



**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO
SERTÃO PERNAMBUCANO
CAMPUS SALGUEIRO
CURSO DE TECNOLOGIA EM SISTEMAS PARA INTERNET**

FABIO DEMETRIO NETO JUNIOR

**ANÁLISE DE SEGURANÇA DOS SISTEMAS WEB DE FINTECHS
BRASILEIRAS**

SALGUEIRO-PE

2022

FABIO DEMETRIO NETO JUNIOR

**ANÁLISE DE SEGURANÇA DOS SISTEMAS WEB DE FINTECHS
BRASILEIRAS**

O Trabalho de Conclusão de Curso (TCC) foi apresentado na disciplina de TCC do curso de tecnologia em Sistemas para Internet, ofertado pelo Campus Salgueiro do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano (IFSertãoPE), como requisito parcial para obtenção do título de tecnólogo em Sistemas para Internet.

Orientador: Francisco Kelsen de Oliveira

SALGUEIRO-PE

2022

J95 Junior, Fabio.

ANÁLISE DE SEGURANÇA DOS SISTEMAS WEB DE FINTECHS BRASILEIRAS /
Fabio Junior. - Salgueiro, 2022.
31 f. : il.

Trabalho de Conclusão de Curso (Sistemas para Internet) -Instituto Federal de Educação,
Ciência e Tecnologia do Sertão Pernambucano, Campus Salgueiro, 2022.
Orientação: Prof. Dr. Francisco de Oliveira Kelsen.

1. Rede de computadores. 2. Fintech. 3. Segurança da Informação. 4. Redes de
Computadores. I. Título.

CDD 004.62

**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO
SERTÃO PERNAMBUCANO
CAMPUS SALGUEIRO
CURSO DE TECNOLOGIA EM SISTEMAS PARA INTERNET**

FABIO DEMETRIO NETO JUNIOR

**ANÁLISE DE SEGURANÇA DOS SISTEMAS WEB DE FINTECHS
BRASILEIRAS**

O Trabalho de Conclusão de Curso (TCC) foi apresentado na disciplina de TCC do curso de tecnologia em Sistemas para Internet, ofertado pelo Campus Salgueiro do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano (IFSertãoPE), como requisito parcial para obtenção do título de tecnólogo em Sistemas para Internet.

Orientador: Francisco Kelsen de Oliveira

Aprovado em 08 de Agosto de 2022.

COMISSÃO EXAMINADORA

Prof. Dr. Francisco Kelsen De Oliveira (IFSertãoPE)
Orientador

Prof. Ms. Augusto Coimbra Costa Pinto. (IFSertãoPE)
Membro Interno

Prof. Ms. Leão João Dehon Costa (Uninassau)
Membro Interno

AGRADECIMENTOS

Gostaria de agradecer primeiramente a Deus secundamente aos meus pais por todo o apoio e força que tem me dado por toda essa caminhada agradecer ao professor Francisco Kelsen de oliveira por ter convidado a entrar no grupo GEPET e por te dado essa oportunidade de ampliar o conhecimento e o complemento de formação como pessoa, esses três anos foram corridos mas muito proveitosos e de grande aprendizagem, gostaria de agradecer também a resistência que foi um alicerce juntamente com todo apoio e conselhos espirituais de Daniel Inácio leite, a cabeça dura e o foco de Jonathan Yuri Rocha dos Santos a todos os professores que nos guiaram por toda essa caminhada cada ação cada passo que demos teve suas tribulações mas conseguimos vencer. Os puxões de orelha que recebi de Daniel foram bons ele sempre está lá para escutar, a Yuri agradecer pelo conhecimento e toda mini raiva que teve comigo e ao foco que ele teve também todas as questões que impulsionaram tanto a gente, também em relação a quando tinha atividade que dava aquela dorzinha de cabeça gostaria de agradecer imensamente a banca que está hoje presente para prestigiar o nosso feito e está presente para ampliar ainda mais o nosso conhecimento e por fim queria agradecer a todos os professores do Instituto Federal Campus Salgueiro no qual sou aluno e ex aluno, aos professores que tiveram presente nessa caminhada um imenso agradecimento sei que não é fácil o trabalho que eles têm mas fazem, mas continua a realizar com todo o coração e amor, obrigado mais uma vez a todos os envolvidos e desejo muitas bênçãos para todos e mais conhecimento porque sempre temos algo para aprender nessa vida.

RESUMO

As inovações tecnológicas, os acessos aos serviços por aplicativos e as reduções de taxas de serviços possibilitaram os avanços dos bancos digitais ou *fintechs*. Este trabalho objetivou analisar a segurança da informação (SI) a partir de teste de vulnerabilidade da aplicação ou página eletrônica dos principais bancos digitais em atuação no Brasil. Para isso, uma pesquisa bibliográfica foi realizada inicialmente para conhecer os conceitos, as possibilidades de teste de invasão e outros trabalhos realizados sobre o assunto. Os aplicativos para dispositivos móveis e as páginas eletrônicas dos bancos digitais, Nubank, Inter, Pagseguro, Next os respectivos foram analisados à luz dos seguintes aspectos: clonagem de página eletrônica, acessos e respostas aos servidores das respectivas aplicações. Os resultados deste trabalho mostraram que há bloqueio das páginas eletrônicas dos referidos bancos digitais contra clonagem, vislumbrando assim um método de prevenção para a empresa e aos dados sob a responsabilidade de guarda às referidas instituições. Escrever um período de forma geral sobre as respostas dos comandos de rede aos servidores. Portanto, esta pesquisa visa contribuir com a SI das instituições financeiras, bem como aos profissionais da área.

Palavras-Chave: Fintechs, Segurança da Informação, Redes de Computadores.

ABSTRACT

Technological innovations, access to services through applications and service fee reductions have enabled the advances of digital banks or fintechs. This paper aimed to analyze the information security (IS) from the vulnerability test of the application or electronic page of the main digital banks operating in Brazil. For this, a bibliographic research was initially carried out to learn about the concepts, the possibilities of penetration test and other works carried out on the subject. The applications for mobile devices and the electronic pages of the digital banks, Nubank, Inter, Pagseguro, Next the respective ones were analyzed in light of the following aspects: cloning of electronic page, accesses and responses to the servers of the respective applications. The results of this work showed that there is blocking of the electronic pages of the referred digital banks against cloning, thus glimpsing a method of prevention for the company and to the data under the responsibility of guard to the referred institutions. Writing a period in general about the responses of network commands to the servers. Therefore, this research aims to contribute to the IS of financial institutions as well as to professionals in the field.

Keywords: Fintechs, Information Security, Computer Networks.

