UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS DE RUSSAS

CURSO DE GRADUAÇÃO EM ENGENHARIA DE SOFTWARE

JOSÉ MOAB DE SOUZA ALVES

UMA ANÁLISE DAS POSTAGENS DOS USUÁRIOS QUANTO A SUA SEGURANÇA EM APLICATIVOS DE INSTITUIÇÕES FINANCEIRAS

RUSSAS

2022

JOSÉ MOAB DE SOUZA ALVES

UMA ANÁLISE DAS POSTAGENS DOS USUÁRIOS QUANTO A SUA SEGURANÇA EM APLICATIVOS DE INSTITUIÇÕES FINANCEIRAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Software do Campus de Russas da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia de Software.

Orientadora: Profa. Dra. Marília Soares Mendes

Coorientador: Ms. Thiago H. Oliveira da Silva

RUSSAS

2022

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

A479a Alves, José Moab de Souza.
Uma análise das postagens dos usuários quanto a sua segurança em aplicativos de instituições financeiras / José Moab de Souza Alves. – 2022.
76 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Russas, Curso de Engenharia de Software, Russas, 2022.
Orientação: Profa. Dra. Marília Soares Mendes.
Coorientação: Prof. Me. Thiago H. Oliveira da Silva.

1. Segurança. 2. Avaliação Textual. 3. Mobile Banking. 4. Classificação de Postagens. 5. Processamento de Linguagem Natural. I. Título.

CDD 005.1

JOSÉ MOAB DE SOUZA ALVES

UMA ANÁLISE DAS POSTAGENS DOS USUÁRIOS QUANTO A SUA SEGURANÇA EM APLICATIVOS DE INSTITUIÇÕES FINANCEIRAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Software do Campus de Russas da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia de Software.

Aprovada em:

BANCA EXAMINADORA

Profa. Dra. Marília Soares Mendes (Orientadora)
Universidade Federal do Ceará (UFC)

Ms. Thiago H. Oliveira da Silva (Coorientador)
Universidade Coorientador (SIGLA)

AGRADECIMENTOS

A Deus! Por ter estado sempre comigo, por ter me guiado até aqui e por ter me dado forças para superar todas as dificuldades durante a minha caminhada.

A minha mãe, Rejane, por sempre estar ao meu lado em todos os momentos, me apoiando, me mantendo de pé, acreditando e investindo em mim. Obrigado por tudo mãe, isso tudo é para você! Você é a razão do meu viver! Te amo muito.

Ao meu pai, Moacir, por sempre acreditar, torcer por mim, e me apoiar quando precisei! Te amo pai.

A minha tia, Adelian, por ser uma segunda mãe para mim, por sempre me apoiar e sempre me aconselhar em todos os momentos. Muito obrigado tia, te amo muito!

Ao meu tio e padrinho, Josean, por ser um segundo pai para mim, por tudo que fez para que eu pudesse ter chegado até aqui, por todo apoio, todos os conselhos e todo incentivo. Muito obrigado tio, amo você!

As minhas tias, Zilian, Vilian e Jalka, pelas orações, por sempre torcerem por mim, e me apoiarem quando precisei. Amo muito vocês!

Ao meu tio, Joatan, por desde o início me apoiar e por tudo que fez por mim ao longo desta caminhada. Obrigado tio, suas palavras e conselhos foram fundamentais para que eu chegasse até aqui!

Aos meus demais familiares, por sempre me apoiarem e me incentivarem durante esta caminhada.

Ao meu amigo e irmão de longa data, Airlon, por ter me apoiado desde o início e por toda a parceria até aqui. Obrigado por todos os conselhos, por toda a paciência e por tudo que fez por mim. Sempre serei grato!

Aos meus amigos, Arthur, Fabricio e Orlando, pela amizade, parceria e por tudo que fizeram por mim. Tenho-os como irmãos que a UFC me presenteou! Obrigado por tudo, vocês são muito especiais para mim!

A minha amiga, Anna, que sempre esteve junto comigo durante toda essa caminhada, me apoiando e me ajudando a enfrentar as dificuldades. Você foi um presente que a UFC me deu, muito obrigado por tudo amiga, você é muito especial para mim!

A minha amiga, Nayara, por ter estado sempre comigo quando precisei, pelos puxões de orelha que me deu, e por todos os conselhos. Você é muito especial para mim, obrigado por tudo!

A minha amiga, Emmily, por ter me apoiado desde o início, por sempre ter torcido por mim e por sempre ter estado ao meu lado quando precisei. Você é muito especial para mim, obrigado por tudo!

A minha amiga, Nágila, pelas palavras de apoio, pela força que sempre me deu, e por estar ao meu lado desde o início. Obrigado por tudo, você é muito especial para mim!

A minha amiga, Rochely, por todo apoio e por sempre torcer por mim. Tenha certeza que você faz parte da minha família! Muito obrigado por tudo.

Aos meus amigos e irmãos, Eneas e João, por estarem sempre comigo, nos momentos bons e ruins, me apoiando e me mantendo firme em meio às dificuldades. Obrigado meus amigos, vocês são muito especiais para mim!

Aos meus amigos Heverton, Renan, Helder e Henildo pela amizade, pelo apoio, pelos conselhos e por sempre estarem comigo quando precisei! Obrigado meus amigos, vocês são muito especiais para mim!

A minha querida professora e orientadora, Marília, por toda confiança e apoio. Tenho muita admiração pela pessoa e profissional que és, e muito orgulho de ter sido seu orientando e aluno. Os conhecimentos compartilhados foram muito enriquecedores para mim, e os levarei para a vida toda. Muito obrigado por tudo!

Ao meu co-orientador, Thiago, por além de ter me auxiliado desde o início, ter se tornado um grande amigo e sempre ter acreditado em mim, me dando forças para chegar até aqui através de suas palavras e conselhos. Muito obrigado Thiago!

E por último, a mim, por nunca ter desistido, e por sempre lutar pelos meus sonhos, mesmo em meio às dificuldades.

“A persistência é o caminho do êxito.”

(Charles Chaplin)

RESUMO

Aplicativos para realizar transações financeiras têm sido amplamente adotados por bancos para disponibilizar seus serviços de forma online. Com a difusão da tecnologia, novas instituições financeiras têm surgido trazendo consigo a proposta de operar 100% de forma digital, ou seja, sem dispor de agências físicas. Com a popularização deste novo tipo de instituição financeira, os bancos tradicionais (aqueles que possuem agências físicas) começaram a ampliar a oferta de serviços prestados em seus aplicativos. Desta forma, os usuários começaram a realizar ainda mais suas transações financeiras pelo aplicativo de seu banco. Por outro lado, esta popularização trouxe uma constante preocupação, uma vez que as fraudes se tornaram cada vez mais comuns no ambiente digital. A experiência do usuário na utilização destes serviços pode ser impactada negativamente por problemas relacionados à segurança, e para contornar isso, os usuários desses aplicativos devem ter o sentimento de que seus dados e transações são mantidos e realizados de forma segura. A partir desta preocupação, este trabalho propõe a realização de uma análise das postagens no que se refere à sua segurança, consequentemente à segurança das suas informações em aplicativos de instituições financeiras. Para isso, foi realizado um experimento envolvendo a escolha de aplicativos de instituições financeiras, e com base na opinião dos usuários publicada nas lojas de aplicativos na rede social Twitter, foram identificados cenários de uso que podem gerar preocupação aos usuários quanto à sua segurança. Com base nestas análises, também foi feito o mapeamento destes problemas a fim de apontar possíveis formas de contorná-los.

