RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

contingenciamaxima.com

Objeto investigado	contingenciamaxima.com — "Contingencia Máxima Keys", sistema que vende chaves de resgate para acesso a contas de serviços de streaming (gTLD .com)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	02/08/2026 (RDAP, DNS, HTTP/TLS, geolocalização, leitura do bundle JavaScript)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do bundle público
Achado central	O bundle público revela que o comprador não recebe uma conta própria: recebe uma "key" que libera credenciais de uma conta de streaming controlada pelo operador, cujo e-mail e senha podem ser trocados a qualquer momento por rotinas administrativas do próprio sistema
Classificação	**RISCO ALTO**
Emissão do laudo	02/08/2026 às 01:38

1. Sumário Executivo

Este laudo documenta a análise técnica do endereço **contingenciamaxima.com**, realizada em **02/08/2026** por técnicas de OSINT e coleta passiva — requisições equivalentes às de um visitante comum, sem criação de conta, sem resgate de chave, sem envio de dados pessoais e sem tentativa de compra. Toda evidência foi preservada com hash SHA-256 (Anexo A).

O endereço **está no ar** e entrega uma aplicação React/Vite de página única (o HTML servido tem apenas 1.628 bytes; toda a interface está no bundle `index-U7NA4bpO.js`, de 697 KB). O título é "Contingencia Máxima Keys" e a descrição declarada é "Melhor sistema de gerenciamento de contas de streaming". O site **não publica CNPJ, razão social, endereço, telefone ou página de termos**, e o domínio não possui registro MX — não há como receber e-mail no próprio endereço.

O achado central está no **modelo do produto**, legível no bundle público. O texto da aplicação informa: "Receba uma key única para acessar sua conta de streaming com todos os códigos de autenticação" e "Cada key tem um período de validade definido". As rotinas administrativas expostas no mesmo bundle mostram o outro lado do arranjo: existem endpoints `/api/admin/keys/replace-email` e `/api/admin/keys/sync-streaming-password`, e mensagens de operação como "Selecione o email para gerar as keys (**o mesmo email será usado em todas**)" e "Os usuários verão a **nova senha** ao acessar a key". A instrução ao comprador, também no bundle, é **"Não alterar o PIN da conta"**.

Tecnicamente, isso descreve **acesso compartilhado a contas de terceiros**, e não a venda de uma assinatura própria. O comprador não é titular da conta que passa a usar: não controla o e-mail de recuperação, não pode alterar a senha nem o PIN, e o operador pode trocar credenciais de todas as chaves de uma só vez. Daí decorre a consequência prática relatada publicamente por um consumidor no Reclame AQUI — pagamento de R$ 19,90 por uma conta Disney+ em 13/07/2026, seguido de bloqueio da conta exigindo **código de verificação enviado a um e-mail que o comprador não controla**, sem canal de suporte disponível para obtê-lo.

O perfil registral acompanha esse quadro: domínio registrado em **29/01/2026** por **um ano**, titular não publicado, DNS e proxy na Cloudflare (origem real oculta) e nenhuma página institucional. O bundle cita ainda a expressão "efi" entre referências de pagamento, sem que o fluxo de cobrança tenha sido acionado nesta coleta — nenhum meio de pagamento foi confirmado em operação.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: o produto vendido é uma **chave de acesso a conta de terceiro**, cujo controle permanece integralmente com o operador. O consumidor paga por um acesso que pode ser revogado, alterado ou bloqueado sem que ele tenha qualquer meio técnico de recuperá-lo — e não há identificação legal nem canal de atendimento a quem recorrer.

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 código do front-end foram obtidos por requisição HTTPS de visitante comum, sem qualquer interação intrusiva, sem envio de dados pessoais e sem tentativa de compra ou de pagamento. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do endereço	RDAP do registro responsável	`rdap_raw.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_records.txt`

Conteúdo / cabeçalhos	curl HTTPS (visitante comum)	`corpo_home.html · headers_home.txt`
Certificado TLS	openssl s_client + x509	`tls_cert.txt`
Hospedagem / origem	ipinfo.io + PTR reverso	`geoip.json`
Aplicação	Leitura do bundle JavaScript público	`bundle_index.js`
Integridade	SHA-256 de cada arquivo coletado	`hash_manifest.txt`

