RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

buquederosas.delivery

Objeto investigado	buquederosas.delivery — loja online de flores e buquês "Buquê de Rosas" (gTLD .delivery)
Natureza	Verificação de legitimidade e de risco ao consumidor (loja anunciada + pagamento PIX)
Data da coleta	12/07/2026 (RDAP, DNS, HTTP/TLS, análise do código, BR Code PIX, bases de CNPJ)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · decodificação EMV/BR Code do PIX · consulta CNPJ
Achado central	Recebedor do PIX (LEGACY DIGITAL LTDA) NÃO corresponde à loja nem ao CNPJ exibido no site
Classificação	**RISCO ALTO**
Emissão do laudo	12/07/2026 às 14:48

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **buquederosas.delivery**, realizada em **12/07/2026** 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. Toda evidência foi preservada em arquivo no momento da coleta e teve seu hash SHA-256 calculado.

O domínio **está no ar** e entrega a loja **"Buquê de Rosas"** — vitrine de flores e buquês com 348 produtos, promessa de "flores frescas montadas por floricultura parceira da cidade de destino", entrega no mesmo dia e frete grátis, servida atrás da **Cloudflare**. O pagamento é **exclusivamente via PIX**. O domínio foi **registrado em 12/06/2026 — 30 dias antes da coleta** — com **titular oculto**, e a loja capta clientes por **tráfego pago** (Google Ads, tag AW-18194665316).

O site declara, em marcação estruturada, pertencer a **OINCASH LTDA** (CNPJ 66.165.764/0001-45) — microempresa de **promoção de vendas e publicidade** de Brasília/DF, **aberta em 09/04/2026**, sem qualquer atividade (CNAE) de comércio de flores. Já o código PIX "copia e cola" gerado no checkout aponta como recebedor **LEGACY DIGITAL LTDA** (São Paulo/SP) — uma **terceira identidade**, que não corresponde nem à loja anunciada nem ao CNPJ exibido. A cobrança é emitida pelo agregador `pix.onlyup.com.br`, domínio registrado por **empresa individual de assessoria** (B2M Assessoria, São José dos Campos/SP), que não figura como instituição de pagamento autorizada pelo Banco Central — o dinheiro do consumidor, portanto, **não vai para a "floricultura"**, e sim para um beneficiário oculto atrás de um intermediário não regulado.

O checkout coleta **nome, CPF, e-mail, telefone e endereço completo** e transmite esses dados a um endpoint de "carrinho abandonado" **segundos após o preenchimento, antes de qualquer confirmação de compra**. O conjunto — domínio de 30 dias, três identidades divergentes, recebedor PIX incompatível, agregador opaco e coleta antecipada de dados — compõe perfil típico de **loja-fantasma de flores** (produto pago e não entregue).

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: quando o recebedor do PIX não é a loja — nem a empresa que a loja declara ser —, o consumidor paga a um terceiro sem vínculo verificável com o produto prometido. Somado ao domínio recém-criado e à coleta de dados pessoais, o risco ao consumidor é **elevado**. Recomenda-se **não comprar e não pagar** (Seção 6).

2. Metodologia e Cadeia de Custódia

Empregaram-se exclusivamente **técnicas passivas**: RDAP, DNS (resolvedor público 1.1.1.1), requisições HTTP/TLS de visitante comum, download e leitura do código JavaScript público do site, decodificação do BR Code PIX (padrão EMV/TLV, com validação do CRC16) e consulta a bases públicas de CNPJ. As respostas foram salvas no momento da coleta e tiveram hash SHA-256 calculado, compondo a cadeia de custódia. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (Identity Digital / .delivery)	`rdap_raw.json`
DNS	dig @1.1.1.1 (A, AAAA, NS, MX, TXT, SOA, www)	`dns_registros.txt`
Conteúdo / cabeçalhos	curl (HTTPS, User-Agent de navegador)	`corpo.html · headers.txt · checkout.html · pagamento.html`
Aplicação (front-end)	Download dos scripts públicos do site	`home.js · checkout.js · catalog.json · reviews.json`

Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização de IP	ip-api.com · PTR reverso	`dns_registros.txt (seção geo)`
Código PIX	Decodificação EMV/TLV + CRC16 · payload dinâmico (JWS) do agregador	`pix_copiaecola.txt · pix_payload_jws.txt`
Intermediário PIX	RDAP registro.br (onlyup.com.br · almeidapay.com.br) + DNS	`rdap_onlyup.com.br.json · rdap_almeidapay.com.br.json`
CNPJ	Bases públicas da Receita (BrasilAPI · OpenCNPJ)	consultas registradas no laudo
Imagens / metadados	Download de amostra do catálogo · exiftool	`imagens/ · metadata_exiftool.txt`

3. Identificação Técnica (Domínio, DNS, Hospedagem e TLS)

Domínio	buquederosas.delivery (gTLD .delivery — Identity Digital)
Registro	**12/06/2026** · expira 12/06/2027 (validade mínima de 1 ano)
Idade na coleta	**30 dias** — domínio muito recente
Titular	**Oculto** (dados do registrante redigidos no RDAP)
Registrador	Dynadot Inc (abuse@dynadot.com · +1.650.262.0100)
Status	clientTransferProhibited
Servidores de nome	jamie / miguel.ns.cloudflare.com (Cloudflare)
DNS — A / AAAA	104.21.55.175 · 172.67.149.184 (+IPv6) — IPs de borda da Cloudflare
MX / TXT	Cloudflare Email Routing (route1–3.mx.cloudflare.net) · SPF Cloudflare · google-site-verification
Hospedagem (borda)	AS13335 Cloudflare, Inc. — **proxy/CDN que oculta o IP de origem**
Geolocalização do IP	Anycast Cloudflare (não revela a localização do servidor real)
Certificado TLS	CN=buquederosas.delivery · emissor Google Trust Services WE1 (DV, via Cloudflare) · válido 12/06/2026–10/09/2026
Série / Fingerprint	5333899FA8B377311305F1E3C9397DCE · SHA-256 96:AE:01:62:85:6F:93:33:4F:6E:7A:71:F4:74:FC:06:62:FD:65:DF…

Leitura técnica. O certificado TLS foi emitido **no mesmo dia do registro do domínio** (12/06/2026): o site inteiro nasceu há um mês. Registro recente, titular oculto e Cloudflare como proxy compõem um perfil de **baixa rastreabilidade do responsável** — o IP de origem, que efetivamente processa pedidos e gera as cobranças PIX (rotas `/api/…` na mesma origem), permanece oculto. O certificado DV comprova apenas o controle do domínio, **não a identidade de qualquer empresa**. O e-mail `contato@buquederosas.delivery` usa o encaminhador gratuito da Cloudflare, sem caixa corporativa própria. Não se imputa conduta ao registrador (Dynadot) nem à Cloudflare, meros provedores de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

A loja é uma vitrine profissional em pt-BR: catálogo com **348 produtos** (`/data/catalog.json`), busca, cupons, "order bump" de upsell, integração com Google Ads/GA4 (com "enhanced conversions" e captura de UTMs de anúncios) e consulta de CEP via ViaCEP. O modelo anunciado é de intermediação: "flores montadas por floricultura parceira da cidade de destino" — nenhuma floricultura é identificada. O arquivo de avaliações (`reviews.json`) está **vazio**. No rodapé/marcação estruturada (schema.org), o site declara `legalName: OINCASH LTDA · taxID: 66.165.764/0001-45`.