Palavras-chave: Segurança. Avaliação Textual. Mobile Banking. Classificação de Postagens. Processamento de Linguagem Natural.

ABSTRACT

Applications for carrying out financial transactions have been widely adopted by banks to make their services available online. With the diffusion of technology, new financial institutions have emerged bringing with them the proposal to operate 100% digitally, that is, without having physical branches. With the popularization of this new type of financial institution, traditional banks (those with physical branches) began to expand the offer of services provided in their applications. In this way, users began to carry out their financial transactions even more through their bank's application. On the other hand, this popularization has brought a constant concern, since frauds have become increasingly common in the digital environment. The user experience when using these services can be negatively impacted by security-related issues, and to circumvent this, users of these applications must have the feeling that their data and transactions are held and carried out in a secure manner. Based on this concern, this work proposes to carry out an analysis of the posts regarding their security, consequently the security of their information in applications of financial institutions. For this, an experiment was carried out involving the choice of applications from financial institutions, and based on the opinion of users published in the application stores on the social network Twitter, usage scenarios were identified that may generate concern for users regarding their safety. Based on these analyses, these problems were also mapped in order to point out possible ways to circumvent them.

Keywords: Security. Textual Evaluation. Mobile Banking. Post Classification. Natural Language Processing.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

API	*Application Programming Interface*
BACEN	Banco Central do Brasil
HTTP	*Hypertext Transfer Protocol*
JSON	*JavaScript Object Notation*
NLTK	Natural Language Toolkit
NPM	*Node Package Manager*
PLN	Processamento de Linguagem Natural
PRUs	Postagens Relacionadas ao Uso
URL	*Uniform Resource Locator*
UUX	Usabilidade e Experiência do Usuário
UX	User Experience

SUMÁRIO

1 INTRODUÇÃO

As aplicações móveis estão transformando a tecnologia do setor bancário, fornecendo aos seus clientes novos meios de transações e comunicação, e abrindo espaço também para novos modelos de negócios, como a oferta de serviços financeiros de forma 100% digital, além de transformar a forma como as pessoas utilizam esse tipo de serviço.

O mobile banking, segundo Shaikh e Karjaluoto (2016), refere-se a um meio de acesso, pelo consumidor, a serviços bancários e a capacidade de realizar transações financeiras por meio de smartphones e tablets. O surgimento da tecnologia móvel trouxe novas oportunidades para o setor bancário, e proporcionou aos consumidores mobilidade na utilização dos serviços ofertados, visto que é possível acessá-los de qualquer lugar, desde que exista conexão disponível à internet.

Embora apresente inúmeras vantagens, esta nova tecnologia apresenta vulnerabilidades (YILDIRIM; VAROL, 2019), que acabam gerando um sentimento de insegurança, dificultando a adoção e adaptação dos usuários a estes serviços bancários. De acordo com Yildirim e Varol (2019), a segurança é um grande problema na adoção de mobile banking e muitos usuários relatam sua preocupação com a segurança no acesso a dados financeiros em dispositivos móveis. A garantia de segurança das informações é uma das prioridades das instituições financeiras e uma das principais exigências dos usuários ao utilizar serviços bancários.

A segurança da informação diz respeito às informações técnicas, como questões de segurança, bem como informações não técnicas, relacionadas a humanos (KRITZINGER; SMITH, 2008). No entanto, de acordo com Crossler *et al.* (2013) os estudos se concentram principalmente em questões técnicas, negligenciando, assim, as questões humanas relacionadas. Portanto, problemas de segurança tornaram-se comuns em diversos setores, principalmente nos setores bancários. Problemas deste tipo não podem ser desconsiderados, e questões humanas devem receber a mesma atenção que questões técnicas, visto que a experiência do usuário está diretamente relacionada aos sentimentos e emoções do usuário ao utilizar sistemas interativos (BARBOSA; SILVA, 2010), e problemas de segurança podem impactar negativamente a experiência do usuário ao causarem sentimentos de desconfiança e preocupação na realização de transações e manutenção de dados de forma segura.

Com base nessas questões, este trabalho apresenta a realização de uma análise das postagens dos usuários de aplicativos de instituições financeiras quanto a sua segurança, bem como a segurança de suas informações. Para isso, foi feito um experimento a partir de aplicativos

selecionados e opiniões de usuários publicadas em lojas de aplicativos e na rede social Twitter, com o objetivo de investigar a opinião dos usuários sobre segurança em aplicativos de instituições financeiras.

Nesse experimento foram realizados os seguintes procedimentos metodológicos: (1) busca por aplicativos de instituições financeiras nas lojas de aplicativos *Google Play Store* e *App Store*, com o objetivo de os conhecer melhor e levantar informações necessárias para definir quais são utilizados no estudo deste trabalho e o porquê da utilização dos mesmos; (2) definição de aplicativos para estudo, com o objetivo de selecionar os aplicativos que serviram de base para a extração de postagens dos usuários; (3) realização de uma avaliação textual, com o objetivo de identificar e classificar os principais problemas de segurança da informação na utilização dos aplicativos através das postagens dos usuários; e (4) análise dos resultados, com o objetivo de através das postagens extraídas e classificadas, realizar um mapeamento dos principais problemas encontrados.

A opinião destes usuários por meio de textos vem sendo frequentemente utilizada para avaliações de User Experience (UX), e esse tipo de avaliação tem apresentado bons resultados, sobretudo por ser capaz de identificar problemas que em outros tipos de avaliação seriam dificilmente encontrados (FREITAS *et al.*, 2016). Segundo Mendes (2015), a avaliação textual consiste em utilizar narrativas dos usuários a fim de avaliar ou obter alguma percepção sobre o sistema por meio de suas postagens. Portanto, com base nestas análise, é apresentado o mapeamento dos principais problemas de segurança envolvidos no uso dos aplicativos da Caixa e do Nubank.

1.1 Motivação

Diante da nova realidade imposta pelos efeitos da pandemia da COVID-19, a utilização de meios digitais tornou-se essencial e passou a ser ainda mais incentivada. As novas necessidades alinhadas à nova realidade de distanciamento social, resultaram em avanços expressivos na digitalização dos serviços bancários, consolidando-se neste setor. Segundo a Deloitte, entre janeiro e abril de 2020, por exemplo, logo nos primeiros efeitos da pandemia, as transações bancárias realizadas por pessoa física via celular cresceram 22%, com queda no mesmo período de 53% nas agências (BOLLINI, 2021).

A tecnologia coloca os bancos em uma nova era e isso é um ponto positivo. Estamos diante de instituições modernas e com serviços muito mais acessíveis (MONTINI, 2021). Com

isso, torna-se necessário investir em ferramentas tecnológicas, principalmente relacionadas à segurança, tendo em vista que o ambiente online está sujeito a ações de criminosos. Segundo Yoon e Barker Steege (2013), muitos clientes acreditam que são vulneráveis a roubo de identidade utilizando serviços de *internet banking*, e portanto, a segurança é uma das categorias mais importantes em serviços bancários. A segurança é uma das principais fontes de insatisfação em serviços bancários pela internet (POON, 2008).

A partir disso foi motivada esta pesquisa, tendo em vista que a segurança é um dos principais fatores levados em consideração pelos usuários de serviços bancários digitais, e como citado anteriormente, uma das principais fontes de insatisfação neste tipo de serviço, impactando diretamente na experiência do uso. Portanto, a pesquisa propõe uma análise das postagens dos usuários quanto a sua segurança em aplicativos que fornecem este tipo de serviço, chamados também de aplicativos de *mobile banking*, e busca responder as perguntas a seguir.