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

Domínio	contingenciamaxima.com (gTLD .com — Verisign)
Registro	**29/01/2026** · expira 29/01/2027 (validade de 1 ano)
Última alteração	03/03/2026
Idade na coleta	**~6 meses**
Registrador	HOSTINGER operations, UAB
Titular	**Não publicado** (o RDAP expõe apenas o registrador)
Status	client transfer prohibited
Nameservers	CLYDE.NS.CLOUDFLARE.COM · GEORGIA.NS.CLOUDFLARE.COM
Endereço IP	172.67.143.2 (AS13335 Cloudflare, Inc.) — origem real oculta pela CDN
Registro MX	**Nenhum** — o domínio não recebe e-mail
Registro TXT	Nenhum (sem SPF, sem verificação de plataforma)
Certificado TLS	Google Trust Services (WE1) · 25/07/2026 → 23/10/2026
Identificação legal	**Ausente** — sem CNPJ, razão social, endereço ou telefone
Páginas legais	Nenhuma — sem termos de uso, política de privacidade ou página de contato

Leitura técnica. Registro de um ano, titular oculto, ausência de MX e ausência total de páginas institucionais compõem o padrão de endereço de baixo compromisso: o custo de abandoná-lo é próximo de zero. Nada disso é ilícito em si — mas, somado à natureza do produto vendido, significa que o consumidor não dispõe de nenhum ponto de contato documentável caso o acesso pare de funcionar.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

A aplicação é uma **SPA React/Vite** servida atrás da Cloudflare. O bundle público (`index-U7NA4bpO.js`, 697 KB) contém tanto a interface do comprador quanto a do painel administrativo, o que permite ler o modelo de operação sem qualquer acesso privilegiado. Nenhum endpoint foi acionado nesta coleta: os caminhos abaixo foram apenas **lidos** do código distribuído publicamente ao navegador.

Item verificado	Constatação
Produto	`"Receba uma key única para acessar sua conta de streaming com todos os códigos de autenticação"`
Validade	`"Cada key tem um período de validade definido. Aproveite durante o tempo contratado."`
Instrução ao comprador	**`"Não alterar o PIN da conta"`**
Compartilhamento	`"Selecione o email para gerar as keys (o mesmo email será usado em todas)"`
Troca de credencial	`"Os usuários verão a nova senha ao acessar a key"`
Endpoint administrativo	`/api/admin/keys/replace-email` — substitui o e-mail vinculado às chaves
Endpoint administrativo	`/api/admin/keys/sync-streaming-password` — sincroniza a senha do streaming
Endpoint administrativo	`/api/admin/generate-reset-code` · `/api/admin/security/devtools-unban`
Endpoint de e-mail	`/api/notletters-emails/active` · `/api/check-email-code`
Referência de pagamento	`"efi"` citado no bundle; **fluxo de cobrança não acionado** nesta coleta
Mensagens de erro	`"Esta key não existe ou já foi utilizada"` · `"Esta key já foi resgatada por outro usuário"`

Aspecto	Constatação
Tipo de serviço	Venda de chaves de resgate que liberam credenciais de contas de streaming
Tecnologia	React/Vite (SPA) atrás da Cloudflare · rocket-loader da Cloudflare
Hospedagem	Origem oculta pela Cloudflare; nenhum IP de origem exposto
Correio eletrônico	Ausente — sem MX, o domínio não recebe mensagens
Identificação do fornecedor	Nenhuma — sem CNPJ, razão social, endereço ou telefone
Canal de atendimento	Apenas o "centro de suporte" interno do painel; nenhum contato externo publicado
Documentos legais	Nenhum
Titularidade da conta entregue	Do operador, não do comprador — e-mail e senha permanecem sob controle de terceiro
Relato público	Reclame AQUI, 14/07/2026: R$ 19,90 por conta Disney+, conta bloqueada exigindo código de verificação, sem suporte

Leitura técnica. O risco aqui é estrutural e independe da boa ou má-fé de quem opera: quando o e-mail de recuperação é comum a várias chaves e a senha pode ser sincronizada em lote, o acesso do comprador é, por construção, **revogável a qualquer momento e irrecuperável por ele**. O bloqueio por código de verificação relatado publicamente é o desfecho previsível desse arranjo, e não uma falha pontual. Acrescente-se que serviços de streaming costumam vedar em contrato o compartilhamento e a revenda de contas, o que expõe o comprador ao encerramento do acesso pelo próprio provedor do conteúdo.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Produto entregue é credencial de conta controlada pelo operador, não assinatura em nome do comprador	`bundle_index.js`	ALTA
2	Endpoints administrativos permitem trocar e-mail e sincronizar a senha das contas já vendidas	`bundle_index.js`	ALTA
3	Mesmo e-mail reutilizado em todas as chaves geradas, conforme mensagem do próprio painel	`bundle_index.js`	ALTA
4	Nenhuma identificação legal do fornecedor e nenhuma página de termos, privacidade ou contato	`corpo_home.html`	ALTA
5	Comprador instruído a não alterar o PIN da conta, isto é, a não assumir controle do acesso	`bundle_index.js`	MÉDIA
6	Domínio registrado por apenas 1 ano, com titular não publicado	`rdap_raw.json`	MÉDIA
7	Ausência de registro MX: o domínio não pode receber e-mail de clientes	`dns_records.txt`	MÉDIA
8	Origem real oculta atrás da CDN, sem servidor ou localização identificáveis	`geoip.json`	BAIXA

