RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

securelimite.com

Objeto investigado	securelimite.com - funil que se apresenta como empréstimo pessoal pre-aprovado do Nubank e cobra um "Seguro Prestamista" por Pix (gTLD .com)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	10/08/2026 (RDAP, DNS, HTTP/TLS, geolocalização, bundle JS, base pública de CNPJ) - reverificação em 11/08/2026
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do funil e do código
Achado central	Uso do nome e do CNPJ do Nubank em funil de 10 etapas que captura CPF, renda e selfie e cobra taxa antecipada por Pix
Classificação	**RISCO ALTO**
Emissão do laudo	11/08/2026 as 08:53

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **securelimite.com**, realizada em **10/08/2026** por técnicas de OSINT (inteligência de fontes abertas) e análise passiva - requisições equivalentes às de um visitante comum e consultas a bases públicas, **sem preenchimento de formulários, sem envio de CPF e sem ativação de câmera**. As páginas do funil foram obtidas diretamente por seus endereços e analisadas em código. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

O domínio **está no ar** e entrega uma página em português intitulada "Crédito Pessoal Pre-Aprovado" que se apresenta explicitamente como o **Nubank**: "Empréstimo pessoal rápido e sem burocracia e com a Nubank!", "Limite de até R$ 30.000", "Taxas a partir de 0,81% a.m.", "parcelamento em até 120x", com simulador, selos de "Banco Central", "Instituição regulada" e "+500 mil clientes", e depoimentos atribuídos a "Maria Silva" e "Joao Santos". No rodapé e na janela "Fale Conosco" o site declara o **CNPJ 30.680.829/0001-43** e a razão social "Nubank Soluções Financeiras Ltda". A consulta a base pública mostra que esse CNPJ e **real e ativo**, mas pertence a **NU FINANCEIRA S.A. - SOCIEDADE DE CREDITO, FINANCIAMENTO E INVESTIMENTO** (aberta em 12/06/2018, São Paulo/SP) - **razão social diferente** da declarada. Trata-se, portanto, de **número de terceiro exibido para simular legitimidade**, e não de identificação do operador do site. O rodapé ainda assina "© 2025 Pagamentos S.A", o telefone informado é o sequencial "(11) 98765-4321", e outras duas sequências apresentadas como CNPJ **reprovam no cálculo do dígito verificador** (módulo 11) - isto é, são números inventados.

O site não é uma página única: é um **funil de dez etapas em HTML estático**, com páginas numeradas em sequência - "Verificação de Dados" (2), "Informações do Empréstimo" (3), "Termos e Condições" (4), "Análise de Crédito" (5), "Empréstimo Aprovado" (5b), "Verificação Facial" (6), "Escolha o Vencimento" (7), "Confirme seus Dados" (8), "Seguro Prestamista" (9) e um checkout final. Todas as etapas continuavam no ar na reverificação de 11/08/2026.

Dois achados são especialmente graves. Primeiro, na etapa 2 o **CPF digitado é enviado a um serviço externo de consulta**, pelo endereço `concurso-inscricao.com/v1/consultarev0ltz/<CPF>/?token=...` - domínio sem relação com o Nubank, registrado em 19/02/2025, que na data desta análise **não resolve mais em DNS**. Esse tipo de consulta devolve o nome do titular do CPF, o que permite ao funil exibir o nome real do visitante e tornar a "aprovação" convincente. Segundo, na etapa 6 o site **abre a câmera do dispositivo** (`getUserMedia`) e captura uma imagem estática em JPEG (`canvas.toDataURL`) a título de "verificação facial" - ou seja, coleta uma **selfie** do visitante. Ao longo do funil são pedidos ainda nome, e-mail, telefone, **profissão**, **renda mensal**, escolaridade, finalidade do empréstimo e dia de vencimento.