(1) Quais os principais problemas de segurança envolvidos no uso de aplicativos de instituições financeiras?

(2) Quais os principais problemas de segurança envolvidos no uso dos aplicativos da Caixa e do Nubank?

(3) Como classificar de forma automática postagens relacionadas à segurança?

1.2 Objetivos

1.2.1 Objetivo geral

Contribuir com o desenvolvimento de aplicativos mais seguros, a partir da análise e classificação das postagens dos usuários quanto a sua segurança em aplicativos de instituições financeiras, sejam eles bancos digitais ou bancos físicos que possuem funcionalidades digitais.

1.2.2 Objetivos específicos

- Investigar a opinião dos usuários sobre segurança nos aplicativos das instituições financeiras Caixa e Nubank;
- Desenvolver um algoritmo de classificação automática de postagens relacionadas a segurança em aplicativos de instituições financeiras;
- Apresentar um mapeamento dos problemas a partir das postagens investigadas e classificadas.

1.3 Metodologia

Nesta seção são apresentados os procedimentos metodológicos utilizados para atingir os objetivos desta pesquisa. Foram realizados os seguintes procedimentos, como mostra a Figura 1: (1) pesquisa por aplicativos de instituições financeiras; (2) definição de aplicativos para estudo; (3) realização de avaliação textual; e (4) análise dos resultados.

Figura 1 – Procedimentos metodológicos.

Fonte: elaborado pelo autor (2022).

1.3.1 Pesquisa por aplicativos de instituições financeiras

Nessa etapa foi realizada uma pesquisa dos aplicativos de instituições financeiras nas lojas de aplicativos *Google Play Store* e *App Store*. A busca foi realizada por meio do filtro da categoria de Finanças de cada loja de aplicativo, categoria na qual estes aplicativos estão inseridos em ambas as lojas. O objetivo desta pesquisa foi conhecer melhor os aplicativos de instituições financeiras que existem e que estão disponíveis nessas plataformas, para que posteriormente fossem definidos quais serão utilizados no estudo deste trabalho e o porquê da utilização dos mesmos.

1.3.2 Definição de aplicativos para estudo

Nessa etapa foram definidos os aplicativos utilizados no estudo, que servirão de base para a extração de postagens dos usuários. Foram definidos critérios para a seleção, baseados em

informações relacionadas aos aplicativos bem como à instituição financeira a qual pertencem. Portanto, esta etapa teve como objetivo principal selecionar os aplicativos para estudo e com base neles realizar as próximas etapas, que consistem na realização de uma avaliação textual e a análise dos resultados obtidos.

1.3.3 Realização de avaliação textual

Para esta etapa foi realizada uma avaliação textual, com base nas postagens dos usuários na rede social *Twitter* e nas páginas dos aplicativos selecionados, nas lojas *Google Play Store* e *App Store*.

Portanto, o principal objetivo desta etapa foi coletar, identificar e classificar os principais problemas de segurança da informação na utilização dos aplicativos através destas postagens. Como a MALTU não possui um modelo pré-definido para identificação e extração de postagens relacionadas à segurança da informação, foi realizado um estudo para identificar e utilizar palavras-chave para classificação automática das postagens. Neste estudo foi realizada inicialmente uma classificação manual a partir das postagens extraídas, com o objetivo de obter apenas as que são relacionadas à segurança. Com base nas postagens obtidas através desta classificação manual, foi executado um algoritmo de frequência de palavras, com o objetivo de obter as palavras mais frequentes nestas postagens e utilizá-las como palavras-chave na classificação automática.

Para realização desta classificação automática foi desenvolvido um algoritmo em *Python*, que utiliza *spaCy*, uma biblioteca para processamento avançado de linguagem natural. Este algoritmo utiliza as palavras-chave obtidas através do algoritmo de frequência citado anteriormente, e realiza uma correspondência com as palavras contidas nas postagens, com o objetivo de extrair e classificar as postagens que contenham estas palavras.

Com base nisso, foi possível mapear os principais problemas de segurança envolvidos no uso destes aplicativos e analisá-los conforme é apresentado na próxima etapa.

1.3.4 Análise dos resultados identificados sobre segurança

Nessa etapa são listados e categorizados os problemas encontrados. Esta etapa foi realizada com base nos problemas descritos nas postagens extraídas e classificadas, para com isso realizar um mapeamento destes problemas. Na próxima seção são apresentados os principais conceitos envolvidos no contexto deste trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

Como neste trabalho é apresentada uma investigação da segurança em aplicativos de instituições financeiras, são apresentados conceitos relacionados, como: segurança da informação, tipos de bancos, físicos e digitais, avaliação textual e Processamento da Linguagem Natural (PLN).

2.1 Segurança da informação

Li *et al.* (2021) definem segurança como uma forma de proteger e garantir, bem como evitar que hackers ataquem informações e a privacidade do cliente. Consequentemente, dizer que algo é seguro significa dizer que é algo estável e certo, portanto, segurança expressa um sentimento de certeza. A informação nesse contexto é um ativo de valor pertencente a um indivíduo ou uma organização, compreendendo dados pessoais, dados relacionados a projetos, dados financeiros e dados bancários, sendo este último o foco principal deste trabalho.

A segurança da informação, segundo Goldstein *et al.* (2011), é considerada um meio crítico de garantir a disponibilidade, confidencialidade e integridade das informações e ativos relacionados de uma organização e, portanto, ajuda a prevenir eventos de perda operacional. Andress (2014) define confidencialidade como a capacidade de manter dados de terceiros não autorizados para visualizá-los; integridade como a capacidade de proteger as informações de mudanças indesejáveis; e disponibilidade como a capacidade de acessar informações quando e onde desejar. Desse modo, a segurança da informação tem como objetivo garantir ao proprietário da informação que nada de ruim acontecerá com ela. Porém, sempre haverá um risco, mesmo que a informação esteja armazenada restritamente. Em vista disso cabe aos profissionais da área trabalhar e zelar para que esse risco seja o menor possível, adotando constantemente técnicas e ferramentas atuais.

De acordo com Soares *et al.* (2013), a segurança da informação compreende um amplo conjunto de técnicas que visam o fornecimento de serviços de segurança, confidencialidade, integridade e autenticação a essas informações. O conceito pode ser estendido e aplicado a sistemas de computador: um sistema é seguro se ele fornece os serviços de segurança desejados para as informações que trata. Todas as organizações devem ter um modelo de segurança da informação, e este é um recurso ou informação a ser protegida e mantida com segurança. Segundo Althobaiti e Mayhew (2014) os sites de bancos são um daqueles que tornam a segurança

uma prioridade, pois lidam com informações confidenciais. Informações importantes de alto risco, como nomes de usuários, senhas e detalhes de cartões de crédito, são enviados por meio de sites para servidores de destino. Esses dados precisam ser protegidos por sites, que implantam protocolos, como certificados SSL, para criptografar informações confidenciais.

A importância do ser humano é nítida ao se deparar com situações como compras online, em que é necessário o fornecimento de dados como senhas, dados de contas bancárias, dados de cartões de crédito, endereços, entre outros. Todos esses dados são sigilosos e devem ser protegidos de qualquer tipo de ameaça ou risco. Nesse contexto, a cibersegurança é responsável pela garantia de que tais dados estejam acessíveis apenas para os indivíduos que possuem autorização para eles.

