Verificação de vínculo com a marca declarada 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	Domínio de 5 dias , hospedado na Moldávia , que se assina "Ultrafarma" no rodapé mas declara três identidades societárias diferentes e conflitantes entre suas páginas legais, com e-mails em domínios de terceiros e o mesmo número de telefone repetido em dois DDDs distintos
Classificação	RISCO ALTO
Emissão do laudo	12/09/2026 as 00:53

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **lojasultrabrasil.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 em português cujo título é simplesmente **"Ultrafarma - Ultrafarma"** e cujo rodapé assina **"© 2026 Ultrafarma. Todos os direitos reservados."**. O catálogo mistura dermocosméticos de marcas conhecidas (Avène, Vichy), fraldas, maquiagem, suplementos e itens de higiene, com preços "de/por" e parcelamento.

O achado central é a **incoerência da identidade societária**. O site não declara um responsável, declara **três**, em páginas diferentes e sem qualquer relação explicada entre eles: (i) o rodapé de todas as páginas traz **CNPJ 62.093.455/0010-47**, e-mail contato@ultrafarmassp.com e endereço na Avenida Cupece, São Paulo/SP; (ii) os "Termos e Condições de Uso" identificam a operadora como **"Deluxe Comércio"**, **CNPJ 66.654.649/0001-34**, em Salvador/BA, com e-mail deluxecomercio@sac.com e site deluxecomercio.com; (iii) a marca ostentada em todo o site é **Ultrafarma**, que não corresponde a nenhum dos dois. Na base pública da Receita Federal, o primeiro CNPJ é da **DROGA VIVER COM SAUDE LTDA** (nome fantasia "Ultrafarma Popular", ativa desde 2021, São Paulo/SP) e o segundo é da **DELUXE BEAUTY COMERCIO VAREJISTA LTDA** (Salvador/BA, aberta em **06/05/2026**, ramo de cosméticos). São empresas distintas, em estados distintos, com ramos distintos.

Os contatos ampliam a inconsistência. O telefone do rodapé é **(11) 98825-1598** e o dos termos é **(71) 98825-1598 - os mesmos oito dígitos sob dois DDDs diferentes**, o que nenhum operador de telefonia entrega. Os e-mails divulgados estão em domínios que não são o da loja: ultrafarmassp.com, registrado em 27/08/2026, e deluxecomercio.com, registrado em 01/06/2026 e sem registro A na coleta - ou seja, um endereço de e-mail apontado para um domínio que não está publicado.

A infraestrutura é o último elemento. O domínio foi registrado em **07/09/2026, 5 dias** antes da coleta, na NameSilo, com **titular oculto**, DNS na Openprovider e servidor no IP 91.208.184.158, da **ALEXHOST SRL, em Chisinau, Moldávia** - hospedagem fora do Brasil e fora do alcance prático da fiscalização e das ordens judiciais brasileiras, para uma loja que se apresenta como rede varejista nacional. O site ainda carrega o plugin hostinger-reach, resíduo de construção em outra hospedagem antes da mudança para a Moldávia.