LISTA DE FIGURAS

- Figura 1. Bancos mais baixados 2022
- Figura 2. Composição de transações por pessoas físicas
- Figura 3. Teste de Ping
- Figura 4. Tracert
- Figura 5. Ping Bancointer
- Figura 6. Ping Bancointer
- Figura 7. Tracert Pagseguro
- Figura 8. Gráfico Comparativo (MS) das Fintechs
- Figura 9. Gráfico Comparativo TTL das Fintechs
- Figura 10. Clonagem do site da Nubank
- Figura 11. Código fonte do site Nubank
- Figura 12. Clonagem do site da Inter
- Figura 13. Clonagem do site da Pagseguro

LISTA DE QUADRO

Quadro 1: Funções e Objetivos

Quadro 2: Quadro metodológico

Quadro 3: Variáveis Analisadas

Quadro 4: Resumo Funções Bancos

Quadro 5: Resultado de coleta entre as *fintechs* listadas

Quadro 6: Resultado de coleta de médias acerca das *fintechs* listadas

LISTA DE ABREVIATURAS E SIGLAS

RC: Redes de Computadores

SI: Segurança da Informação

IOT: Internet das Coisas

TTL: Time to Live

IP: Internet Protocol

ISO: Organização Internacional para Padronização

CMD: Prompt de Comando

PhaaS: Phishing-as-a-Service

(SSL): Secure Sockets Layer

Ms : Milisegundos

Sumário

1. Introdução	12
2. Fundamentação Teórica	13
3. Metodologia	16
3.1 Ping	18
3.2 Traceroute	20
4. Resultado e Discussões	21
4.1 Banco Nubank	27
4.2 Banco Inter	28
4.3 Banco PagueSeguro	29
5. Considerações Finais	29
6. Referências	31

1. Introdução

O mundo está vivendo a era Tecnologia da Informação com maior acesso dos cidadãos à Internet e serviços disponíveis a partir de diversos tipos de dispositivos, como computador pessoal, dispositivos móveis ou mesmo nas tecnologias vestíveis, como o smartwatch, ou nos aparelhos formadores da internet das coisas (IOT).

Os maiores usos das redes de computadores e dos serviços disponibilizados em tal ambiente trouxeram consigo as necessidades de garantias maiores de segurança aos dados, sistemas e usuários desses serviços. Isso não seria diferente no âmbito dos bancos e outras instituições financeiras, tais quais como os bancos digital e *fintechs*, que se utilizam de um uso intenso de tecnologia por se tratarem de empresas que estão em muitos momentos introduzindo inovações nos mercados financeiros e, diferentemente dos bancos físicos que contam com instalações em várias localidades, as *fintechs* dispõem apenas do âmbito on-line.

Os avanços dos serviços digitais também geraram um maior número de golpes e fraudes digitais. Nesse sentido, a Segurança da Informação (SI) também teve um maior número de pesquisas e ações para identificar, mapear e barrar golpes digitais, bem como tem agido de forma a prevenir ou evitar a ocorrência de crimes digitais. Fontes (2017) define que SI é um conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e sua missão seja alcançada.

Desse modo, SI está presente para proteger nossos dados e até mesmo nos proteger por todo momento, seja ele no âmbito virtual ou no mundo físico, pois nossos usos das tecnologias deixam rastros com dados, que podem ser utilizados para realizações de crimes.

O objetivo deste trabalho foi analisar a segurança da informação (SI) a partir de teste de vulnerabilidade da aplicação ou página eletrônica dos principais bancos digitais em atuação no Brasil.

A metodologia utilizada foi seguida a partir do uso de ferramentas disponíveis no sistema operacional Kali Linux, que dispõe da ferramenta *Setoolkit*, um conjunto de ferramentas voltado para engenharia social, e, por meio desta, foram realizados testes nas páginas web das *fintechs*, bem como foram realizados testes de comunicação aos servidores de tais aplicações, cujos dados coletados foram utilizados na análise desta pesquisa.

O presente artigo está dividido de modo a contemplar a fundamentação teórica, metodologia e resultados, seguindo com a organização e explanação dos testes e realizações que levaram à seção de considerações finais.

2. Fundamentação Teórica

A rede de computadores (RC) nos presentes dias se torna necessária e de grande valor pois graças a mesma pode-se compartilhar recursos, serviços e em certos casos uni las para criar um dispositivo com maior processamento e realizar funções distintas, salientando que a mesma possibilitou a criação de novos empregos incluindo a área da informática

Para Tanenbaum (2003), as “Redes de Computadores são conjuntos de máquinas destinadas ao processamento de dados independentes, com conexão entre seus sistemas operacionais por apenas um processo tecnológico.”

Kurose (2006) fala que o termo rede de computadores(RC) está ficando desatualizado pois como mencionado anteriormente o IOT está entrando nesse meio, “O termo Redes de Computadores está começando a soar um tanto desatualizado, dados os muito equipamentos não tradicionais que está sendo ligados às Redes”.

Nesse sentido pode-se perceber entre os conceitos apresentados por kurose e tannenbaum que rede de computadores está sendo cada vez mais ampliada graças aos adventos e inovações que vem chegando a cada momento, e nesta fase é onde se chega a um ponto importante sobre a segurança desses equipamentos alocados na rede.

Dentro da lógica abordada sobre a RC podem ser abordadas alguns métodos que se obtém a partir dos dados que circulam dentro, um grande exemplo é o Time to Live (TTL) o tempo de vida do pacote que caso ele não chegue no seu destino a tempo vai acabar se perdendo ou morrendo no percurso, sendo a quantidade de saltos que o mesmo dá desde a sua origem a seu ponto de destino

No âmbito das redes de computadores nos utilizamos de alguns elementos que servem para medir a qualidade da rede um deles é o traceroute definido pelo site <https://www.hostmidia.com.br/> como sendo o modelo para ter um cálculo médio acerca do tempo que um pacote levou dá origem ao seu destino que por ventura utilizaremos tal métrica para calcular a quantidade de saltos que o pacote levou de um servidor para outro e sucessivamente até chegar no seu destino final, onde contém informações pertinentes sobre um bom exemplo é o Endereço IP de cada local por onde está se dando o salto que tem um tempo para chegar que é baseado em milissegundos e se ele passar do valor limite ele se perde e mostra como tempo esgotado.

Como podemos ver na figura Figura 1, no presente ano de 2022 algumas *fintechs* tiveram um aumento significativo de downloads , sendo o Nubank com a maior taxa de instalações neste período de janeiro.

A utilização das RC vem sendo muito utilizada e explorada pois um ponto que é vislumbrado é a conexão que interliga milhares de sistemas computacionais e resulta na transmissão de dados sejam eles de envio ou recebimento com troca de tráfego de dados de voz, vídeo e dados sigilosos referentes aos bancos e organizações governamentais.

A segurança da informação (S.I) está presente e se torna necessária para que esse ciclo de perpetuidade se mantenha estável e sem violações perante todas as movimentações e questões que envolvam as diretivas de proteção de dados, tornando assim o ambiente seguro para ser utilizado e trafegado, sendo tratado junto com a Organização Internacional para Padronização (ISO) 27002 que trata sobre as diretrizes relacionadas ao escopo e a proteção das informações do S.I contra possíveis ameaças que possam ocasionar vazamentos de dados ou brechas de segurança para não deixar nada exposto e maximizar o investimento que o contratante faz para sua necessária segurança.