2.2 Bancos físicos ou tradicionais

Os bancos físicos ou tradicionais são caracterizados, principalmente por possuírem agências físicas e por oferecerem grande parte dos seus serviços financeiros de forma presencial, seja no caixa eletrônico presente na agência, ou por intermédio de funcionários do banco - no atendimento presencial. Chiorazzo *et al.* (2018) definem bancos tradicionais ou sistemas bancários tradicionais por quatro características: empréstimos de relacionamento, financiamento de depósito básico, fluxos de receita provenientes dos tradicionais serviços bancários, e a agências bancárias físicas.

No quesito segurança, à primeira vista, os bancos tradicionais demonstram ser seguros e confiáveis, dado o seu longo tempo de atuação na sociedade além de ter diversas agências físicas onde é possível se ter um contato pessoal com um gerente de conta.

2.3 Bancos digitais

Segundo Leite (2019), banco digital é o nome dado às instituições financeiras que funcionam de forma online. Isso significa que praticamente tudo o que o cliente precisa pode ser feito virtualmente, desde a abertura da conta ao atendimento de suporte e pagamento de boletos.

Portanto, um banco digital é caracterizado pela oferta de seus produtos e serviços de forma digital, sem a necessidade de se locomover até uma agência, sendo esta outra característica, de não possuir estruturas físicas como nos bancos tradicionais. Mtambalika *et al.* (2016) definem como um canal de distribuição usado para fornecer serviços financeiros sem depender

necessariamente da construção de agências bancárias. Isto oferece aos clientes a capacidade de realizar transações bancárias em uma ampla gama de varejo em vez de acessar serviços em agências bancárias.

Segundo Pereira (2021), os novos hábitos adquiridos pela população durante o isolamento social aceleraram a participação dos bancos digitais no Brasil. Apesar do poder financeiro e da alta concentração das instituições tradicionais, esses novos personagens estão dando cara nova ao sistema financeiro nacional, que aos poucos ganha mais competição. Sem tarifas nem agências bancárias, alguns conseguiram dobrar a carteira de clientes durante a pandemia e ganharam, pelo menos, três anos na corrida por maior presença no setor.

Por serem compostos por operações inteiramente digitais, essas instituições financeiras conseguem ter um menor custo operacional, se comparado aos bancos tradicionais, e com isso, são capazes de oferecer serviços de melhor qualidade em busca de atrair mais clientes e gerar competitividade. Segundo a UBS Evidence Lab, em 2019, a participação dos maiores bancos era de 52% e dos novos, 48%. No ano passado, essa posição se inverteu, com os bancos digitais alcançando uma fatia de 52% (PEREIRA, 2021).

Segundo o IBGE, até o ano de 2018 mais de 34 milhões de brasileiros não possuíam acesso a serviços bancários (CARNEIRO, 2021). Isso se deve a um tipo de exclusão social relacionada a falta de democratização no acesso aos serviços financeiros. Contudo, os serviços financeiros no Brasil têm se revolucionado nos últimos anos com o surgimento dos chamados Bancos Digitais.

A principal vantagem deste tipo de banco é ser livre de taxas operacionais e dispensar a necessidade do cliente ter que se dirigir até uma agência física para abrir uma conta ou ter acesso a determinados serviços, já que os Bancos Digitais não dispõem de uma.

Com a popularização do acesso e uso dos Bancos Digitais (PEREIRA, 2021) têm se percebido uma maior inclusão financeira entre os brasileiros, democratizando o acesso aos serviços bancários por qualquer pessoa independente da renda ou da finalidade de uso da conta. Honohan (2004) acredita que o desenvolvimento da inclusão financeira significa que todos os participantes do sistema econômico têm fácil acesso a recursos financeiros, como depósitos bancários, crédito e seguros. Dahlman *et al.* (2016) apontam que a economia digital promove o crescimento, a produtividade e o desenvolvimento inclusivo.

Atualmente, alcançar a liberdade financeira é tida como uma das tarefas mais difíceis na sociedade, exigindo mudanças de pensamento que possibilitem diferenciar necessidades de

desejos. Segundo Casella (2017), liberdade financeira é o estado em que o indivíduo obtém a liberdade de fazer as suas escolhas na vida sem se preocupar com o dinheiro. No entanto, para atingir esse estado é essencial que seja desenvolvida e aprimorada a educação financeira, assim como a organização das finanças. Assim, os bancos, principais agentes financeiros da sociedade, têm uma clara responsabilidade e um importante papel a desempenhar para promover a adequada conscientização de funcionários e clientes sobre o uso de seus produtos e serviços, a fim de contribuir para uma sociedade mais esclarecida, menos inadimplente e mais saudável financeiramente (OUTEIRO; SANTOS, 2019).

2.4 Avaliação textual

A opinião dos usuários por meio de seus textos vem sendo frequentemente utilizada para avaliar a sua experiência de uso em determinado sistema ou aplicativo. Essa forma de avaliação apresenta bons resultados, tendo em vista a espontaneidade dos usuários ao realizar um comentário a respeito de determinado aplicativo, permitindo assim uma melhor identificação de problemas que em outros tipos de avaliação não seriam facilmente identificados. A partir das postagens realizadas por usuários em sistemas, como lojas de aplicativos e redes sociais, como o *Twitter*, é possível analisar suas opiniões em relação ao uso e através disso servir como base para avaliações voltadas à área de Experiência do Usuário (UX). Mendes (2015) apresenta um modelo e uma metodologia para avaliação da interação com base na linguagem textual do usuário. A MALTU - Modelo para Avaliação da interação em Sistemas Sociais a partir da Linguagem textual do Usuário, é utilizada na avaliação da Usabilidade e Experiência do Usuário (UUX) de sistemas através de um conjunto de Postagens Relacionadas ao Uso (PRUs). Ela engloba cinco etapas: (1) definição do contexto de avaliação; (2) extração de PRUs; (3) classificação das PRUs; (4) interpretação dos resultados e (5) relato dos resultados.

Muitas das vezes, é necessário realizar um processamento do texto para realização destas análises e avaliações, o Processamento de Linguagem Natural (PLN). O PLN é uma área da computação que tem como objetivo extrair representações e significados mais completos de textos livres escritos em linguagem natural (INDURKHYA; DAMERAU, 2010). Segundo Rodrigues (2017), o objetivo do PLN é fornecer aos computadores a capacidade de entender e compor textos. “Entender” um texto significa reconhecer o contexto, fazer análise sintática, semântica, léxica e morfológica, criar resumos, extrair informação, interpretar os sentidos, analisar sentimentos e até aprender conceitos com os textos processados.

De acordo com Scaccia (2022), um texto é uma sequência de palavras, ou de maneira mais granular é uma sequência de caracteres. Ao se trabalhar com texto estamos na verdade trabalhando com um dos tipos de dados sequenciais mais difundidos atualmente, sendo assim necessitamos de modelos específicos que levam em conta essa estrutura sequencial onde a ordem das observações importa.

