



RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

lojaoficialultrafarma.com

Objeto investigado	lojaoficialultrafarma.com - loja virtual que se apresenta como a "Ultrafarma", rede de farmácias brasileira, e vende medicamentos, dermocosméticos e suplementos
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 registrado 4 dias antes da coleta, com titular oculto, que reproduz a identidade completa da Ultrafarma - CNPJ, Inscrição Estadual, AFE, SIVISA e nomes de farmacêuticas responsáveis com número de CRF - sem qualquer vínculo demonstrado com a empresa titular desses registros
Classificação	RISCO ALTO
Emissão do laudo	12/09/2026 as 00:53

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **lojaoficialultrafarma.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 virtual WordPress/WooCommerce inteiramente vestida com a identidade da **Ultrafarma**, rede de farmácias amplamente conhecida no Brasil. O título da página é copiado literalmente da rede - "*Ultrafarma - Tá no coração da gente!*" -, o texto de "Quem Somos" reproduz o institucional da empresa ("Uma marca fundada em 2000, que revolucionou o setor de comercialização de medicamentos com a venda de genéricos...") e o catálogo oferece medicamentos, dermocosméticos, vitaminas, protetores solares e produtos infantis, com preços à vista no **Pix** e parcelamento no cartão.

O achado central está nas páginas legais. Os "Termos e Condições de Uso" trazem um bloco intitulado "Informações da Empresa" que estampa **toda a identidade regulatória da Ultrafarma**: razão social "Ultrafarma Saúde", **CNPJ 02.543.945/0006-90**, Inscrição Estadual 130.762.850.113, **AFE 780.2129** (Autorização de Funcionamento de Empresa, ANVISA), **SIVISA 354680110-477-000062-1-1** (vigilância sanitária estadual), endereço em Santa Isabel/SP, telefone (11) 5070-1900 e, no rodapé, até os **nomes de duas farmacêuticas responsáveis com seus números de CRF-SP**. O CNPJ é válido pelo módulo 11 e, na base pública da Receita Federal, corresponde de fato a **ULTRAFARMA SAUDE LTDA**, ATIVA desde 05/06/2007, em São Paulo/SP, com CNAE de comércio varejista de produtos farmacêuticos. Ou seja: os dados são reais - mas são **dados de outra empresa**.

Nada na coleta liga esse domínio à empresa cujos registros ele exhibe, e vários elementos apontam no sentido contrário. O domínio foi registrado em **08/09/2026**, apenas **4 dias** antes da coleta, na NameSilo, com **titular oculto**; está hospedado em um VPS avulso da Hostinger (PTR srv1961176.hstgr.cloud) e usa certificado TLS gratuito emitido no mesmo dia. A Ultrafarma real opera há anos em **ultrafarma.com.br**, em infraestrutura própria e distinta. Um domínio com quatro dias de vida não pode ter acumulado o histórico institucional que o texto descreve.

Os canais de contato reforçam o quadro. Os e-mails divulgados não estão no domínio da loja nem no da Ultrafarma verdadeira, mas em **dois outros domínios parecidos e igualmente recentes**: **atendimento@ofertasultrafarma.com** (domínio registrado em 18/08/2026) e **atendimento@ultrafarmabrasil.com** (20/06/2026), ambos ativos e hospedados na SiteGround. Somado ao **lojasultrabrasil.com**, investigado em separado neste mesmo lote, e ao **ultrafarmassp.com** (27/08/2026), desenha-se um **conjunto de domínios sucessivos explorando a mesma marca**, criados ao longo de poucos meses.

CLASSIFICAÇÃO DE RISCO

RISCO ALTO

Leitura: um domínio de **4 dias**, com titular oculto, que copia título, texto institucional, CNPJ, Inscrição Estadual, AFE, SIVISA e até os CRF das farmacêuticas responsáveis de uma rede de farmácias real, e cujos e-mails de contato ficam em **outros domínios parecidos**, oferece **risco elevado** - agravado por vender medicamentos. Recomenda-se **não comprar, não pagar por Pix 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	lojaoficialultrafarma.com (gTLD .com - registro Verisign)
Registro	08/09/2026 · expira 08/09/2027 (validade de 1 ano)
Idade na coleta	4 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.srv1961176.hstgr.cloud · ns2.srv1961176.hstgr.cloud (VPS Hostinger)
DNS	A 2.25.177.122 · MX apontando para o próprio domínio · SPF v=spf1 ip4:2.25.177.122 +a +mx ~all
Hospedagem	AS47583 Hostinger International · VPS avulsa
PTR reverso	srv1961176.hstgr.cloud - VPS sem identidade corporativa
Servidor web	Server: nginx
Certificado TLS	CN=*.lojaoficialultrafarma.com · emissor Let's Encrypt YR1 (DV) · válido 08/09/2026-07/12/2026
Emissão do TLS	no mesmo dia do registro do domínio
Plataforma	WordPress + WooCommerce · tema bevesi · plugins Elementor, Contact Form 7, Google Site Kit, woo-custom-installments
CNPJ declarado	02.543.945/0006-90 - válido, mas pertence a ULTRAFARMA SAUDE LTDA (ATIVA desde 05/06/2007, São Paulo/SP) - vínculo com o site não demonstrado
Domínio da marca real	ultrafarma.com.br - infraestrutura distinta (IP 170.82.173.10)