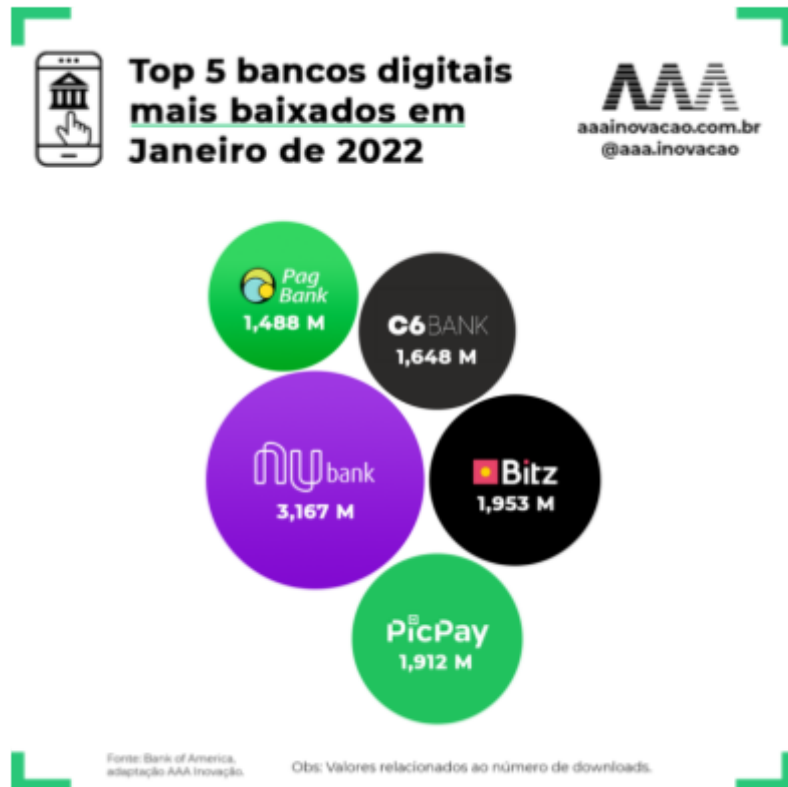
A própria S.I visa a proteção de dados por meio das diretrizes confidencialidade, integridade, disponibilidade e a autenticidade. a confidencialidade de acordo com (PEIXOTO, 2006):

[...] as informações devem ser seguras para que não se dissipem no decorrer do seu destino. Sobre a integridade é a propriedade que garante que as informações não sofreram alterações, mantendo sempre sua veracidade e exatidão. Sobre a disponibilidade e tratada a confidencialidade e a integridade de tais informações para mantê-la sempre disponíveis para confirmação de sua veracidade.

Uma informação importante é que estas diretrizes devem estar presentes para o maior aproveitamento das informações para não haver discordância entre ambos, caso uma das supracitadas venha a ser violada a ISO terá que ser respeitada a todo custo fazendo os prestadores a revisarem seus métodos para resolução de problemas.

Graças a esse advento na tecnologia é necessário frisar a necessidade de testes de segurança para garantir uma melhor usabilidade por parte dos usuários. Uma observação que pode ser feita é no período de abril de 2020 com a questão das porcentagens em relação ao mobile bank que é o que está sendo utilizado para a maior utilidade e facilidade pois é mais fácil estar com o celular na mão do que acesso ao computador.

Figura 1. Bancos mais baixados 2022



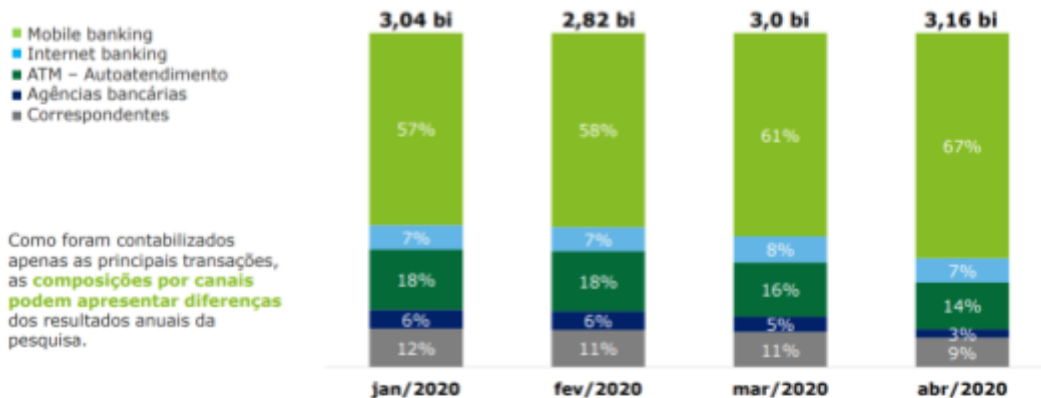
Fonte: <https://blog.aaainovacao.com.br/bancos-digitais/>

Figura 2. Composição de transações por pessoas físicas

IMPACTO COVID-19

Os canais digitais representaram 74% do total das transações pesquisadas em abril de 2020; o aumento de 10 p.p. em relação a janeiro foi impulsionado pelo Mobile Banking

Composição das transações realizadas por pessoas físicas¹



Nota 1: Não foram considerados todas as transações bancárias. Somam-se apenas: Saques, transferências, contratação de crédito, consulta de investimentos, depósitos, pagamentos de contas, saques, recarga de celular.
 Nota 2: Os totais nas colunas estão em milhões de transações.
 © 2020 Deloitte Touche Tohmatsu. Todos os direitos reservados. Pesquisa FEBRABAN de Tecnologia Bancária 2020 33

Fonte: <https://noomis.febraban.org.br/temas/inovacao/canais-digitais-respondem-por-74-15-das-transacoes-bancarias-em-abril>

Como podemos observar na Figura 2 o crescimento da utilização do Mobile Banking está em flutuação e ao mesmo tempo em crescimento graças a evolução das conexões das redes, no qual gerou um bem estar pois possibilitou a compra e utilização destes serviços de qualquer lugar com uma conexão de internet estável. Nesse sentido, a próxima seção tratará como está pesquisa foi desenvolvida.

3. Metodologia

A pesquisa visou analisar a SI nas páginas eletrônicas das *fintechs*, explicando que o escopo desta pesquisa estará vinculado aos bancos digitais, pois estes compõem o rol de alguns dos mais conhecidos bancos digitais.

Conforme Appolinário (2011), esta pesquisa é caracterizada como aplicada, pois realizou uma aplicação direta de testes, tendo em vista avaliar seus níveis de segurança. Já em relação a profundidade é considerada descritiva pois inicialmente foi realizada uma identificação de materiais já publicados, bem como também pode ser caracterizada como experimental quanto ao aspecto pois busca explicar o porquê de tal fenômeno, manipulando deliberadamente algum aspecto da realidade, tendo em vista que foi realizado uma sequência de testes durante o período de uma semana para comparação dos dados obtidos.

Ainda de acordo com Appolinário (2011), a pesquisa foi caracterizada como quali-quantitativa, , quanto ao aspecto qualitativos foi observado a segurança das *fintechs* e no quesito quantitativo foi realizado a verificação dos dados para explanação futura, pois tem de forma geral na primeira parte a análise quantitativa dos dados e posteriormente segue com uma análise mais subjetiva dos dados que foram obtidos através das testagens dos aplicativos webs, no qual foram descritos nesta pesquisa, que contém os dados e ações realizadas durante os testes, dos quais possibilitaram as análises das startup ou *fintechs* e suas funções disponíveis nos *apps* e na páginas eletrônicas, à luz de conceitos de SI.