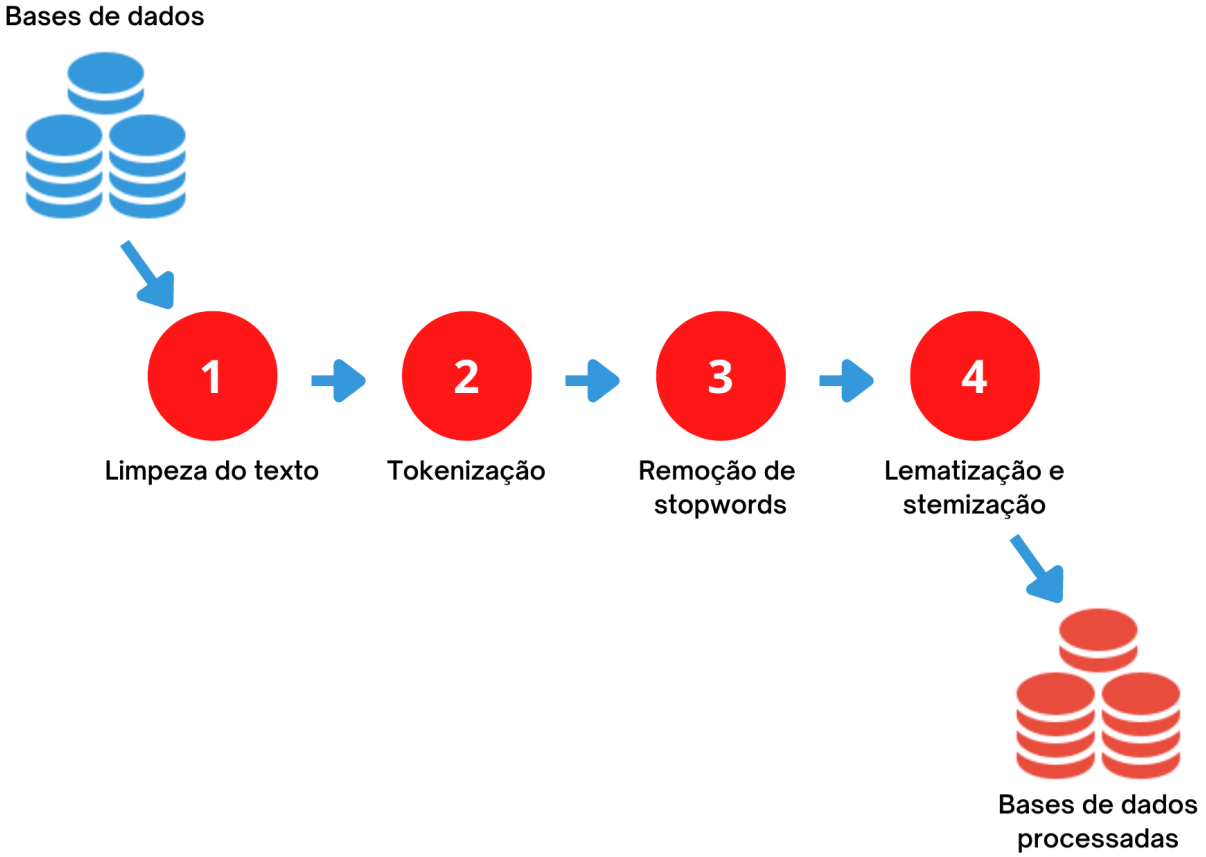
O PLN será utilizado neste trabalho para processar e tratar as postagens dos usuários extraídas das lojas de aplicativos Google Play Store e App Store, e da rede social Twitter. O PNL possui várias etapas para processar um texto, dentre elas etapas de pré-processamento, que serão apresentadas no próximo tópico.

2.4.1 Etapas de pré-processamento do PLN

Um dos principais problemas do PLN é a qualidade dos dados utilizados, principalmente quando se trabalha com textos informais, como os destacados neste trabalho, obtidos de postagens em lojas de aplicativos e redes sociais. Além disso, a escassez de material replicável em português torna bastante difícil a modelagem. Assim sendo, o objetivo do pré-processamento é extrair de textos uma representação estruturada e manipulável por algoritmos de classificação que identifique o subconjunto mais significativo para a coleção de texto (REZENDE *et al.*, 2011), ou seja, obter uma representação com qualidade melhor do que a inicial.

Segundo Pinheiro (2021), para modelar a língua e possibilitar que a máquina a entenda, são necessários pré-processamentos que abstraem e estruturam a língua, deixando apenas o que é informação relevante. Esse pré-processamento reduz o vocabulário e torna os dados menos esparsos, característica conveniente para o processamento computacional, uma vez que os conjuntos de documento de texto são representados por um grande número de características, que podem ser irrelevantes ou redundantes no processo de classificação do texto. A Figura 2 apresenta as etapas realizadas no pré-processamento de textos.

Figura 2 – Etapas de pré-processamento de texto para PLN.



Fonte: elaborado pelo autor (2022).

1. **Limpeza do texto**

   A primeira etapa, considerada a mais importante, é a limpeza do texto. Essa etapa consiste em tratar tudo que pode atrapalhar o processo de modelagem. Segundo Pinheiro (2021), esse pré-processamento reduz o vocabulário e torna os dados menos esparsos, característica conveniente para o processamento computacional, uma vez que os conjuntos de documento de texto são representados por um grande número de características. São realizados os seguintes passos:

   - Conversão do texto em letras minúsculas;
   - Remoção de pontuação e caracteres especiais;
   - Remoção de acentuação das palavras;
   - Remoção de citações;
   - Remoção de número;
   - Remoção de emojis.

2. **Tokenização**

   Também conhecida como segmentação de palavras, a tokenização é um processo que tem

como objetivo separar as palavras ou sentenças em unidades, unidades essas definidas como *tokens*. A tokenização quebra a sequência de caracteres em um texto localizando o limite de cada palavra, ou seja, os pontos onde uma palavra termina e outra começa (PALMER, 2010).

3. **Remoção de *stopwords***

   Stopwords são palavras consideradas irrelevantes para a modelagem e para o entendimento do sentido de um texto, ou seja, palavras irrelevantes semanticamente, como “a”, “e”, “que”, “do”, entre outras. De acordo com Lima e Linhares (2021), a remoção dessas palavras ajuda o código a se concentrar nas principais palavras-chave do texto que adicionam mais contexto.

4. **Lematização e stemização**

   De acordo com lematização e a stemização são processos que tem como objetivo reduzir as palavras para facilitar a abstração do significado das frases. A lematização reduz a palavra ao seu lema, ou seja, a sua forma no masculino e no singular e em caso de verbos reduz ao infinitivo, como por exemplo as palavras “tiver”, “tinha” e “tenho” seriam reduzidas para “ter”. Embora a lematização seja mais lenta em comparação com a stemização, ela considera o contexto da palavra levando em consideração a palavra anterior, o que resulta em melhor precisão (LIMA; LINHARES, 2021). Já a stemização, de acordo com Lima e Linhares (2021) é uma abordagem baseada em regras que converte as palavras em sua palavra raiz (radical) para remover a flexão sem se preocupar com o contexto da palavra na frase.

3 TRABALHOS RELACIONADOS

Nesta seção são apresentados alguns trabalhos que analisam a segurança em aplicativos de instituições financeiras e as relações com a experiência e satisfação dos usuários. Foram realizadas pesquisas e busca de trabalhos que se relacionam com este, bem como conceitos e referências que auxiliam o embasamento teórico do trabalho e a compreensão do cenário no qual está inserido. Como a MALTU não possui um modelo pré-definido para identificação de postagens de segurança, na identificação de trabalhos, pesquisas relacionadas e das próprias postagens foram utilizadas algumas palavras-chave: *security*; *information security banking*; *digital banking*; *mobile banking*; *internet banking*; *security banking*; *banking user reviews*; *ux banking*; *security and ux banking*; *cibersecurity banking*; *textual evaluation banking*; *security problems banking* e *social engineering*. As buscas pelos trabalhos foram realizadas nas bases de artigos científicos ACM *Digital Library*, IEEE e *ResearchGate*.