CLASSIFICAÇÃO DE RISCO

RISCO ALTO

Leitura: uma loja de **5 dias**, hospedada na **Moldávia**, que se assina "Ultrafarma" mas declara **três identidades societárias conflitantes**, publica e-mails em domínios de terceiros (um deles sequer no ar) e repete o mesmo número de telefone em dois DDDs, oferece **risco elevado**. Recomenda-se **não comprar, não pagar e não fornecer CPF ou dados de cartão** (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 resolvidor 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	lojasultrabrazil.com (gTLD .com - registro Verisign)
Registro	07/09/2026 · expira 07/09/2027 (validade de 1 ano)
Idade na coleta	5 dias - domínio recém-criado
Titular	Oculto no RDAP (o registro expõe apenas o registrador)
Registrador	NameSilo, LLC (IANA 1479) · abuse@namesilo.com
Status	clientTransferProhibited
Servidores de nome	ns1.openprovider.nl · ns2.openprovider.be · ns3.openprovider.eu
DNS - A	91.208.184.158 · sem AAAA · sem MX · sem TXT
Hospedagem	AS200019 ALEXHOST SRL · Chisinau, Moldávia (MD)
PTR reverso	lojasultrabrazil.com
Servidor web	Server: nginx
Certificado TLS	CN=lojasultrabrazil.com · emissor Let's Encrypt YR2 (DV) · válido 07/09/2026-06/12/2026
Emissão do TLS	no mesmo dia do registro do domínio
Plataforma	WordPress 6.8.7 + WooCommerce 10.4.3 · tema woodmart · plugins Elementor Pro, hostinger-reach, woo-custom-installments
CNPJ do rodapé	62.093.455/0010-47 - válido · DROGA VIVER COM SAUDE LTDA ("Ultrafarma Popular"), ativa desde 07/07/2021, São Paulo/SP
CNPJ dos termos	66.654.649/0001-34 - válido · DELUXE BEAUTY COMERCIO VAREJISTA LTDA, aberta em 06/05/2026, Salvador/BA
Marca exibida	Ultrafarma - não corresponde a nenhum dos dois CNPJs declarados

Leitura técnica. Registro de 5 dias, titular oculto, ausência de MX e hospedagem em **Chisinau, Moldávia** compõem um perfil de **baixa rastreabilidade e baixa exequibilidade**: uma loja que se apresenta como varejo nacional brasileiro não tem razão operacional para servir de um provedor moldavo, e essa escolha dificulta na prática notificações, ordens de remoção e produção de provas. O certificado DV gratuito comprova apenas o controle do domínio, **não a identidade de qualquer entidade**. Não se imputa conduta à NameSilo, à Openprovider nem à AlexHost, meras provedoras de registro, DNS e hospedagem.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site é uma **loja WooCommerce** em português com árvore de categorias muito extensa (dermocosméticos, hidratantes, protetores solares, fraldas, maquiagem, suplementos, higiene bucal), lista de desejos, comparador e área do cliente. Chama atenção a **duplicação repetida de categorias** - "Hidratantes", "Protetores Solares" e "Fraldas" aparecem dezenas de vezes no menu -, sinal de catálogo importado em massa, sem curadoria. As páginas legais (Quem somos, Trocas e devoluções, Política de Reembolso, Privacidade, Frete, Termos) existem, mas é justamente nelas que as identidades divergem. Na coleta, com carrinho vazio, o checkout não expôs o intermediário de pagamento; não houve compra nem envio de dados.

Aspecto	Constatação
Tipo de site	Loja online de dermocosméticos, higiene, maquiagem e produtos infantis voltada ao público brasileiro
Marca exibida	"Ultrafarma" no título da página e no rodapé ("© 2026 Ultrafarma")
Identidade nº 1 (rodapé)	CNPJ 62.093.455/0010-47 - DROGA VIVER COM SAUDE LTDA ("Ultrafarma Popular"), São Paulo/SP, Av. Cupece 1277
Identidade nº 2 (termos)	CNPJ 66.654.649/0001-34 - DELUXE BEAUTY COMERCIO VAREJISTA LTDA , Salvador/BA, aberta em 06/05/2026
Identidade nº 3 (marca)	Ultrafarma - rede de farmácias conhecida, que não corresponde a nenhum dos CNPJs declarados
Telefones	(11) 98825-1598 e (71) 98825-1598 - mesmos oito dígitos em dois DDDs diferentes
E-mails de contato	Em domínios de terceiros: contato@ultrafarmassp.com (reg. 27/08/2026) e deluxecomercio@sac.com
Site citado nos termos	deluxecomercio.com - registrado 01/06/2026, sem registro A na coleta (fora do ar)
Hospedagem	Moldávia (AlexHost, Chisinau) - fora do alcance prático da fiscalização brasileira
Idade do domínio	5 dias na data da coleta, titular oculto
Catálogo	Categorias duplicadas dezenas de vezes no menu - importação em massa sem curadoria
Resíduo de construção	Plugin hostinger - reach presente, embora o site esteja hospedado na Moldávia