Ainda segundo Appolinário (2011), a coleta de dados se deu em modelo de campo, quanto ao critério da facilidade de criação de conta nos banco sem a presente necessidade de comprovação de renda e a versão web dos bancos, juntamente com base nas ferramentas e técnicas de Ângelo e Oliveira (2019) *in prelo*, cujas ferramentas descritas nortearam esta pesquisa.

Houve a necessidade ainda de listar as funcionalidades a serem consideradas nas análises das aplicações, pois a clonagem das páginas poderiam ocorrer e essas funções estariam vinculadas aos servidores das páginas eletrônicas clonadas. Nesse sentido, foram listadas as funções comuns disponíveis nos referidos serviços, conforme pode ser observado no quadro 1.

Quadro 1: Funções e Objetivos

ID	Funções	Objetivo
01	Localização de compra	Identificar o nome do estabelecimento e a sua localização geográfica no Google Maps.
02	Fatura	Amostra de todos os gastos que estão acometidos no presente mês.
03	Controle Total do Limite	Ação que possibilita controlar o valor disponível de compra.
04	Dados do Cartão	Informações pertinentes aos dados
05	Investimento	Funcionalidade de investimento em cripto moeda ou ações
06	Transferencias	Realizar a movimentação bancária sendo ela por pix ou não
07	Emprestimo	Pegar um valor antecipado ao banco tendo em vista o ressarcimento através do valor e de juros
08	Atendimento ao cliente	Atendimento com operadores do banco através de um chat
09	Cartão Virtual	Cartão no qual pode ser criado e deletado para utilização sem necessitar usar os dados do fisico.
10	Bloqueio / Desbloqueio	Verificar a possibilidade de bloqueio e desbloqueio dos cartões (virtual ou fisico)

Fonte: Pesquisa direta.

As funções observadas no quadro 1 foram analisadas em cada *fintech*, que compõem os objetos de estudo deste trabalho, a fim de averiguar se cada uma possui tais funções em seus respectivos app e página eletrônica.

As ferramentas Wireshark, terminal de comandos do Windows e do Linux, e *Setoolkit* do Kali Linux foram utilizadas na pesquisa. A ferramenta Wireshark forneceu os relatórios dos acessos aos serviços, principalmente, em relação aos tipos de pacotes trafegados para tais conexões. Os comandos de rede (Ping e Traceroute) listados a seguir também foram ainda utilizados para comparar os resultados obtidos sobre o tráfego de rede da ferramenta Wireshark.

Outro teste foi realizado com a ferramenta *Setoolkit*, disponível no sistema operacional Kali Linux, que teve o objetivo de verificar a possibilidade de clonagem da página eletrônica das *fintechs* listadas nesta pesquisa. A fase de clonagem se deu a partir

dos passos apresentados pela ferramenta, que foi acessado a partir dos privilégios de administrador concebidos pelo acesso do comando SU através do terminal de comandos do Linux.

- Social-Engineering Attacks
- Website Attack Vectors
- Credential Harvester Attack Method
- Site Clonner

A ferramenta setoolkit após ser acessada apresenta em forma de lista opções de escolha no qual o primeiro passo, Social-Engineering Attacks, pode ser selecionada a partir da digitação do número correspondente a sua posição

Selecionado o primeiro passo a ferramenta retorna a apresentar à seleção em lista no qual o usuário deverá escolher a opção que deseja realizar onde a escolhida foi Website Attack Vectors.

Após a escolha da segunda opção uma nova lista é apresentada e o passo seguinte escolhido foi Credential Harvester Attack Method, abrindo assim uma lista reduzida a três escolhas e a selecionada é Site Clonner, sendo necessário colocar o IP da máquina em questão após seguir os passos, sendo necessário colocar o site que deseja realizar a clonagem, seguindo assim para a digitação no browser utilizando o ip da máquina escolhido no passo anterior no local de busca, exibindo assim o site clonado.

Considerou-se como escopo desta pesquisa apenas os exemplos listados anteriormente que possuem sites web disponíveis para acesso e salientando que eles foram escolhidos partindo da premissa que são *fintechs* cujo cadastro é realizado sem necessitar de comprovação de renda e que possam ser acessados pelo navegador web. Destaca-se ainda que bancos tradicionais não estão inclusos no escopo desta pesquisa, a saber Banco do Brasil, Santander, Caixa e Itaú, porque não se enquadram nos termos *startups* ou *fintechs*.

As funções supracitadas no quadro 1 demonstram cada ação que está disponível para cada banco em suas respectivas plataformas exemplo a plataforma mobile do banco nubank traz consigo uma gama de usabilidades onde no site (browser) o usuário tem um acesso limitado deixando restrito funções como cartão virtual, empréstimo e etc. Em comparação com o banco inter que disponibiliza tanto o acesso total no aplicativo mobile quanto no acesso pelo browser.

3.1 Ping

O ping é uma ferramenta no qual foi desenvolvida para testar a disponibilidade entre equipamentos conectados à uma rede e é tão essencial que está presente em quase todos os sistemas operacionais.

O comando ping pode ser utilizado no CMD (Prompt de Comando) do terminal do Windows onde ele mostra a latência em ‘ms’ milissegundos onde quanto menor o tempo melhor foi o tempo de resposta.

Figura 3: Teste de Ping

```
Selecionar C:\Windows\system32\cmd.exe
Microsoft Windows [versão 10.0.19044.1706]
(c) Microsoft Corporation. Todos os direitos reservados.

C:\Users\jonny>www.google.com
'www.google.com' não é reconhecido como um comando interno
ou externo, um programa operável ou um arquivo em lotes.

C:\Users\jonny>ping www.google.com

Disparando www.google.com [142.250.218.196] com 32 bytes de dados:
Resposta de 142.250.218.196: bytes=32 tempo=44ms TTL=55
Resposta de 142.250.218.196: bytes=32 tempo=45ms TTL=55
Resposta de 142.250.218.196: bytes=32 tempo=45ms TTL=55
Resposta de 142.250.218.196: bytes=32 tempo=40ms TTL=55

Estatísticas do Ping para 142.250.218.196:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
    perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 40ms, Máximo = 45ms, Média = 43ms

C:\Users\jonny>
```

Fonte: Pesquisa direta

Como podemos observar na figura acima a mesma contém o seu endereço ip que é o seu nome além do próprio nome do site, e demonstra a quantidade de vezes que foi realizada a solicitação para medir o ping mínimo e máximo.

3.2 Traceroute

Tracert é uma ferramenta que mostra a quantidade de saltos e por quais locais é necessário para que nossa requisição chegue ao local de destino mostrando tanto o local da saída quanto o ponto de chegada.

Na figura 4 pode se observar a sequência de saltos que a requisição teve que ir do ponto raiz para o destino no qual se almejou chegar, que nesta questão foi o site do google com o referido IP 172.217.162.100.