Leitura técnica. Registro de 4 dias, validade de 1 ano, titular oculto e VPS avulsa compõem um perfil de **baixa rastreabilidade do responsável**, incompatível com a operação de uma rede de farmácias estabelecida - que precisaria, entre outros requisitos, de AFE da ANVISA e de responsável técnico farmacêutico vinculados à **pessoa jurídica que efetivamente opera o comércio**. O certificado DV gratuito comprova apenas o controle do domínio, **não a identidade de qualquer entidade**. Não se imputa conduta à NameSilo nem à Hostinger, meras provedoras de registro e hospedagem, tampouco à Ultrafarma Saúde LTDA, cujos dados aparecem exibidos **sem que se possa afirmar qualquer participação sua**.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site é uma **loja WooCommerce** completa em português, com catálogo por categorias (Ofertas, Cuidados Capilares, Vitaminas e Suplementos, Mamãe e Bebê, Higiene Pessoal, Skincare), carrinho, área de conta e páginas legais próprias (Quem Somos, Termos e Condições, Política de Privacidade). Cada produto exibe preço cheio, parcelamento no cartão e um **preço menor "no Pix"** - o desconto à vista que empurra o comprador para o meio de pagamento sem contestação. 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	Farmácia online voltada ao público brasileiro - medicamentos, dermocosméticos, vitaminas, produtos infantis
Marca explorada	Ultrafarma - título, logotipo textual e slogan "Tá no coração da gente!" copiados da rede real
Texto institucional	Página "Quem Somos" reproduz o institucional da rede ("Uma marca fundada em 2000, que revolucionou o setor...")
CNPJ exibido	02.543.945/0006-90 - da Ultrafarma Saúde LTDA , empresa real e ativa desde 2007; vínculo com o site não demonstrado
Registros sanitários exibidos	AFE 780.2129 · SIVISA 354680110-477-000062-1-1 · IE 130.762.850.113 - registros da empresa real
Responsáveis técnicas	Nomes de duas farmacêuticas com números de CRF-SP estampados no rodapé
E-mails de contato	Em outros domínios: atendimento@ofertasultrafarma.com (reg. 18/08/2026) e atendimento@ultrafarmabrasil.com (reg. 20/06/2026)
Telefone exibido	(11) 5070-1900 - número associado à empresa real
Idade do domínio	4 dias na data da coleta, com titular oculto
Meio de pagamento	Preço reduzido "no Pix" em todos os produtos, mais parcelamento no cartão
Domínios correlatos	ultrafarmabrasil.com · ofertasultrafarma.com · ultrafarmassp.com · lojasultrabrasil.com - todos de 2026
Único link à marca real	Uma URL de ultrafarma.com.br na política de privacidade, para "solicitar exclusão de cadastro"

Leitura técnica. O elemento decisivo é a **apropriação de identidade regulatória**. Exibir CNPJ, Inscrição Estadual, AFE da ANVISA, número SIVISA e o nome e o CRF de farmacêuticas responsáveis não é um detalhe estético: são exatamente os dados que um consumidor cuidadoso procura para confirmar que está comprando medicamento de uma farmácia habilitada. Quando esses dados pertencem a uma empresa que não é a operadora do site, o efeito é **inverter a checagem de segurança contra o próprio consumidor**. O risco aqui não se limita à perda do valor pago: envolve **medicamentos de origem não verificada** e a entrega de CPF, endereço e dados de pagamento a um responsável não identificado. O desconto "no Pix", presente em todos os produtos, empurra o comprador para o meio de pagamento que **não admite contestação**. A coleta foi passiva: nenhuma compra foi feita e nenhum dado pessoal enviado.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Exibição do CNPJ, IE, AFE/ANVISA, SIVISA e CRF de farmacêuticas de uma rede de farmácias real, sem vínculo demonstrado	corpo_termos.html · corpo_home.html	ALTA
2	Domínio registrado 4 dias antes da coleta, titular oculto, validade de 1 ano	rdap_raw.json	ALTA

3	Cópia do título, do slogan e do texto institucional da marca real	corpo_home.html · corpo_quem_somos.html	ALTA
4	Venda de medicamentos e dermocosméticos por operador não identificado	corpo_home.html	ALTA
5	E-mails de atendimento em dois outros domínios recentes que também exploram a marca	corpo_termos.html · corpo_home.html	ALTA
6	Conjunto de domínios sucessivos com a mesma marca (ultrafarmabrasil.com, ofertasultrafarma.com, ultrafarmassp.com, lojasultrabrasil.com)	rdap_raw.json · dados.json	MEDIA
7	Desconto "no Pix" em todos os produtos, favorecendo o meio de pagamento sem contestação	corpo_home.html	MEDIA
8	Hospedagem em VPS avulsa (PTR srv1961176.hstgr.cloud), sem identidade corporativa	geoip.json · dns_records.txt	MEDIA
9	Certificado TLS DV gratuito emitido no mesmo dia do registro do domínio	tls_cert.txt	BAIXA
10	Domínio .com genérico para operação brasileira de farmácia, enquanto a marca real usa .com.br	rdap_raw.json	BAIXA