Leitura técnica. O elemento decisivo aqui não é um único dado falso, mas a **impossibilidade de saber com quem se está negociando**. Uma loja legítima tem um CNPJ, um endereço e um canal de contato - este site tem três identidades que não se explicam entre si, duas delas de empresas reais e uma terceira que é apenas uma marca conhecida usada como assinatura. Nesse arranjo, uma eventual disputa não tem destinatário: o consumidor não sabe se reclama à drogaria de São Paulo, à empresa de cosméticos de Salvador ou à rede cujo nome está no rodapé. O número de telefone repetido em dois DDDs e o e-mail apontado para um domínio fora do ar mostram que os contatos **não foram feitos para funcionar**. A hospedagem na Moldávia fecha o quadro, reduzindo na prática qualquer chance de remoção rápida ou de identificação do operador. A coleta foi passiva: nenhuma compra foi feita e nenhum dado pessoal enviado.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Três identidades societárias diferentes e conflitantes entre rodapé, termos de uso e marca exibida	corpo_termos.html · corpo_home.html · corpo_quem_somos.html	ALTA
2	Uso da marca "Ultrafarma" como assinatura do site sem corresponder a nenhum dos CNPJs declarados	corpo_home.html	ALTA
3	Domínio registrado 5 dias antes da coleta, titular oculto, validade de 1 ano	rdap_raw.json	ALTA

4	Hospedagem em Chisinau, Moldávia (AlexHost), para loja que se apresenta como varejo nacional brasileiro	geoip.json	ALTA
5	Mesmo número de telefone declarado sob dois DDDs diferentes - (11) e (71)	corpo_termos.html · corpo_home.html	ALTA
6	E-mails de contato em domínios de terceiros, um deles (deluxecomercio.com) sem registro A na coleta	corpo_termos.html · dados.json	MEDIA
7	Domínio sem MX próprio - a loja não tem servidor de e-mail no próprio endereço	dns_records.txt	MEDIA
8	Catálogo com categorias duplicadas dezenas de vezes, indicando importação em massa sem curadoria	corpo_home.html	MEDIA
9	Certificado TLS DV gratuito emitido no mesmo dia do registro do domínio	tls_cert.txt	BAIXA
10	Plugin hostinger-reach remanescente em site hospedado na Moldávia - resíduo de construção anterior	corpo_home.html	BAIXA

Síntese: 5 indicadores de severidade ALTA, 3 MEDIA e 2 BAIXA. **Nenhum fator de legitimidade consistente** foi constatado: embora dois CNPJs válidos apareçam no site, eles apontam para empresas distintas, em estados distintos, e nenhum deles corresponde à marca sob a qual a loja se apresenta.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em **12/09/2026**, conclui-se que **lojasultrabrazil.com** apresenta **risco alto ao consumidor**. O site vende dermocosméticos, produtos de higiene e itens infantis assinando-se "**Ultrafarma**", mas não é possível determinar quem o opera: o rodapé declara o CNPJ da **DROGA VIVER COM SAUDE LTDA** (São Paulo/SP), os termos de uso declaram a **DELUXE BEAUTY COMERCIO VAREJISTA LTDA** (Salvador/BA, aberta quatro meses antes) e a marca ostentada é de uma terceira empresa. Os canais de contato não sustentam nenhuma dessas versões - o mesmo número de telefone aparece sob dois DDDs, e um dos e-mails aponta para um domínio fora do ar. O domínio tem **5 dias**, titular oculto, e está hospedado em **Chisinau, Moldávia**, arranjo sem justificativa operacional para um varejo brasileiro e que dificulta notificação e responsabilização. Não se imputa conduta às empresas cujos CNPJs aparecem exibidos: o que se constata é que **o vínculo entre elas e este site não está demonstrado**. Recomenda-se **não comprar neste endereço**.