Figura 4: Resultado do comando Tracert

```
C:\Windows\system32\cmd.exe
Microsoft Windows [versão 10.0.19044.1706]
(c) Microsoft Corporation. Todos os direitos reservados.
C:\Users\jonny>tracert www.google.com

Rastreando a rota para www.google.com [172.217.162.100]
com no máximo 30 saltos:

  1    5 ms    1 ms    <1 ms   192.168.1.1
  2    2 ms    2 ms    2 ms   10.105.1.1
  3    5 ms    4 ms    5 ms   200.133.22.254
  4   13 ms   14 ms   18 ms  200.133.31.41
  5    9 ms   12 ms   12 ms  200.133.31.125
  6   10 ms    9 ms   32 ms  170.79.214.157
  7   41 ms   13 ms   20 ms  170.79.213.26
  8   18 ms   17 ms   17 ms  170.79.213.42
  9   25 ms   25 ms   20 ms  170.79.213.28
 10   21 ms   21 ms   20 ms  ba-cba1.bkb.rnp.br [200.143.252.36]
 11   35 ms   33 ms   33 ms  200.143.253.206
 12   44 ms   43 ms   59 ms  nj-es-oi.bkb.rnp.br [200.143.252.85]
 13   60 ms   55 ms   56 ms  sp2-nj-oi.bkb.rnp.br [200.143.253.221]
 14   59 ms   58 ms   65 ms  as15169.saopaulo.sp.ix.br [187.16.218.58]
 15   60 ms   62 ms   60 ms  74.125.243.65
 16   67 ms   60 ms   62 ms  216.239.51.225
 17   61 ms   58 ms   58 ms  gru14s07-in-f4.1e100.net [172.217.162.100]

Rastreamento concluído.
```

Fonte: Pesquisa direta

Teste longitudinais realizados nas respectivas *fintechs* demonstraram que mesmo durante dadas de maior uso como dia dos namorados, no qual o fluxo de dados seria de maior volume e os mesmos não sofreram alteração no tráfego trazendo com sigio uma melhor segurança contra queda e perda de estabilidade durante períodos de pico de transações.

Quadro 2. Classificação da pesquisa

Dimensão	Classificação
----------	---------------

Finalidade	Aplicada
Tipo / Profundidade	Descritiva
Origem dos Dados	Documental / campo
Estratégia	Campo
Natureza	Quali-Quantitativa
Temporalidade	Longitudinal
Delineamento	Levantamento

Fonte: Pesquisa direta.

No quadro (2) acima podemos observar a classificação da pesquisa, tanto na questão da estratégia abordada quanto no seu delineamento e temporalidade, visando os dados que foram analisados no decorrer da pesquisa.

4. Resultado e Discussões

Partindo das análises realizadas nas presentes variáveis foi possível adquirir dados relevantes e explicativos a respeito das funções disponíveis pelos bancos digitais.

Quadro 3: Variáveis Analisadas

Funções	Dispositivo	Nubank	Next	Inter	Pagbank
Locais de compra	Browser	x			
Fatura	Browser	x		x	x
Controle Total do Limite	Browser				x
Dados do cartão	Browser				x
Investimento	Browser			x	x
Transfêrencias	Browser				x
Empréstimos	Browser			x	
Atendimento ao cliente	Browser	x		x	x
Cartão virtual	Browser				
Bloqueio / Desbloqueio	Browser	x			x

Fonte: Pesquisa direta.

Neste quadro 3, pode-se notar algumas informações acerca das funções e ações que são realizadas em seus respectivos sites após a validação do login.

Seguindo com análise pertinente das *fintechs* a quadro 4 abaixo é mostrada algumas funções que estão disponíveis tanto no app quanto nos sites relacionados às startups.

Quadro 4: Análises dos bancos fintechs.

NUBANK		NEXT		INTER		PAGBANK	
FUNÇÕES		FUNÇÕES		FUNÇÕES		FUNÇÕES	
Site	App	Site	App	Site	App	Site	App
Localização da Compras	Ver Fatura	Somente App	Ver Fatura	Empréstimo e ações referentes	Controle das Funções referente ao cartão	Vendas Online	Produtos e Investimento
Faturas	Controle Total do Limite		Controle Total do Limite	Controle das Funções referente ao cartão	Dados do Cartão	Investimentos	Serviços
Atendimento	Empréstimo		Empréstimo	Saldo	Saldo	Transferências	Principais (PIX, adicionar dinheiro, Cartões, pagar contas)
	Cartões Virtuais		Cartões Virtuais	Dados do Cartão	Empréstimo e ações referentes	Acesso Similar ao do APP	Acesso Similar ao do Site

Na quadro 1 vislumbra de forma explanada e detalhada funções de seus respectivos bancos, onde notou-se em certos casos uma singularidade de funcionalidades entre os mesmos.

Quadro 5:Resultado de coleta entre as *fintechs* listadas

Site	Versão do IP	Ping	Tipo do IP	Ping (ms)	IP visível	Tracert	método Teste
nubank.com.br	IPV4	sim	Ip dinâmico	99ms	Sim Via Wireshark	sim	manual via cmd windows
https://pagseguro.uol.com.br/	IPV4	sim	Ip estático	72ms	Sim Via Wireshark	sim	manual via cmd windows
https://next.me/	IPV4	sim	Ip dinâmico	46ms	Sim Via Wireshark	sim	Via cmd e wireshark Kali
https://www.bancointer.com.br/	IPV4	sim	Ip dinâmico	90ms	Sim Via Wireshark	sim	Via cmd e wireshark Kali

Fonte: Pesquisa direta

Testes realizados através da ferramenta wireshark em dois sistemas operacionais distintos o Kali Linux e o Windows 10, visando a melhor obtenção de variáveis no qual gerou a obtenção dos dados totais que resultou na afirmação da mudança do Internet Protocol (IP) em cada tentativa de nova testagem, gerando assim uma segurança maior em relação a ataques direcionados ao IP que é visto na realização do teste, os dados recolhidos no início contém informações acerca dos seguintes testes tracert (windows) traceroute (Kali), Ping, podendo ser observado na tabela 2 acima variáveis que demonstram o tipo utilizado, a latência em milissegundos a possibilidade de um tracert e vislumbra a alocação que neste caso está sendo IP dinâmico.

Os testes realizados utilizando os comandos de ping e tracert foram realizados com diferença longitudinal no qual visou a obtenção de dados para mostrar o determinado modelo de ip utilizado nas fintechs analisadas, no qual testes de tracert

demonstra a quantidade de saltos, na figura 5 abaixo podemos observar os pacotes enviados o ip o TTL e tempo em ms mantendo uma estabilidade após a primeira resposta.e observou-se uma conclusão sem perda de resposta no teste

Figura 5. Ping Bancointer

```
C:\Users\jonny>ping bancointer.com.br

Disparando bancointer.com.br [18.65.48.14] com 32 bytes de dados:
Resposta de 18.65.48.14: bytes=32 tempo=89ms TTL=242
Resposta de 18.65.48.14: bytes=32 tempo=92ms TTL=242
Resposta de 18.65.48.14: bytes=32 tempo=92ms TTL=242
Resposta de 18.65.48.14: bytes=32 tempo=92ms TTL=242

Estatísticas do Ping para 18.65.48.14:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
    perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 89ms, Máximo = 92ms, Média = 91ms
```

Fonte: Pesquisa direta

O mesmo teste foi realizado em uma data x e mostrou um ip diferente onde pode-se observar na figura 5 e ao realizar a comparação entre os dois teste notou-se uma alteração no ip do site, resultando assim em uma melhoria na segurança pois vislumbra um mecanismo que o torna dinâmico o internet Protocol do referido site, dessa forma temos aqui possivelmente um sistema formado por diversas máquinas que respondem de forma sincronizada ao serviço de disponibilidade da fintech analisada..