O desfecho é o mecanismo clássico da **fraude da taxa antecipada**: após anunciar o empréstimo como aprovado e "reservado para liberação imediata", a última etapa exige o pagamento de um **"Seguro Prestamista" de R$ 36,84 por Pix**, descrito como "100% reembolsável" e condição para "confirmar a liberação em seu CPF". O código Pix é gerado pelo próprio site (`api.php?action=generate`), de modo que o beneficiário final não é exposto ao visitante. O checkout é parametrizado por oferta (`checkout/index.php?offer=main`) e um comentário esquecido no código pelo desenvolvedor menciona **ofertas de upsell subsequentes** - indicando que o valor inicial é a porta de entrada de uma cadeia de cobranças. Nenhuma instituição financeira regulada condiciona a liberação de crédito ao pagamento prévio de seguro por Pix a terceiro.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: um site que se diz Nubank sem o ser, exibe CNPJ de terceiro, coleta CPF, renda e selfie e exige uma taxa por Pix **antes** de liberar um crédito que não existe, oferece **risco elevado**. Recomenda-se **não pagar, não enviar selfie e não fornecer CPF ou dados financeiros** (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 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 (Verisign / .com - registrador Dynadot)	`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)	`corpo_home.html · headers_home.txt`
Funil completo	curl HTTPS de cada etapa (2 a 9, 5b e checkout)	`corpo_2..corpo_9.html · corpo_checkout.html`
Aplicação (front-end)	Download do bundle JS e leitura do código das etapas	`bundle_js.txt`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · PTR reverso	`geoip.json`
Identidade declarada	Base pública de CNPJ (Receita Federal)	`cnpj_publico_30680829000143.json`
Serviço externo de CPF	RDAP .com (concurso-inscricao.com) · resolução DNS	`rdap_concurso_inscricao.json`

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

Domínio	securelimite.com (gTLD .com - Verisign)
Registro	**06/01/2026** · expira 06/01/2027 (validade de 1 ano) · última alteração 09/08/2026
Idade na coleta	**~7 meses**
Titular	**Oculto** (o RDAP expõe apenas o registrador)
Registrador	Dynadot Inc (IANA 472) · abuse@dynadot.com
Status	clientTransferProhibited
Servidores de nome	jake / melissa.ns.cloudflare.com
DNS - A / AAAA	172.67.217.48 e 104.21.86.87 · AAAA 2606:4700:3034::ac43:d930 e 2606:4700:3031::6815:5657 · **sem MX** · **sem TXT**
Hospedagem	AS13335 Cloudflare, Inc. - IP de origem não exposto
Servidor web	Server: cloudflare · `last-modified: 14/07/2026`
Certificado TLS	CN=securelimite.com · emissor Google Trust Services WE1 (DV) · válido 09/08/2026-07/11/2026
CNPJ declarado	**30.680.829/0001-43** - existe e está ATIVA, mas pertence a **NU FINANCEIRA S.A. - SCFI** (12/06/2018, São Paulo/SP), **não** a "Nubank Soluções Financeiras Ltda" como o site declara
Outros "CNPJ" na página	18373902151619 e 77141819031603 - **reprovam no dígito verificador** (módulo 11): números inventados

Contato declarado	Telefone sequencial "(11) 98765-4321" · rodapé "© 2025 Pagamentos S.A" · sem endereço verificável

Leitura técnica. Titular oculto, validade de 1 ano, ausência de e-mail próprio (sem MX) e uso de proxy reverso que oculta o servidor de origem compõem um perfil de **baixa rastreabilidade do responsável** - incompatível com uma instituição financeira, que é autorizada e supervisionada pelo Banco Central e se identifica publicamente. O certificado DV gratuito comprova apenas o controle do domínio, **não a identidade de qualquer empresa** nem autorização para operar crédito. A exibição de um CNPJ real de terceiro ao lado de duas sequências numéricas invalidas demonstra que os dados de identificação foram **montados para aparentar conformidade**. Não se imputa conduta ao registrador nem a Cloudflare, meros provedores de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site é um **funil de conversão em HTML estático**, com páginas numeradas servidas em sequência fixa e estado guardado no navegador (localStorage). O percurso vai da simulação de empréstimo até um checkout que cobra uma taxa por Pix. As tabelas abaixo descrevem o percurso, os dados coletados em cada etapa e o desfecho financeiro.