Identidades societárias envolvidas

Papel	Identidade	Constatação (bases públicas da Receita)
Loja anunciada	"Buquê de Rosas" (buquederosas.delivery)	Marca sem CNPJ próprio; "floricultura parceira" jamais nomeada
Empresa declarada no site	OINCASH LTDA · CNPJ 66.165.764/0001-45	ME de **promoção de vendas / publicidade / marketing direto**, Brasília/DF, aberta em **09/04/2026**; nenhum CNAE de comércio de flores
Recebedor do PIX	**LEGACY DIGITAL LTDA** · São Paulo/SP	Nome que **não corresponde** nem à loja nem à empresa declarada; CNPJ não exposto no código PIX (chave aleatória)

Decodificação do código PIX "copia e cola" (EMV/BR Code)

GUI (campo 26-00)	br.gov.bcb.pix — arranjo PIX oficial do Banco Central
URL do payload (26-25)	`pix.onlyup.com.br/qr/v3/at/0634b323-98e7-43cf-a378-9ea9d92b41c5` (QR dinâmico)
MCC (52)	0000 — comerciante **não categorizado** (floricultura seria 5992)
Moeda / País (53 · 58)	986 (BRL) · BR
Recebedor (59)	**LEGACY_DIGITAL_LTDA**
Cidade (60)	SAO_PAULO
CRC16 (63)	CAE2 — **validado** (código íntegro e pagável)
Payload dinâmico (JWS)	cobrança ATIVA criada em 12/07/2026 13:44 UTC · valor **R$ 69,90** · chave PIX aleatória 40b8ca0f-5584-4109-9644-e98dc5e50f3c · txid 9932f6b1fc4d96843d1fc8e024d78b
"Devedor" na cobrança	"Fulano de Tal", CPF 346.095.350-09 — **dados fictícios/de amostra** registrados pelo gerador da cobrança

Intermediário de pagamento

O QR dinâmico é servido por `pix.onlyup.com.br`, que aponta (CNAME) para `onlyup-prod.onz.software` — software de emissão PIX da ONZ — hospedado em AWS São Paulo (54.94.248.228). O domínio **onlyup.com.br** está registrado desde 2022 em nome de **Bruno Marin Mota** (CNPJ 45.299.812/0001-18 — empresa individual "B2M Assessoria", de serviços de escritório e desenvolvimento, São José dos Campos/SP), com DNS delegado a `almeidapay.com.br` (titular Gustavo Rossi). Nenhuma dessas entidades consta como **instituição de pagamento autorizada pelo Banco Central**; trata-se de agregador que emite cobranças em nome de terceiros — arranjo que **oculta o beneficiário final** do dinheiro.

Dados pessoais coletados

O checkout coleta **nome, CPF, e-mail, telefone, CEP e endereço completo**, além dos dados do destinatário do presente e mensagem do cartão. O código (`checkout.js`) envia nome, CPF, e-mail, telefone, carrinho e UTMs ao endpoint `/api/abandoned` por beacon **1,2 segundo após o preenchimento** — os dados chegam ao operador **mesmo que a compra nunca seja concluída**. O pagamento é gerado em `/api/pix`; não há opção de cartão de crédito ou gateway com proteção ao comprador.