Figura 6. Ping Bancointer

```
C:\Users\jonny>ping bancointer.com.br

Disparando bancointer.com.br [65.8.214.8] com 32 bytes de dados:
Resposta de 65.8.214.8: bytes=32 tempo=207ms TTL=239
Resposta de 65.8.214.8: bytes=32 tempo=45ms TTL=239
Resposta de 65.8.214.8: bytes=32 tempo=41ms TTL=239
Resposta de 65.8.214.8: bytes=32 tempo=41ms TTL=239

Estatísticas do Ping para 65.8.214.8:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
    perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 41ms, Máximo = 207ms, Média = 83ms
```

Fonte: Pesquisa direta

Figura 7. Tracert PagSeguro

```
C:\Users\jonny>tracert pagseguro.uol.com.br

Rastreando a rota para fp27ad.wpc.gammacdn.net [152.199.52.197]
com no máximo 30 saltos:

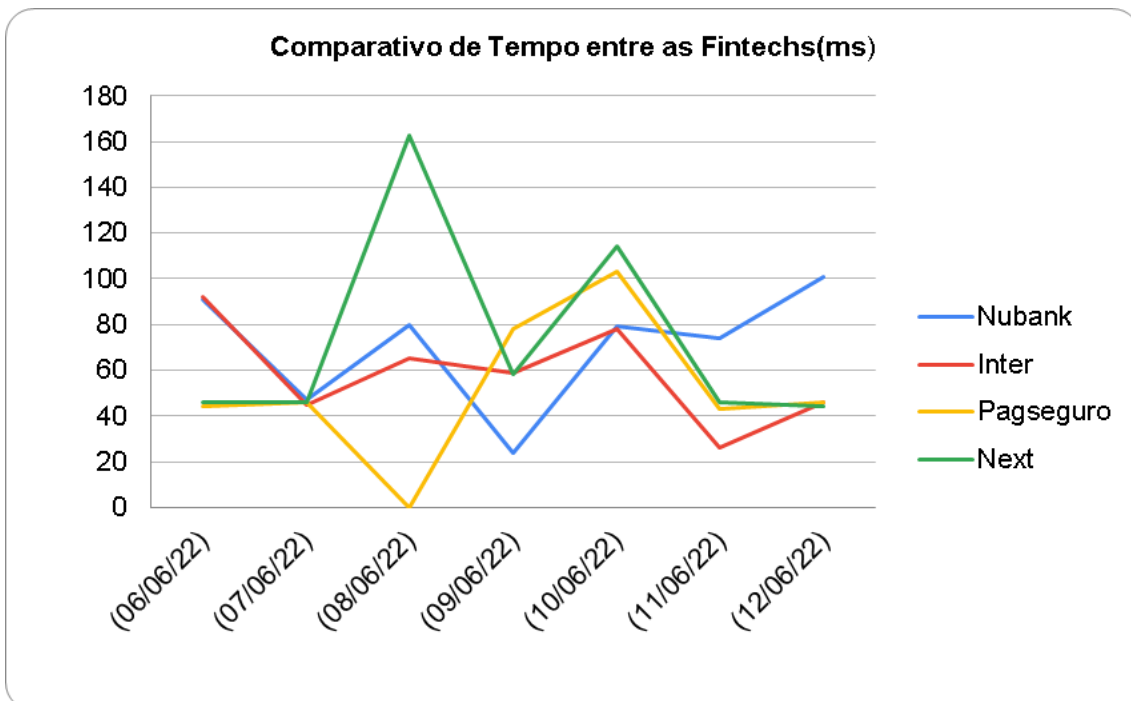
  1    5 ms    5 ms    5 ms    200.133.22.254
  2   11 ms   18 ms   11 ms   200.133.22.254
  3   12 ms   24 ms   12 ms   200.133.31.41
  4   21 ms  101 ms   67 ms   200.133.31.125
  5   12 ms   11 ms   11 ms   170.79.214.157
  6   72 ms   29 ms   22 ms   170.79.213.9
  7   42 ms   15 ms   32 ms   170.79.213.11
  8   96 ms   59 ms   49 ms   170.79.213.41
  9   67 ms   68 ms   64 ms   170.79.213.3
 10   65 ms   65 ms   64 ms   as15133.saopaulo.sp.ix.br [187.16.219.83]
 11   64 ms   64 ms   64 ms   ae-65.core1.spb.edgecastcdn.net [152.195.206.131]
 12   66 ms   64 ms   63 ms   152.199.52.197

Rastreamento concluído.
```

Fonte: Pesquisa direta

Partindo do vislumbre dos dados coletados do teste tracert notou-se que o valor de saltos até a chegada no referido ponto foi de doze (12) tendo uma variação nos milissegundos e relatando que não houve perda de pacotes ou TTL excedido, dessa forma ao se analisar e verificar essas possibilidade partimos para a última fase do teste que foi ir em busca de realizar a clonagem das páginas dos bancos *fintechs*.

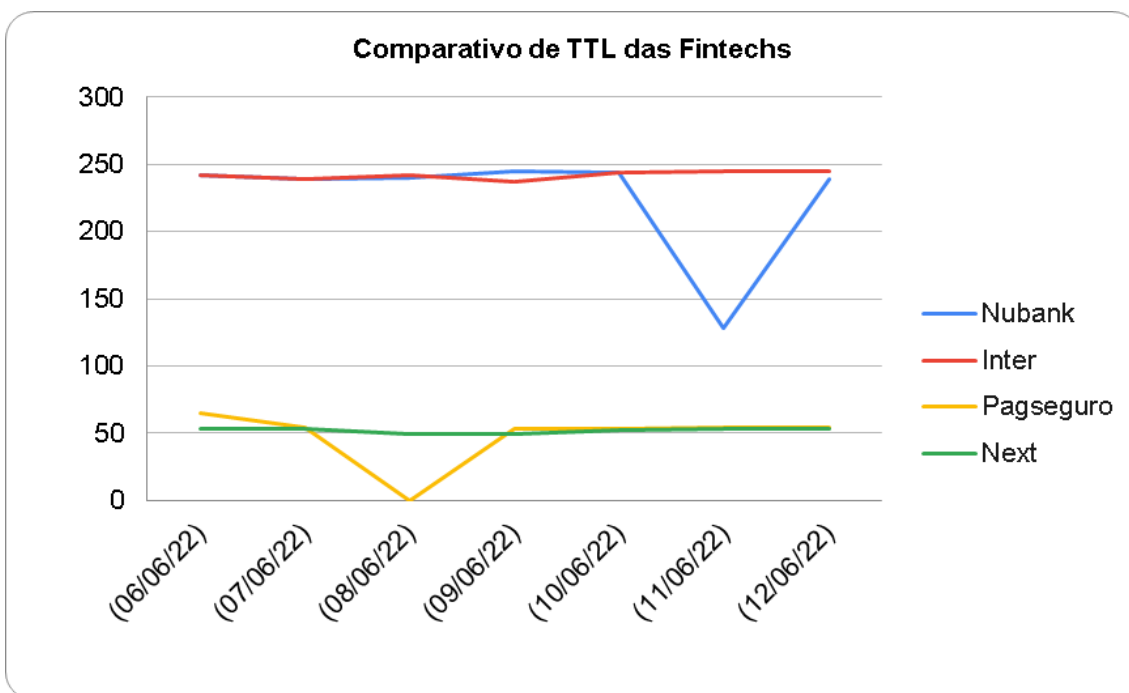
Figura 8. Gráfico Comparativo (MS) das Fintechs