Etapa	Página e o que faz
1 - Home	"Crédito Pessoal Pre-Aprovado" com a marca Nubank, simulador de até R$ 30.000 em 120x e selos de "Banco Central" / "Instituição regulada"
2 - Verificação de Dados	Pede o **CPF** e o envia a serviço externo de consulta (`concurso-inscricao.com`), que devolve o nome do titular
3 - Informações do Empréstimo	Coleta finalidade do empréstimo, **renda mensal**, **profissão** e escolaridade
4 - Termos e Condições	Aceite de termos
5 - Análise de Crédito	Tela de espera simulando análise
5b - Empréstimo Aprovado	Anuncia a aprovação do crédito
6 - Verificação Facial	**Abre a câmera** (`getUserMedia`) e captura uma imagem JPEG (`canvas.toDataURL`) - coleta de **selfie**
7 - Escolha o Vencimento	Coleta o dia de vencimento das parcelas
8 - Confirme seus Dados	Revisão dos dados pessoais e de contato
9 - Seguro Prestamista	Introduz a cobrança do "seguro" como condição para liberar o valor
10 - Checkout	`checkout/index.php?offer=main` - cobra **R$ 36,84 por Pix**, código gerado por `api.php?action=generate`

Aspecto	Constatação
Tipo de serviço	Funil de "empréstimo pessoal pre-aprovado" anunciado sob a marca Nubank
Tecnologia	HTML estático com páginas numeradas e checkout PHP, atrás da Cloudflare
Marca de terceiro	**Nubank** citada nominalmente na home, nos termos, na política de privacidade e no checkout
Identidade declarada	CNPJ 30.680.829/0001-43 (**real**, de NU FINANCEIRA S.A. - SCFI) atribuído a razão social inexistente "Nubank Soluções Financeiras Ltda"
Vínculo empresa↔site	**Não demonstrado** - domínio anônimo, sem MX, sem endereço e sem qualquer registro que ligue o site a instituição
Dados coletados	CPF, nome, e-mail, telefone, profissão, **renda mensal**, escolaridade, finalidade do empréstimo, dia de vencimento e **imagem facial (selfie)**
Envio do CPF a terceiro	**concurso-inscricao.com/v1/consultarev0ltz/<CPF>/?token=...** - serviço de consulta alheio ao Nubank; domínio registrado em 19/02/2025 e **sem resolução DNS** em 11/08/2026
Cobrança	**R$ 36,84** a título de "Seguro Prestamista", anunciado como "100% reembolsável" e condição para liberar o empréstimo
Meio de pagamento	**Pix**, com código gerado no próprio site (`api.php?action=generate`) - beneficiário final **não exposto**

Cadeia de cobranças	Checkout parametrizado por oferta (`?offer=main`); comentário do desenvolvedor no código menciona **ofertas de upsell** subsequentes
Aquisição de tráfego	Rastreador `cdn.utmify.com.br` (atribuição de tráfego pago) e player `api.vturb.com.br`
Prova social	Depoimentos fictícios ("Maria Silva", "Joao Santos") e métricas não verificáveis ("500K+ clientes", "+500 mil clientes")