Conforme os objetivos desta pesquisa, foram tomados como base trabalhos que analisam a experiências dos usuários quanto a sua segurança e de suas informações em aplicativos de instituições financeiras. Foram priorizados trabalhos de anos mais recentes, entre 2008 e 2021, analisando as problemáticas, as metodologias e técnicas aplicadas, as dificuldades encontradas e seus principais resultados. Ao todo foram encontrados 10 trabalhos, porém apenas 5 foram selecionados. Dentre os trabalhos encontrados, oito foram obtidos na ACM, e os outros dois no *ResearchGate* e IEEE. Como critérios de exclusão foram utilizados trabalhos que não possuíam objetivos ligados diretamente a problemas de segurança ou satisfação dos usuários em relação à segurança, como trabalhos que avaliam o desempenho e o desenvolvimento de aplicações. A Tabela 1 apresenta todos os trabalhos encontrados e a Tabela 2 apresenta os que foram selecionados.

Tabela 1 – Trabalhos encontrados na pesquisa.

Citação do trabalho relacionado	Objetivos principais
Albashrawi e Motiwalla (2017)	Compreender a satisfação dos usuários no uso de aplicações de *m-banking* associado à lealdade para com os bancos.
Arisya *et al.* (2020)	Mensurar a conscientização da segurança da informação para usuários de aplicativos de *mobile banking*.
Botacin *et al.* (2019)	Avaliar as implementações atuais das aplicações móveis bancárias brasileiras, com foco na segurança.
Chen *et al.* (2018)	Rastrear e investigar as vulnerabilidades de aplicativos de *mobile banking*.
Shaikh e Karjaluoto (2016)	Analisar a relação entre o uso de aplicações de m-banking com a satisfação geral e a intenção de recomendar o banco.
Zomai *et al.* (2008)	Descrever uma investigação de solução de segurança métodos para autenticação de usuários por meio de canais fora de banda para cada transação.
Blasi *et al.* (2010)	Analisar a aplicabilidade de métricas de segurança para autenticação adaptativa, autorização e confidencialidade de ponta a ponta, e a aplicabilidade de métricas de confiança.
Carminati *et al.* (2018)	Investigar um sistema de apoio à decisão para análise de fraude bancária que avalia a influência no desempenho de detecção de ataques.
Nourallah *et al.* (2019)	Estudar a relação entre confiança e satisfação em aplicativos bancários móveis (MBAs) com base na experiência de jovens clientes bancários (YBCs).
Weerasinghe *et al.* (2010)	Apresentar uma nova estrutura de autenticação e autorização para aplicativos bancários móveis seguros.

Fonte: elaborado pelo autor (2022).

Tabela 2 – Trabalhos selecionados na pesquisa.

Citação do trabalho relacionado	Objetivos principais
Albashrawi e Motiwalla (2017)	Compreender a satisfação dos usuários no uso de aplicações de *m-banking* associado à lealdade para com os bancos.
Arisya *et al.* (2020)	Mensurar a conscientização da segurança da informação para usuários de aplicativos de *mobile banking*.
Botacin *et al.* (2019)	Avaliar as implementações atuais das aplicações móveis bancárias brasileiras, com foco na segurança.
Chen *et al.* (2018)	Rastrear e investigar as vulnerabilidades de aplicativos de *mobile banking*.
Shaikh e Karjaluoto (2016)	Analisar a relação entre o uso de aplicações de m-banking com a satisfação geral e a intenção de recomendar o banco.

Fonte: elaborado pelo autor (2022).

Shaikh e Karjaluoto (2016) examinaram como o uso de aplicações de *m-banking* está relacionado a quatro fatores, sendo estes, compromisso de relacionamento, a satisfação geral, a intenção de recomendar o banco e as futuras intenções de permanecer com o banco. Este estudo, portanto, investigou como experiências reais dos clientes no uso de aplicativos de *m-banking* moldam suas relações com seus bancos. Os autores examinaram os fatores citados anteriormente, e hipotetizaram que a satisfação do usuário com aplicativos de *m-banking* está

positivamente associada ao uso, o que por sua vez afeta positivamente o relacionamento entre o cliente e o banco em termos de compromisso, satisfação geral, intenção de recomendar e intenção de permanecer um cliente do banco. Com isso, os autores organizaram os quatro resultados para os efeitos de sexo, idade, renda e duração da relação bancária. Foi utilizado um painel online de uma empresa de estudos de mercado para coletar dados a partir dos resultados de um instrumento de pesquisa pré-testado. Foi adotado um procedimento em três etapas para desenvolver a validar o questionário de pesquisa. Durante a primeira etapa, as variáveis foram medidas utilizando a escala Likert de sete pontos, variando de 1 (discordo totalmente) a 7 (concordo totalmente). Ao mensurar a intenção de recomendar o banco, foi utilizada a escala *Net Promoter Score* (NPS), que tem como objetivo medir a fidelidade do cliente, variando de 0 (nem um pouco provável) a 10 (muito provável). O uso do sistema foi medido levando em consideração a quantidade de serviços bancários que são conduzidos via *m-banking* (em uma escala de dez pontos variando de 0 a 10 por cento a 100 por cento) e a quantidade de vezes que aplicações de m-banking estavam envolvidas em serviços bancários sem fio, considerando as últimas dez vezes que o usuário estava conectado. Portanto, este estudo mostra a importância da satisfação do usuário e do uso do sistema no fortalecimento do vínculo com o banco. Os resultados deste estudo mostram que o uso do sistema exerce forte influência sobre o comportamento futuro pretendido e o compromisso com o banco, e é portanto, vital para os bancos estabelecerem uma forte conexão com os clientes.

Botacin *et al.* (2019) investigaram como os aspectos técnicos e sociais do *internet banking* atuam juntos para impulsionar o desenvolvimento de tecnologia. Neste estudo os autores revisaram o ecossistema bancário brasileiro, investigando como fatos históricos passados moldaram as decisões de projeto relativas à implementação de serviços bancários, e como as futuras aplicações podem também ser moldadas pelas atuais tendências sócio-culturais. Os autores avaliaram as implementações atuais das aplicações móveis bancárias brasileiras, com foco na segurança, discutindo vulnerabilidades, capacidades e possíveis ameaças futuras. Também discutiram acerca das lições aprendidas com base nas observações, e forneceram diretrizes gerais para auxiliar no desenvolvimento de aplicações mais seguras de *internet banking*. Os autores limitaram o escopo da seleção dos aplicativos à plataforma *Android*, justificando que esta é a plataforma móvel dominante no mercado brasileiro. Eles apresentaram uma visão representativa das vulnerabilidades da maioria dos clientes brasileiros. Na análise também foi incluído o aplicativo principal da Nubank, *fintech* brasileira que lidera o segmento bancário. A inclusão de

um aplicativo desse contexto, permitiu aos autores realizar comparações apoiadas por culturas distintas (bancos tradicionais e fintechs). Os autores utilizaram o guia de teste de segurança móvel OWASP na investigação, e a partir das suas diretrizes selecionaram as categorias de testes mais impactantes, sendo estas (1) Qualidade e configurações de construção do código, (2) Segurança no armazenamento de dados, (3) Comunicação de rede, (4) Resiliência contra engenharia reversa e (5) Autenticação local. A partir desta análise, os autores descobriram 1) que os bancos migraram para o ambiente móvel antes de aprender suas principais características e particularidades. 2) que todos os aplicativos de bancos implementam uma tecnologia para reconhecimento de caracteres a partir de um arquivo de imagem chamada Reconhecimento Óptico de Caracteres (OCR), do inglês *Optimal Character Recognition*, incorrendo na inclusão de bibliotecas nativas como parte da base de códigos da aplicação. Dessa forma, comparando-se ao Nubank, que funciona completamente de forma digital, sem o uso de bibliotecas nativas e nem OCR, foi observada uma redução significativa na superfície de ataques e dependências de códigos de terceiros. Com isso, os autores identificaram algumas diretrizes as quais os bancos devem seguir para garantir o desenvolvimento seguro de seus aplicativos, como reduzir a heterogeneidade, tendo em vista a diversidade de aplicativos disponíveis no âmbito bancário brasileiro; evitar armazenamento de dados confidenciais localmente; evitar terceirização de manutenção de serviços de segurança; utilizar certificados de segurança; e melhorar a regulamentação.