Fonte: Pesquisa direta

Ao se analisar a figura 8 pode-se observar que ocorreu uma leve alteração no tempo em milissegundo durante os testes tendo como pico o dia 08/06/22 referente ao next tendo uma elevação acima do valor de 160.

Figura 9. Gráfico Comparativo TTL das Fintechs



Fonte: Pesquisa direta.

Referente à análise da figura 9 pode-se observar que o banco inter permaneceu com o tempo de vida do pacote o TTL dentro do limite de 230 a 250 tendo um tempo para que o dado chegue maior que as demais *fintechs* explanadas e notasse que e um certo momento o pagseguro teve seu tempo esgotado e levando a perda do pacote nesse referido dia, Já o banco next manteve uma estabilidade com um valor mínimo no qual ficou em 50 o TTL .

Quadro 6: Resultado de coleta de médias acerca das *fintechs* listadas.

Médias	Nubank	Inter	Pagseguro	Next
TTL	240	242	54	53
Tempo (ms)	79	59	46	46

Fonte: Pesquisa direta

Graças às análise das figuras 8 e 9 foi possível explicar e relatar os dados acometidos e recolhidos nos referidos testes dentro do período longitudinal do dia 06/06/22 a 12/06/22 relatando quais se mantiveram estáveis e com disponibilidade para os usuários mesmo em dias de pico. No Quadro 6 relata as médias tanto de TTL quanto

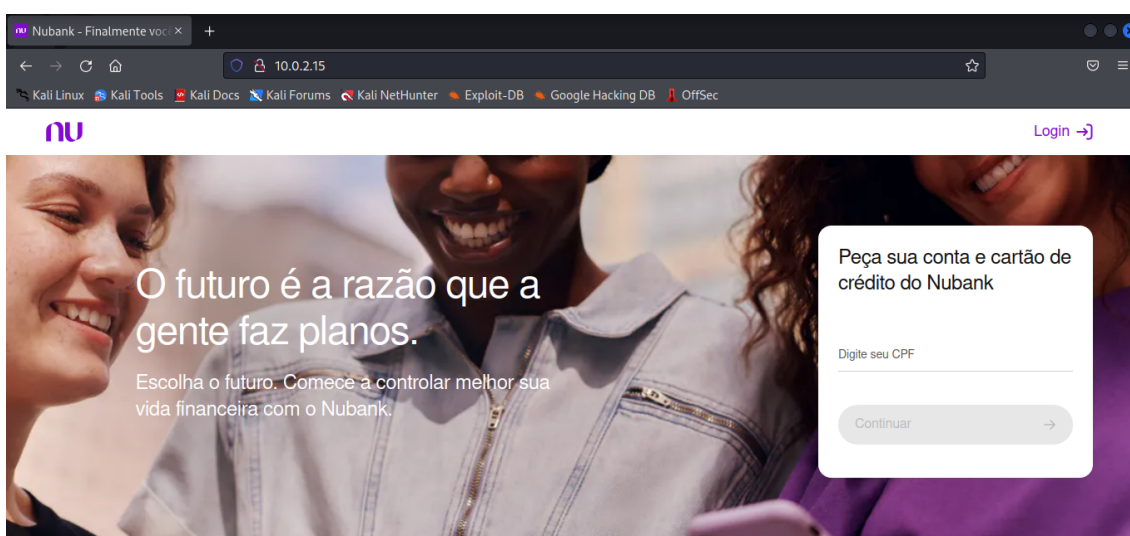
de MS de cada banco digital testado, e os que se mostraram com maior tempo de vida dos pacotes foram o Nubank e o Inter que se sobressaíram à frente das demais testadas.

Partindo de testes que foram realizados com a ferramenta setoolkit que foi utilizada no sistema operacional Kali linux e partindo das funcionalidades desta ferramenta foi realizado a clonagem de três sites referentes às *fintechs*.

4.1 Banco Nubank

O primeiro teste que foi feito é referente ao site do Nubank.com.br, onde foi observado que houve uma clonagem semelhante mas teve objetos e aspectos que não vinham perante sua clonagem como os menu que estão presente no código da figura abaixo, salientando que durante o mesmo teste os botões direcionam para o mesmo a página principal.

Figura 10. Clonagem do site da Nubank



Fonte: Pesquisa direta

Figura 11. Código fonte do site Nubank

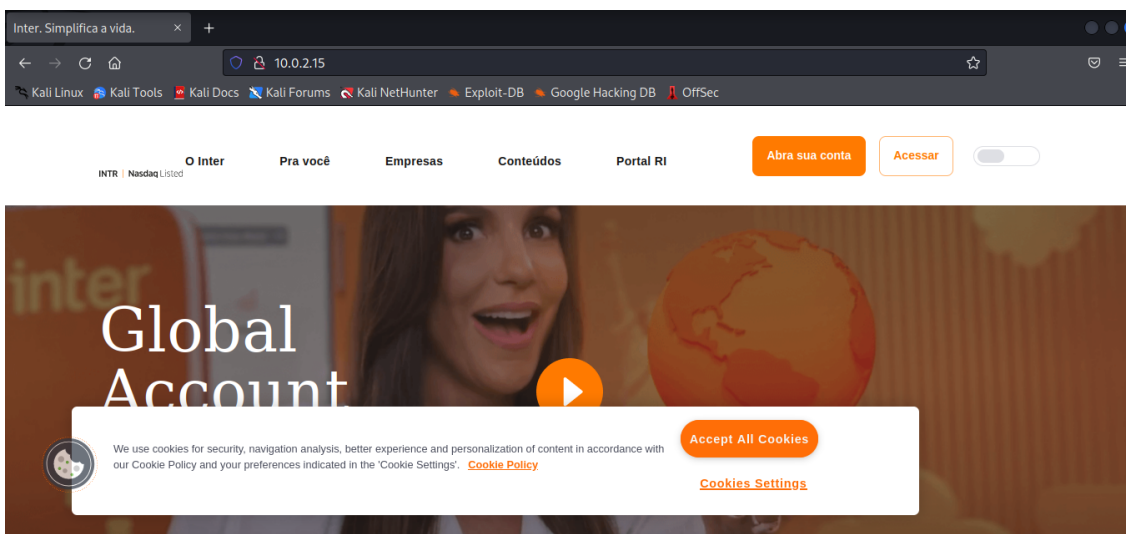
```
> <div class="sc-qXhiz lZZk">...</div> grid
▼ <nav class="sc-qXhiz vozPK NavigationListSmallScre
nWrapper-sc-1ghillz-0 ewaPpz"> == $0
  ▼ <ul class="sc-qXhiz vozPK" role="menubar">
    ▶ <li class="sc-qXhiz bHzJYh">...</li>
    ▶ <li class="sc-qXhiz bHzJYh">...</li>
    ▶ <li class="sc-qXhiz bHzJYh">...</li>
    ▶ <li class="sc-qXhiz bHzJYh">...</li>
    ▶ <li class="sc-qXhiz bHzJYh">...</li>
  </ul>
  ▶ <div class="sc-qXhiz jxCjLA">...</div>
</nav>
</div>
```

