

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

comercialfpo.com

Objeto investigado	comercialfpo.com - loja online multicategoria (eletrodomésticos, ferramentas, móveis, automotivo)
Natureza	Verificação de legitimidade da loja, da empresa declarada e da infraestrutura
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 **14 dias**, em DNS e hospedagem de provedor que se apresenta como “offshore” (offsh.nl, servidor na Alemanha), operado em nome de uma empresa real de marketing direto de Cuiabá
Classificação	**RISCO MÉDIO**
Emissão do laudo	18/11/2026 as 00:54

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **comercialfpo.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 é uma loja genérica com quinze departamentos — de ar-condicionado a jardim e construção —, frete grátis para todo o Brasil “em 2 a 3 dias úteis” e 5% de desconto no Pix. O rodapé identifica FPO NEGOCIOS DIGITAIS LTDA, CNPJ 44.214.717/0001-01, com endereço em Cuiabá/MT que confere com a Receita.

A empresa existe desde 2021, mas sua atividade registrada é **marketing direto**, não varejo. O domínio foi criado em 03/11/2026 (Dynadot, titular oculto), com servidores de nome `ns3/ns4.offsh.nl` e hospedagem em cPanel/Apache no IP 45.151.91.170 (IP Vendetta Inc., Colônia/Alemanha, PTR `cp4.offsh.nl`) — um serviço de hospedagem que se identifica como “offshore”.

O telefone exibido difere em um dígito do registrado na Receita para a empresa, e a promessa de entrega nacional em 2 a 3 dias úteis para toda a vitrine é pouco realista para uma operação sem histórico.

CLASSIFICAÇÃO DE RISCO **RISCO MÉDIO**

Leitura: a empresa é real e o endereço confere, o que pesa a favor; mas o domínio é de dias, a atividade registrada não é de varejo e a infraestrutura escolhida (hospedagem “offshore”) dificulta a responsabilização. O vínculo operacional entre a empresa e esta loja não é demonstrado (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	comercialfpo.com
Registro	03/11/2026 · expira 03/11/2027 · **14 dias** antes da coleta
Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)

Registrador	Dynadot Inc · abuse@dynadot.com
Servidores de nome	ns3.offsh.nl · ns4.offsh.nl
DNS - A	45.151.91.170 · MX: mail.comercialfpo.com
Hospedagem	AS209101 IP Vendetta Inc. · Köln/DE · PTR/hostname `cp4.offsh.nl` · cabeçalho `server: Apache/2`
Certificado TLS	Let's Encrypt (YE2) · emitido em 03/11/2026 · válido até 01/02/2027
CNPJ exibido	44.214.717/0001-01 · FPO NEGOCIOS DIGITAIS LTDA · ativa desde 11/11/2021 · Cuiabá/MT (endereço confere) · CNAE principal **marketing direto** · capital R$ 10 mil · telefone na Receita (11) 3301-4012, o site exibe (11) 3301-4013

Leitura: domínio de 14 dias, titular oculto, DNS e servidor no mesmo provedor “offshore” na Alemanha, e-mail próprio com SPF via MailBaby.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Loja em PHP servida por Apache (cPanel), com rotas `/api/config` e `/api/feedset`. Não foram coletadas páginas de checkout além do código público da vitrine.

Aspecto	Constatação
Pagamento	Pix com 5% de desconto; demais meios não demonstrados na vitrine
Identidade	FPO NEGOCIOS DIGITAIS LTDA · CNPJ 44.214.717/0001-01 · R. Mistral, 332, Ed. The Point, sala 209 A, Cuiabá/MT · contato@comercialfpo.com · WhatsApp (11) 3301-4013
Promessas	Frete grátis nacional em 2 a 3 dias úteis; trocas em até 30 dias
Infraestrutura	Hospedagem “offshore” (offsh.nl) em Colônia/Alemanha

Leitura: antes de pagar, o comprador deve confirmar que o recebedor do Pix é FPO NEGOCIOS DIGITAIS LTDA; nome diferente indica que o pagamento não vai à empresa exibida.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Domínio de 14 dias, titular oculto	`rdap_raw.json`	ALTA
2	Hospedagem e DNS em provedor “offshore” no exterior	`dns_records.txt` · `geoip.json`	MEDIA
3	CNAE “marketing direto”, não varejo	`cnpj_publico_44214717000101.json`	MEDIA
4	Telefone do site difere do cadastrado na Receita	`cnpj_publico_*.json` · `corpo_home.html`	BAIXA
5	Entrega nacional em 2-3 dias para catálogo de 15 departamentos	`corpo_home.html`	BAIXA

Síntese: cinco indicadores, um de severidade alta. A identificação formal coerente reduz o risco, mas não o elimina.

6. Conclusão Técnica e Recomendações

A comercialfpo.com exibe dados corretos de uma empresa real, porém com atividade de marketing direto, num domínio de 14 dias hospedado em provedor “offshore” no exterior. O vínculo operacional entre a empresa e a loja não está demonstrado. Classificação técnica: **RISCO MÉDIO**.

Recomendações ao consumidor / solicitante

- Contate a empresa pelo telefone registrado na Receita para confirmar que a loja é dela antes de comprar.
- 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@dynadot.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
bundle_js.txt (20398 bytes)	a16be11bca80a7bea03741a6dd406c39d8f79171a6a2747306569c4f38c56628
cnpj_publico_44214717000101.json (2290 bytes)	f0f1fabcc71c016126de50028522c01a4b00224cad5b5ca072e26bb3e7d11720
corpo_home.html (28233 bytes)	6d51015ffde4b26b725d2f903b32b5cf7095a55b2fcb0b398205daa628f80e2b
dns_records.txt (421 bytes)	e059eaa7edab57bf12b4ad76fcef0e3eb55113a4e77c1062a91fa1a7b7823578
geoip.json (295 bytes)	57f11f78a59c8c4f3c05303ab179e62b253a54139790d475bb160920d549e097
headers_home.txt (457 bytes)	c83c123416885fdab6e6f9112ff33c66d2c04bacd008da8b0e9d8fb6046efc45
rdap_raw.json (2568 bytes)	3fc065a77f00ad263f71e083db1dcbbf47be0c66052298413036002ce5196cf6
tls_cert.txt (303 bytes)	c9deca500670cda2148969f0f8b5c13e7a6fa1a26e349e767eab5a16b39fbb17

- Fim do relatório -