Recomendações ao consumidor / solicitante

- **Não comprar, não se cadastrar e não fornecer CPF, endereço ou dados de cartão** ao site.
- Antes de qualquer compra online, conferir se o **CNPJ do rodapé e o dos termos de uso são o mesmo** - divergência entre eles é sinal de alerta imediato.
- Checar o CNPJ declarado na base pública da Receita Federal e confirmar se o ramo de atividade bate com o que a loja vende.
- Desconfiar de lojas que usam o nome de uma rede conhecida como assinatura sem que esse nome apareça no CNPJ declarado.
- Se já houve pagamento: acionar o banco e o mecanismo **MED** do Pix imediatamente, reunir comprovantes e registrar Boletim de Ocorrência e reclamação em **consumidor.gov.br**.

Recomendações de mitigação / denúncia

- Denunciar o domínio aos canais de abuse do registrador (abuse@namesilo.com), do DNS (Openprovider) e da hospedagem (AlexHost), anexando este laudo.
- Comunicar as empresas cujos CNPJs aparecem exibidos, para que avaliem as medidas cabíveis quanto ao uso de seus dados.

- Comunicar a titular da marca **Ultrafarma** o uso do nome como assinatura do site, para as medidas de proteção de marca que entender cabíveis.
- Denunciar em conjunto os domínios correlatos identificados neste lote (lojaoficialultrafarma.com, ultrafarmassp.com, ofertasultrafarma.com, ultrafarmabrasil.com), evidenciando o padrão.
- Preservar este relatório e as evidências (pasta evidencias/, com hashes SHA-256) para eventual uso administrativo ou judicial.

*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. Não se imputa conduta ilícita aos provedores de infraestrutura citados (NameSilo, Openprovider, AlexHost) nem às empresas **DROGA VIVER COM SAUDE LTDA, DELUXE BEAUTY COMERCIO VAREJISTA LTDA** e à titular da marca **Ultrafarma**, cujos dados aparecem exibidos **sem que se possa afirmar qualquer vínculo entre elas e o domínio investigado**.*

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	d2e7cb4baa27bda65addf7678cc444d5d39f5a7c55e648a26889271148a77451
cnpj_publico_62093455001047.json	01fd59ee89bf3ed62a711e205586238094883cd6c528d31530ec2391a6a03d9c
cnpj_publico_66654649000134.json	d7992278d215efe37da7c854f0f8335862069b5f384130c53f13177e6b57a1b2
corpo_carrinho.html	1e24c5f20aeb86c29a1e4679dc4716e7136d3953caaf73beaff9ddb763784b59
corpo_checkout.html	6f539221ebd4598ba880ea23e263199159ac77a49d72a2462eec2dfcb0d44c62
corpo_home.html	3b8d0eed83cac591f7fd2346580dcc16755193501fc66f3c3a4da159756cc408
corpo_politica_de_privacidade.html	f6da7f00c4bd5dc1b2cb824f903fe1a7730610abc6cb12c30b5532c6e2eb7c78
corpo_quem_somos.html	44728b31ce48d7c7db28e5d0398b1ce08220b31a6bd87a2b3b1d252fd2557491
corpo_termos.html	66267e80fa44eb467e746cc95c2a6804ca45f365a7134501f6eb8b391f578dd5
dns_records.txt	a0c99d6aa165796a0306adddf845034d0dff3ddfae5e2b4ca54605599db2e7d3
geoip.json	d63f88148625ba3a307fd47cfff9979fc42333d11dcb29eb937b14e5e2c91c3b8
headers_home.txt	41a3314e4346bc79f9ebd3c0c704d27594f6c068201bc752a691113ae6bd9b69
rdap_raw.json	63331bfdf3aed388646f7dea13b308af47f685ba7e7ffb84f42a01b55737ca63
tls_cert.txt	25c81057eaefc250ad8c9fac1fd635a7e8a6b2fb679f4b70d56869fe9ac7699c

- Fim do relatório -