Síntese: 4 indicadores de severidade ALTA, 3 MÉDIA e 1 BAIXA. **Não se registrou nenhum fator de legitimidade**: não há identificação legal, documentos contratuais, canal de atendimento externo nem correio eletrônico configurado no domínio.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em **02/08/2026**, **contingenciamaxima.com** vende **acesso compartilhado a contas de streaming de terceiros**, e não assinaturas em nome do comprador. O próprio código distribuído ao navegador documenta que o e-mail de recuperação é comum a várias chaves, que a senha pode ser sincronizada em lote pelo operador e que o comprador é instruído a não alterar o PIN — ou seja, a **não assumir o controle do acesso que pagou**. Some-se a ausência completa de identificação legal, de páginas contratuais e de correio eletrônico no domínio, e o resultado é um consumidor que, ao perder o acesso, não tem nem meio técnico de recuperá-lo nem destinatário a quem reclamar. Classifica-se o caso como **RISCO ALTO**. Registre-se que o modelo também tende a contrariar os termos de uso dos próprios serviços de streaming, o que adiciona ao comprador o risco de encerramento do acesso pelo provedor do conteúdo.

Recomendações ao consumidor / solicitante

- **Não adquirir** contas de streaming por meio de chaves de resgate: o acesso permanece sob controle de terceiro e pode cessar a qualquer momento, sem direito recuperável.
- Preferir a assinatura direta junto ao provedor do conteúdo, na qual o e-mail e a senha ficam sob titularidade do próprio consumidor.
- Quem já pagou deve preservar comprovante, data, valor e todas as telas do resgate — sem CNPJ publicado, esse é o único conjunto documental disponível.
- Havendo pagamento por Pix, procurar o próprio banco quanto aos mecanismos disponíveis, observando os prazos aplicáveis, e registrar o caso no consumidor.gov.br.

Recomendações de mitigação / denúncia

- Ao responsável pelo site: publicar identificação legal (razão social, CNPJ, endereço), termos de uso e um canal de atendimento externo; e esclarecer ao comprador, antes da compra, que a conta entregue permanece sob controle do operador.

- Aos serviços de streaming cujas contas são revendidas: as evidências deste laudo permitem instruir comunicação aos seus próprios canais de proteção de marca e de uso indevido de contas.
- Aos canais de *abuse* do registrador (Hostinger) e da Cloudflare: o material aqui preservado pode instruir comunicação, observando que ambos são provedores de infraestrutura sem responsabilidade sobre o conteúdo do cliente.
- Ao consumidor lesado: registrar reclamação administrativa e, se for o caso, boletim de ocorrência, anexando este laudo e o comprovante de pagamento.

Ressalva metodológica: este laudo baseia-se em fontes abertas e reflete o estado do endereço na data indicada. A coleta foi integralmente passiva — requisições equivalentes às de um visitante comum, sem criação de conta, sem envio de dados pessoais, sem tentativa de compra e sem qualquer interação intrusiva. Não se imputa conduta ilícita a provedores de infraestrutura (registrador, hospedagem, CDN, autoridade certificadora) nem a intermediários de pagamento regulados, que não respondem pelo conteúdo publicado por seus clientes. A classificação de risco é juízo técnico sobre o conjunto de indicadores observados, não decisão judicial nem afirmação sobre a intenção de quem opera o endereço. Sinais aqui descritos como alerta podem decorrer de escolhas de configuração e ser corrigidos pelo próprio responsável pelo site.

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 (709129 bytes)`	`0040f1927c99df80d7ed5236002458460a5c4b760d0a046fc7b33b1e6eeffb47`
`corpo_home.html (1630 bytes)`	`3a50536297e73b4776678087623fdbf36b16b7a87039b06ab3e20479166e209c`
`dns_records.txt (436 bytes)`	`565b5c7513e72e4b69571700fe2cdc32c943c331203a5240da19d7b500553a6d`
`geoip.json (287 bytes)`	`27cba33120d500cc27b7886772f04b2e37b9ea46e610060e37d3a3a7c47307bb`
`headers_home.txt (972 bytes)`	`075cc18140b92d2ef45861776899712435ee71dd311e10fde3fdd7623d622818`
`rdap_raw.json (2672 bytes)`	`c52d61226fecd05ae17099603da92797d180c6209e2b933e842aa225d6273d9c`
`tls_cert.txt (311 bytes)`	`23123fc382bf2d11c5933d5e091be33eebf936ba3642237ce8fef8281d632dc4`

— Fim do relatório —