Albashrawi e Motiwalla (2017) combinaram dois modelos de aceitação de sistemas de informação para fornecer uma compreensão mais profunda acerca da satisfação dos usuários no uso de aplicações de m-banking: o modelo de sucesso de sistemas de informação (*IS success model*), que foca na qualidade do sistema, do serviço e da informação; e a teoria unificada de aceitação e uso da tecnologia (UTAUT), que foca na expectativa de desempenho, influência social e condições facilitadoras. Combinados, estes modelos fornecem uma ampla estrutura para compreensão do uso de *m-banking*, e para o uso do sistema. Em complemento, os autores adicionaram o fator de lealdade no modelo de pesquisa, para determinar de que forma a satisfação e uso do *m-banking* afeta a lealdade do usuário para com os bancos, fator que pode auxiliar na retenção de clientes. Foi realizada uma pesquisa de campo de forma online para testar suas hipóteses, com auxílio do banco, e também foram analisados dados de usuários de *m-banking* extraídos dos arquivos de log do banco. A amostra dos autores consistiu de 1165 usuários, dos quais 760 são usuários de *m-banking*, e destes 760 foram obtidos 472 respondentes válidos, combinados com os usuários dos arquivos de log. O gênero dos respondentes foi bem

equilibrado, e a idade pertencia à população idosa. Em relação ao trabalho e educação, a maioria dos respondentes eram alfabetizados e empregados em tempo integral. Os autores chegaram à conclusão que a integração dos dois modelos foi responsável por 73,3% da satisfação dos usuários, superando os modelos aplicados de forma individual. Com isso, comprovaram que a satisfação do usuário é um importante antecedente para a lealdade, e portanto, reflete o aumento da retenção de clientes.

Arisya *et al.* (2020) conduziram um estudo para medir a conscientização da segurança da informação para usuários de aplicativos de *mobile banking* utilizando o modelo *Knowledge-Attitude-Behavior* (KAB), ou Conhecimento-Atitude-Comportamento, que considera estas três dimensões como base para medir a consciência da informação. Conhecimento é definido como o que uma pessoa sabe ou entende; atitude é definido como o que uma pessoa sente ou pensa; e comportamento é definido como uma ação realizada. Baseado nestas três dimensões, os autores dividiram várias áreas de foco desenvolvidas na pesquisa de Parsons et al. (2014), que consistem em sete variáveis: gerenciamento de senha, uso de e-mail, uso da internet, uso de redes sociais, dispositivo móvel, tratamento de informações e informações de relatórios de incidentes, conhecidos como Aspectos Humanos da Segurança da Informação (HAIS-Q), do inglês *Human Aspects of Information Security*. Os autores realizaram um questionário aplicado enquanto os entrevistados utilizavam a aplicação de mobile banking, contendo perguntas a respeito de conhecimento, compreensão e comportamento utilizando a escala de Likert. Ao todo foram 51 perguntas relacionadas ao modelo KAB, aplicado às sete variáveis das áreas de foco do HAIS-Q, juntamente com quatro perguntas acerca das características dos entrevistados. No processamento dos dados foi utilizado um processo analítico, que cria uma estrutura começando com o primeiro objetivo e pondera cada variável das áreas de foco da conscientização da segurança da informação. Os resultados mostraram que o nível de conhecimento dos usuários de aplicações de *mobile banking* acerca da segurança da informação em termos das dimensões e áreas de foco mostraram um valor de 83,32%, que foi incluído na categoria de satisfatório. Apesar disso, várias outras áreas demonstraram resultados medianos e foram recomendadas ações como melhorias da sensibilização dos usuários para com a segurança da informação, melhorias de segurança nos aplicativos, condução de treinamentos, e melhorias de comunicação.

Chen *et al.* (2018) realizaram um estudo para rastrear e investigar as vulnerabilidades de aplicativos de *mobile banking* e compreender o status de segurança atual deles. Primeiramente, os autores investigaram e coletaram durante seis meses as principais vulnerabilidades de cerca

de 693 aplicativos de *mobile banking* utilizando uma ferramenta automatizada de avaliação de riscos de segurança (AUSERA), que emprega duas estratégias de detecção de vulnerabilidades em aplicativos de *mobile banking*: uma análise de dados para determinar se existem fluxos inseguros de informações confidenciais e uma verificação de comunicações seguras em termos de infraestrutura de APIs. Com as vulnerabilidades coletadas, os autores as enviaram para as entidades bancárias e marcaram reuniões para discussão, além de realizarem uma pesquisa com desenvolvedores de aplicativos sobre suas considerações de segurança e compreensão das vulnerabilidades. Os autores compilaram os *feedbacks* das entidades e dos desenvolvedores, analisaram os problemas de segurança relatados, e forneceram algumas recomendações para bancos, entidades, pesquisadores e desenvolvedores de políticas sobre como corrigir estes problemas. Os resultados da pesquisa mostraram que as entidades bancárias devem melhorar o fornecimento de canais para respostas à vulnerabilidades, principalmente para pesquisadores que se concentram nesse tópico de estudo; escolher cuidadosamente as bibliotecas de terceiros a serem utilizadas; dar mais ênfase à questões de segurança ao invés de apenas bugs funcionais; e utilizar ferramentas de empacotamento de aplicativos, considerado um dos métodos mais eficazes para proteção de aplicativos.

Embora os autores tenham utilizado formas de avaliação do uso de aplicações de instituições financeiras, bem como aspectos de satisfação, conscientização acerca da segurança da informação e vulnerabilidades das aplicações, não houve nenhum relato, investigação ou avaliação voltada à segurança da informação no contexto de uso das aplicações.

A Tabela 3 apresenta um comparativo entre este trabalho e os trabalhos relacionados, utilizando os seguintes critérios: 1) objetivos principais, que apresenta os propósitos principais da pesquisa; 2) metodologia, que apresenta a metodologia utilizada na execução da pesquisa; 3) participação de usuários, que apresenta se houve ou não participação de usuários na execução da pesquisa; 4) análise de aplicativos bancários, que apresenta se foi feita ou não uma análise de aplicativos bancários durante a pesquisa; 5) opinião dos usuários, que apresenta se foi considerada ou não a opinião dos usuários durante a pesquisa; 6) implementou algoritmo, que apresenta se foi implementado ou não algum algoritmo; e 7) critérios avaliados em cada trabalho, incluindo este.

Tabela 3 – Diferenças entre este trabalho e os trabalhos relacionados.