Síntese: 5 indicadores de severidade ALTA, 3 MEDIA e 2 BAIXA. **Nenhum fator de legitimidade próprio** foi constatado: toda a identificação exibida pertence a terceiro, e não há CNPJ, endereço, e-mail ou responsável verificável ligado a quem de fato opera o domínio.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em **12/09/2026**, conclui-se que **lojaoficialultrafarma.com** apresenta **risco alto ao consumidor**. O site vende medicamentos, dermocosméticos e suplementos ao público brasileiro sob a marca **Ultrafarma**, reproduzindo o título, o slogan e o texto institucional da rede e estampando, nas páginas legais, a **identidade regulatória completa de uma empresa real** - CNPJ 02.543.945/0006-90, Inscrição Estadual, AFE da ANVISA, número SIVISA e os nomes e CRF de duas farmacêuticas responsáveis. Nenhum elemento da coleta liga o domínio a essa empresa: ele foi registrado **4 dias antes**, tem titular oculto, roda em VPS avulsa e divulga e-mails de atendimento em **outros dois domínios recentes** que também exploram a marca. O conjunto caracteriza **apropriação de identidade de terceiro** - e não se imputa aqui qualquer conduta à Ultrafarma Saúde LTDA, que aparece como **marca e registros usados sem vínculo demonstrado**. O desconto no Pix em todo o catálogo direciona o comprador ao meio de pagamento sem contestação. Recomenda-se **não comprar neste site** e conferir sempre o endereço oficial da rede antes de qualquer pagamento.

Recomendações ao consumidor / solicitante

- **Não comprar, não se cadastrar e não fornecer CPF, endereço ou dados de cartão** ao site.
- **Evitar o Pix:** o desconto anunciado à vista direciona ao único meio de pagamento sem direito a contestação junto à administradora.
- Comprar medicamentos apenas em farmácia com **AFE e responsável técnico vinculados a quem efetivamente vende** - conferir o endereço oficial da rede digitando-o à mão no navegador, sem clicar em links de anúncios ou mensagens.
- Desconfiar de domínios que combinam o nome de uma rede conhecida com palavras como "loja", "oficial", "ofertas" ou "brasil": a rede real usa um endereço só.
- 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 e da hospedagem (abuse@namesilo.com, abuse@hostinger.com), anexando este laudo.
- Comunicar a **Ultrafarma Saúde LTDA**, titular da marca e dos registros exibidos, para as medidas de proteção de marca que entender cabíveis.
- Comunicar a **ANVISA e a vigilância sanitária estadual** a oferta de medicamentos por site que exhibe AFE e SIVISA de terceiro.
- Denunciar em conjunto os domínios correlatos (ultrafarmabrasil.com, ofertasultrafarma.com, ultrafarmassp.com, lojasultrabrasil.com), evidenciando o padrão de repetição.
- 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, Hostinger, SiteGround) nem à **Ultrafarma Saúde LTDA** e às profissionais nomeadas no rodapé do site, 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	275ff2d9025c357b801a12e1718ad0e0265f06308abe32acf6434492d5d361dc
cnpj_publico_02543945000690.json	f67bdd39737551f333b8d8ce372c4f7b2ee2616921f2214acac1149ef7e73107
corpo_cart.html	717be85067cf1a0361f952678d3cc388de3f0aa4faaa7d3474675792998eb355
corpo_checkout.html	6a1593cb3369d790b72556d9990b42906622b4e9a00a77903c4df0ad8b5cc457
corpo_home.html	dfead4076a0e5807856acd4f94f4980104ca0f0e4d9fcefca7f1c2a0b5bf88b
corpo_politica_de_privacidade.html	13db8e85a319ec4e1e192bf8a292bc52233ffc83aa1cd35a52a1baefac79d68f
corpo_quem_somos.html	7056d0f7cdfb45d893c6b0296f2e6f31e2b352be1208194289b625e7e37dd542
corpo_termos.html	c9f8cb19ea21cae25aae72431d8f2fc2bca7a82bd13aba76a994c1c051bfdf57
dns_records.txt	2b6940a7262a04fca33711ac297857df58ea683e2cf2ca8647314ca29a092c54
geoip.json	98d2f05abbb0cbeab70033f9e6af02b5c4d4d1c2330877ac77ffaafc523b8a74
headers_home.txt	8971772c439e44e062c4f89e5e17f709c7eccc706d23406e5b6db3c5c7035d22
rdap_raw.json	3b2a88cdd4e780db7a2d32675d1d7cffe907dd3b7107b173e29bbe01e97a176b
tls_cert.txt	2dea32e87c271ee8ffa6de58644b93c1455795f02cc80dc15ae419a62d7f5070

- Fim do relatório -