Leitura técnica. A arquitetura do funil é a de uma **fraude de taxa antecipada**: o crédito é anunciado como já aprovado e reservado, e só então surge uma cobrança pequena e "reembolsável" como último obstáculo - desenho que explora o custo afundado emocional de quem já percorreu nove etapas. A consulta externa do CPF é o que dá verossimilhança ao golpe, porque permite tratar o visitante pelo nome real logo após ele digitar apenas o número do documento; e a "verificação facial" acrescenta ao operador uma **selfie associada a um CPF, a uma renda e a um telefone**, conjunto de valor próprio para abertura de contas e outras fraudes de identidade, independentemente do pagamento. O beneficiário do Pix não é observável de fora porque o código é gerado no servidor. Não se imputa conduta a instituição financeira cuja marca e CNPJ aparecem no site - ela figura como **titular da identidade usada sem vínculo demonstrado** -, nem aos provedores de infraestrutura citados.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Cobrança de taxa antecipada ("Seguro Prestamista", R$ 36,84 por Pix) como condição para liberar crédito	`corpo_9.html` · `corpo_checkout.html`	ALTA
2	Uso da marca Nubank e de CNPJ real de terceiro (NU FINANCEIRA S.A.) sem vínculo demonstrado	`corpo_home.html` · `cnpj_publico_30680829000143.json`	ALTA
3	CPF do visitante enviado a serviço externo de consulta alheio a instituição	`corpo_2.html` · `rdap_concurso_inscricao.json`	ALTA
4	Captura de imagem facial (selfie) pela câmera do dispositivo sob pretexto de "verificação"	`corpo_6.html`	ALTA
5	Coleta de renda mensal, profissão, escolaridade e contato antes de qualquer contratação	`corpo_3.html` · `corpo_8.html`	ALTA
6	Razão social declarada ("Nubank Soluções Financeiras Ltda") não corresponde ao CNPJ exibido	`corpo_home.html` · `cnpj_publico_30680829000143.json`	MEDIA
7	Duas sequências apresentadas como CNPJ reprovam no dígito verificador - números inventados	`corpo_home.html`	MEDIA
8	Código Pix gerado no servidor - beneficiário final oculto ao visitante	`corpo_checkout.html`	MEDIA
9	Cadeia de upsell no checkout, indicada por comentário do desenvolvedor no código	`corpo_9.html`	MEDIA
10	Depoimentos fictícios, métricas não verificáveis e selos de "Banco Central" / "Instituição regulada"	`corpo_home.html`	BAIXA
11	Titular oculto, sem MX, telefone sequencial "(11) 98765-4321" e sem endereço verificável	`rdap_raw.json` · `dns_records.txt` · `corpo_home.html`	BAIXA

Síntese: 5 indicadores de severidade ALTA, 4 MEDIA e 2 BAIXA. **Nenhum fator de legitimidade** (autorização para operar crédito, identificação do operador, vínculo verificável com a instituição financeira citada, beneficiário identificado) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 10/08/2026, conclui-se que **securelimite.com** é um **funil de empréstimo falso de alto risco**: publicado em domínio anônimo, usa o nome do **Nubank** e um

CNPJ real de terceiro (NU FINANCEIRA S.A.) - ao lado de dois números de CNPJ inventados - para conduzir o visitante por dez etapas que capturam **CPF, renda, profissão, contato e uma imagem facial**, enviam o CPF a um serviço externo de consulta e culminam na cobrança de um **"Seguro Prestamista" de R$ 36,84 por Pix** como condição para liberar um crédito que nunca existiu, com indícios de cadeia de upsell no checkout. Classifica-se o caso como **RISCO ALTO** ao consumidor, tanto pela perda financeira quanto pelo conjunto de dados pessoais e biométricos coletados.

Recomendações ao consumidor / solicitante

- **Não pagar o Pix, não enviar selfie e não fornecer CPF, renda ou dados de contato** a este site.
- Fixar a regra geral: **empréstimo legítimo não cobra nada antecipadamente**. Seguro prestamista, quando existe, é embutido nas parcelas do contrato - nunca pago por Pix a terceiro antes da liberação.
- Contratar crédito apenas pelos canais oficiais da instituição (aplicativo ou site oficial), digitando o endereço ou usando o app já instalado, nunca por links de anúncios, SMS ou WhatsApp.
- Verificar no site do **Banco Central** se a instituição que oferece o crédito é autorizada a operar; o site investigado não se identifica de forma verificável.
- Se já houve pagamento: acionar o banco e o mecanismo **MED** do Pix, reunir comprovantes e registrar Boletim de Ocorrência e reclamação em **consumidor.gov.br**.
- Se já foram enviados CPF, renda e selfie: tratar os dados como comprometidos - monitorar o CPF (Registrato/Banco Central, birôs de crédito), desconfiar de contatos que citem esses dados e não confirmar códigos recebidos por SMS.