Fonte: <https://nubank.com.br/>

4.2 Banco Inter

Após a realização da clonagem do site do banco Inter, nota-se que a tela de cookies foi adicionada juntamente, a logo que tem no canto superior próximo ao menu do cabeçalho, o botão ao lado do acesso que contém as bandeiras para mudança de idioma não veio, a central de ajuda está em falta, o carrossel de imagens que deveria estar na parte de baixo mas não veio, imagens com desfocamento em alto grau e ícones em falta, o vídeo que está presente não é executável

Figura 12. Clonagem do site da Inter

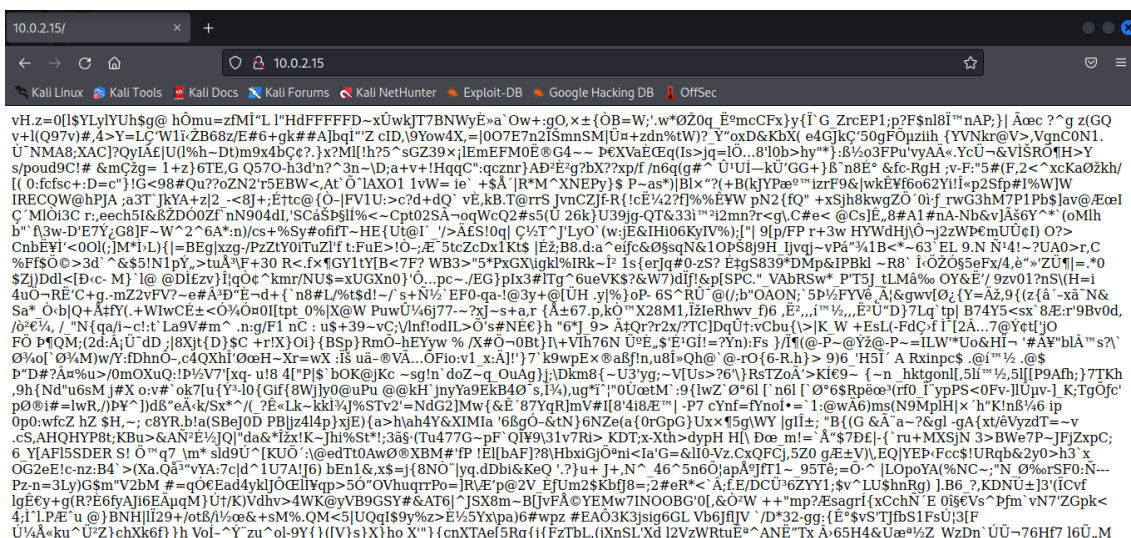


Fonte: Pesquisa direta

4.3 Banco Pagueuro

O teste realizado no presente site do pagueuro.oul.com.br a ferramenta não obteve sucesso em mais de uma tentativa em datas e conexões diferentes, pode-se observar uma segurança maior em relação ao site e sistemas que estão inclusos, pois a informação obtida partindo do teste está na figura abaixo, onde a referida mostra uma criptografia que impossibilita a visualização e clonagem dos dados que deveriam estar presente e visível para utilização da página clonada

Figura 13. Clonagem do site da Pagueuro



Fonte: Pesquisa direta.

Após uma comparação entre ambos os sites clonados e reais, observa-se algumas divergências, como o local mostrado na url é diferente ao utilizado no site principal e não traz consigo o cadeado de segurança com o código Secure Sockets Layer (SSL) o certificado digital que autentica a identidade do site, botões direcionam para o site principal, os sites clonados vinherem com falta de informações, no qual não os tornam cópias fiéis e notou-se uma segurança onde prevaleceu de ocultar alguns aspectos ou o bloqueio do site como foi explanado na Figura 13 que mostrou uma criptografia durante a realização tornando o mesmo mais seguro mesmo mantendo um ip estático como apresentado no quadro 5.

5. Considerações Finais

De forma geral, este trabalho buscou explicar a utilização dos métodos de testagem e conhecimentos pertinentes às *fintechs* e questões voltadas para a área da segurança da informação, onde inclui dados referentes à maneira e comportamento que melhoram a segurança para o usuário e a prestadora do serviço.

Quanto aos resultados obtidos foi vislumbrado a necessidade da realização dos mesmos, pois trazem consigo um ponto de vista voltado ao usuário no quesito a segurança dos dados e a proteção da empresa quanto às informações disponibilizadas.

Para trabalhos futuros fica a sugestão de testes referentes a Phishing-as-a-Service (PhaaS), e novos métodos de clonagem para deixar o site mais fiel tanto no quesito do conteúdo quanto ao link mostrado na url.

6. Referências

ANGELO, R; OLIVEIRA, F. K. Engenharia Social e Phishing a partir da ferramenta SeToolKit. Trabalho de Conclusão de Curso. Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano (IFSertãoPE). Salgueiro, 2019. *in prelo*.

Appolinário, F. (2011) “Metodologia da ciência: filosofia e prática da pesquisa”, 2ª edição, páginas 62-70.

BRASIL. BANCO CENTRAL DO BRASIL - BCB. **Fintechs**. 2022. Disponível em: <<https://www.bcb.gov.br/estabilidadefinanceira/fintechs>>. Acesso em: 07/08/2022.

DE OLIVEIRA, Jeferson Gonçalves et al. INTERNET DAS COISAS E PRIVACIDADE: UMA REVISÃO SISTEMÁTICA DA LITERATURA.

FONTES, Edison Luiz Gonçalves. Segurança da informação. Saraiva Educação SA, 2017.

Hostmidia. (2022) “Traceroute: o que é, como funciona e como usar?”, Disponível em: <https://www.hostmidia.com.br/blog/traceroute/> Acessado em 06/07/2022

Pickert, L. (2022) “Bancos Digitais estão superando os Maiores Bancos do Brasil”, <https://blog.aaainovacao.com.br/bancos-digitais/>. Acessado em 06/07/2022

Tadeu, E. (2020) “Canais digitais respondem por 74% das transações bancárias em abril”

<https://noomis.febraban.org.br/temas/inovacao/canais-digitais-respondem-por-74-das-transacoes-bancarias-em-abril> Acessado em 06/07/2022

SOUSA, Lindeberg Barros. Redes de computadores. Dados Voz e Imagem, 2009.