Leitura técnica. O fluxo financeiro é real e operante: o consumidor paga R$ 69,90 (ou outro valor de carrinho) a **LEGACY DIGITAL LTDA** por meio de um agregador não regulado — não à floricultura, não à OINCASH. Em uma loja legítima, o recebedor do PIX corresponde ao estabelecimento (ou a um gateway autorizado que o nomeia). A tripla divergência de identidades, o MCC genérico "0000" e a cobrança de amostra com devedor fictício "Fulano de Tal" são incompatíveis com operação comercial regular. As imagens do catálogo (WebP re-otimizadas, **sem qualquer metadado EXIF/autor**) não permitem comprovar origem própria do acervo fotográfico. Não se imputa conduta ilícita à ONZ (fornecedora de software), à AWS nem às plataformas de anúncio.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Recebedor do PIX (LEGACY DIGITAL LTDA) não corresponde à loja nem ao CNPJ declarado	`pix_copiaecola.txt · pix_payload_jws.txt`	ALTA
2	CNPJ exibido pertence a empresa de publicidade (OINCASH LTDA, aberta 09/04/2026), sem CNAE de floricultura	`corpo.html · bases CNPJ`	ALTA
3	Domínio registrado há 30 dias, titular oculto, sem histórico	`rdap_raw.json`	ALTA
4	Pagamento exclusivamente PIX, via agregador não regulado que oculta o beneficiário final	`checkout.js · rdap_onlyup.com.br.json`	ALTA
5	Coleta de nome, CPF, e-mail e telefone transmitida antes da conclusão da compra (/api/abandoned)	`checkout.js`	MÉDIA
6	Captação por tráfego pago (Google Ads) com promessas de "entrega hoje" e frete grátis	`corpo.html (tag AW-18194665316)`	MÉDIA
7	Origem do servidor mascarada por Cloudflare (IP real oculto)	`dns_registros.txt · headers.txt`	MÉDIA
8	"Floricultura parceira" jamais identificada; sem endereço físico ou telefone	`corpo.html · checkout.html`	MÉDIA
9	Estrutura de avaliações presente porém vazia (reviews.json)	`reviews.json`	BAIXA
10	Imagens de catálogo sem metadados de autoria (re-otimizadas)	`metadata_exiftool.txt`	BAIXA

Síntese: 4 indicadores de severidade ALTA, 4 MÉDIA e 2 BAIXA. **Nenhum fator de legitimidade verificável** (floricultura identificada, endereço físico, telefone, recebedor compatível, histórico) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 12/07/2026, conclui-se que **buquederosas.delivery** é uma loja de flores online criada há **30 dias**, com titular oculto, que promete entrega por "floricultura parceira" jamais identificada e cobra **exclusivamente por PIX** cujo recebedor — **LEGACY DIGITAL LTDA**, via agregador não regulado — **não corresponde nem à loja nem à empresa declarada no próprio site** (OINCASH LTDA, ramo de publicidade, constituída 3 meses antes). O perfil é típico de **loja-fantasma**: o consumidor paga um terceiro sem vínculo verificável com o produto e entrega dados pessoais completos já no preenchimento do formulário. Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não comprar e não pagar o PIX**; desconfiar de anúncios (Google, redes sociais) que conduzam ao site com promessas de entrega no mesmo dia e frete grátis.

- Se já houve pagamento: acionar imediatamente o banco e o mecanismo **MED** do PIX (devolução), guardar o comprovante, o código "copia e cola" e capturas de tela, registrar Boletim de Ocorrência (estelionato) e reclamação em **consumidor.gov.br**.
- Quem forneceu dados no checkout deve ficar alerta a golpes derivados (falsa central bancária, cobranças em nome da "loja"), pois nome, CPF, telefone e endereço foram transmitidos ao operador.

Recomendações de mitigação / denúncia

- Reportar o domínio ao registrador **Dynadot** (abuse@dynadot.com) e à **Cloudflare** (abuse.cloudflare.com), anexando este laudo.
- Reportar o recebedor **LEGACY DIGITAL LTDA** e a cobrança (txid) ao agregador OnlyUp e ao **Banco Central** (canais do PIX/MED via instituição pagadora), para bloqueio do beneficiário.
- Denunciar o anúncio ativo no **Google Ads** (tag AW-18194665316) como destino fraudulento.
- Preservar este relatório e as evidências (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. A classificação expressa um juízo técnico de risco e não substitui decisão de autoridade policial, administrativa ou judicial. Não se imputa conduta ilícita aos provedores de infraestrutura e de pagamento citados (Dynadot, Cloudflare, Google, AWS, ONZ), meros intermediários técnicos.

— Fim do relatório —

Documento gerado por Dono do Site — OSINT & Investigação Digital · Relatório técnico baseado em dados públicos e análise de conteúdo aberto.