Recomendações de mitigação / denúncia

- Denunciar o domínio aos canais de abuse do registrador (`abuse@dynadot.com`) e da Cloudflare, anexando este laudo.
- Comunicar o **Nubank** sobre o uso não autorizado da marca e do CNPJ do grupo, para as providências de propriedade intelectual e de alerta a clientes.
- Reportar a cobrança ao banco pagador assim que o beneficiário do Pix for conhecido por quem tiver efetuado o pagamento, e registrar o caso no **Banco Central** e na plataforma **consumidor.gov.br**.
- Reportar o endereço aos mecanismos de navegação segura (Google Safe Browsing, Microsoft SmartScreen) e as plataformas de anúncios que eventualmente veiculem o funil.
- 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 nas datas indicadas (coleta em 10/08/2026, reverificação em 11/08/2026). A classificação expressa um juízo técnico de risco e não substitui decisão de autoridade policial, administrativa ou judicial. Não se imputa conduta ilícita a instituição financeira cuja marca e CNPJ aparecem no site - que figura como **titular da identidade usada sem vínculo demonstrado** e pode ser vítima de apropriação -, nem aos provedores de infraestrutura citados (Dynadot, Cloudflare). Nenhum CPF, dado pessoal ou imagem foi enviado ao site durante a investigação, e nenhuma câmera foi ativada.*

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`	`fdad0a0d1f449fd50d27604bbdedf1bdbf856c1b82ad439e8eb4a2041581643a`
`cnpj_publico_30680829000143.json`	`e2558a5a17b81489f59b6c0698476082090ae1dd1e90bbc7495fceb0a3fdf0e6`
`corpo_10.html`	`cc0b4e42510d49c6decd464123ecf3b14ae9b47f9b4ed2ee64893e2d6520a264`
`corpo_2.html`	`3b39253f5fda73f363fc9806af78b64069b4e04a9c058786f04bfc20c037edd2`

corpo_3.html	08146b85262b34331a10d05d135023cda41434d6bd2675b0cb0e5c9d6f08d3cc
corpo_4.html	2718472e9085dfdfa94e1fb2d5242c4e9123013a927246a0d29d94989d7caa6d
corpo_5b.html	36a4658eab466e38175d8cb08ed80efe3c984c185ae11c3363111ccc84414b57
corpo_5.html	c715727fdd882ba99e28fa8738e08371176262d0a4cfd2275fc0c82bb0acc4b4
corpo_6.html	60bf47f7eaf02d3bdf6f7c1e852e65cf24b4f76b21ad9e05fcdbcf9190bc0990
corpo_7.html	4671573976ebcd33bebd711defb5658afed6bdaae63c9d4b53f152a1eea6f1e5
corpo_8.html	0f65c0eaccc893d189111b28df87cb0bce3a39a2e8b2bd134aa5b1a195d48784
corpo_9.html	665d2a10f3259915cd3b9f3fea7f2bf4d926a4505017fa4f49eec6dceab6e048
corpo_checkout.html	20a5eb29d37f9e5995fd78b1331f9e8615ae6bb367b14b05171fb8c284a22678
corpo_home.html	c2b09a26bfb378bb0beb11dbcc2f0955a809b409887546c7b6697f939a831955
dns_records.txt	6d97dd855b635a192930a0c5b71381e7b6e1264029ad3dc7774acbb264855567
geoip.json	9dec64f09e562d7efd1d80bceacea96eb148d0462b1554b7065bbc7e1c63b7dc
hash_manifest.txt	c5d5db01fcbba24ce7ee679ac4985b89db6bb1764bae7ddf71390b3eb0046137
headers_home.txt	d3b95da28327687085ec4b09ac3cef6b41bedcf56145d2ee02f56941c6b875ba
rdap_concurso_inscricao.json	b4ee9b26e1b698e4d126bf26eb7a256c83de903fc97cd02999aa9669adad59a5
rdap_raw.json	b5cf95e7a63de229924238098219a2aec77c917fcb7920fcee0df53a82d63554
tls_cert.txt	f0cf4b802ca5f40ec61d76968d208270f142c926a8737507a622a578540bc0dc

- Fim do relatório -