Citação do trabalho relacionado	Objetivos principais	Metodologia	Teve a participação de usuários?	Fez uma análise de aplicativos bancários?	Considerou a opinião dos usuários?	Implementou algoritmo?	Critério(s) avaliado(s)
Albashrawi e Motiwalla (2017)	Compreender a satisfação dos usuários no uso de aplicações de *m-banking* associado à lealdade para com os bancos.	Questionário e combinação dos modelos de aceitação *IS success* e UTAUT	Sim	Não	Não	Não	Usabilidade
Arisya *et al.* (2020)	Mensurar a conscientização da segurança da informação para usuários de aplicativos de *mobile banking*.	Questionário e modelo *Knowledge-Attitude-Behavior* (KAB)	Sim	Não	Sim	Não	Usabilidade
Botacin *et al.* (2019)	Avaliar as implementações atuais das aplicações móveis bancárias brasileiras, com foco na segurança.	Guia de teste de segurança móvel OWASP	Não	Sim	Não	Não	-
Chen *et al.* (2018)	Rastrear e investigar as vulnerabilidades de aplicativos de *mobile banking*.	Questionário e ferramenta automatizada de avaliação de riscos de segurança (AUSERA)	Não	Sim	Não	Não	-
Shaikh e Karjaluoto (2016)	Analisar a relação entre o uso de aplicações de *m-banking* com a satisfação geral e a intenção de recomendar o banco.	Questionário de pesquisa	Sim	Sim	Sim	Não	Usabilidade
Este trabalho	Analisar a experiência dos usuários quanto a sua segurança em aplicativos de *mobile banking*.	Avaliação textual	Sim	Sim	Sim	Sim	Segurança da Informação

Fonte: elaborado pelo autor (2022).

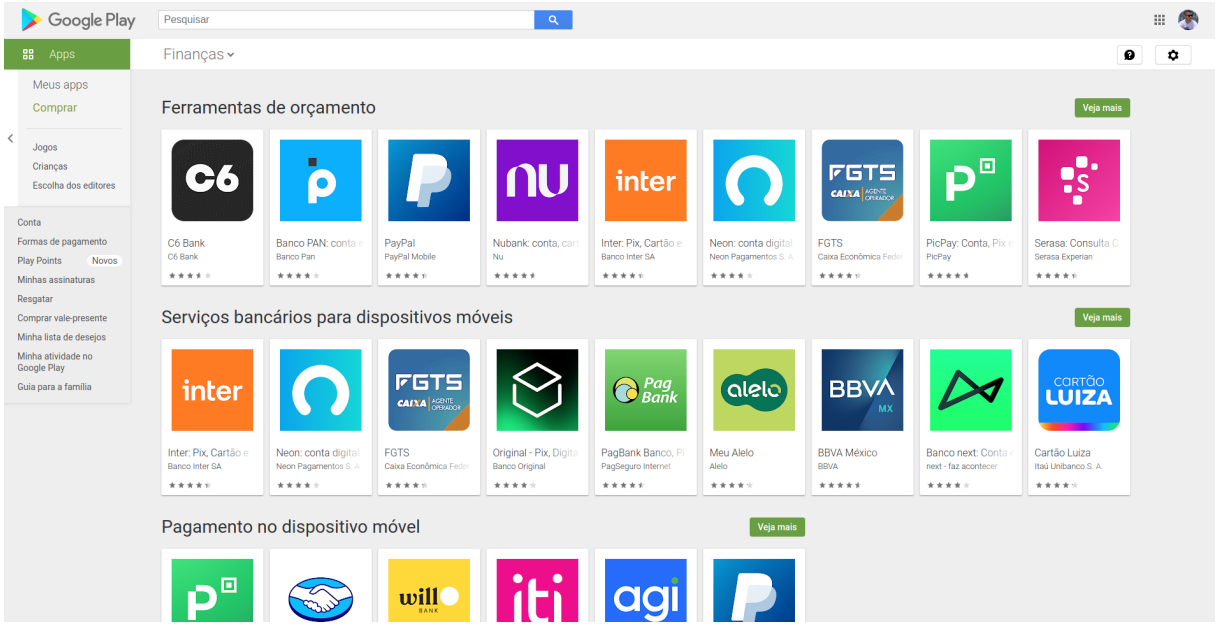
4 INVESTIGAÇÃO: CAIXA ECONÔMICA FEDERAL E NUBANK

Nesta seção é relatada a investigação realizada nesses dois aplicativos de instituições financeiras.

4.1 Processo de seleção dos aplicativos para investigação

Nesta etapa, foi realizada uma busca por aplicativos de mobile banking na *Google Play Store*, filtrada através da categoria "Finanças", e da subcategoria "Serviços bancários para dispositivos móveis", como mostra a Figura 3. A escolha de aplicativos utilizados na plataforma Android, consequentemente disponibilizados na *Google Play Store*, foi definida dado que atualmente este é o sistema operacional mais utilizado no mundo (ZURIARRAIN, 2017). Segundo Kleina (2022), o *Android* 11 está presente em quase um quarto dos smartphones, mas o *Android* 10 (lançado em 2019) ainda é o sistema operacional mais usado (ALMENARA, 2021).

Figura 3 – Categoria de aplicativos "Finanças" na *Google Play Store*.

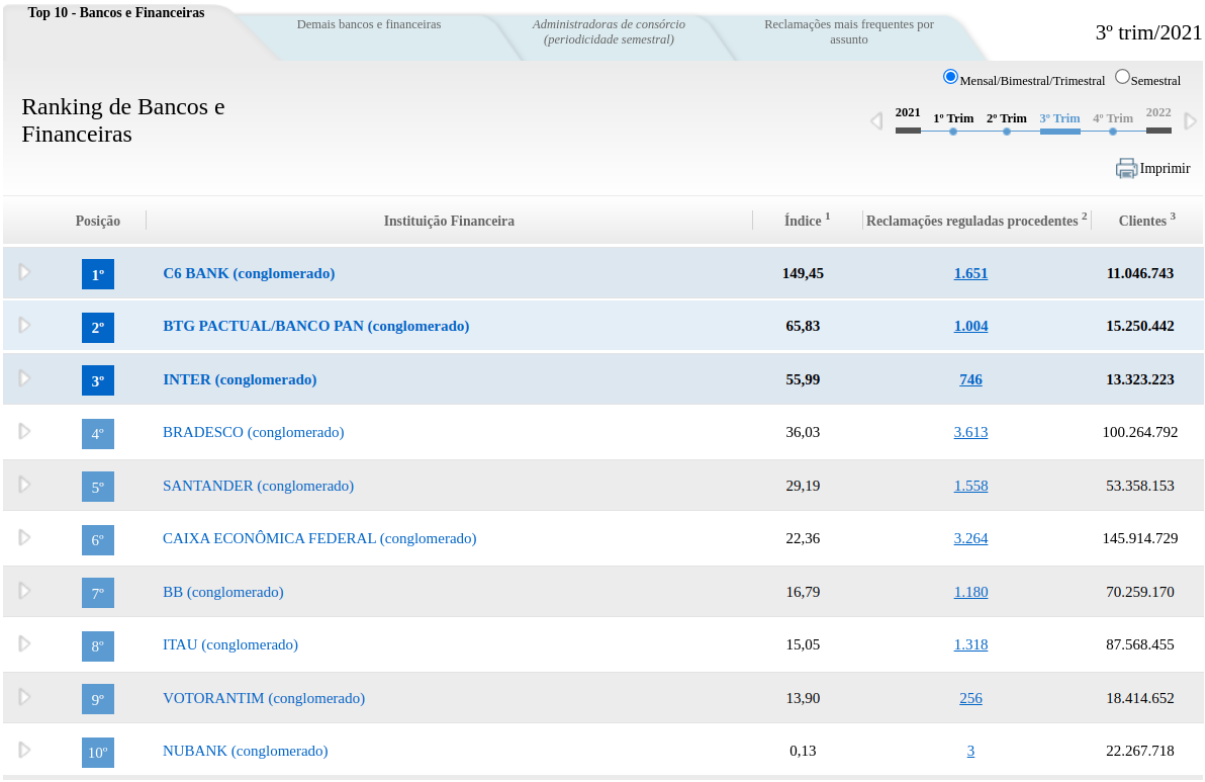


Fonte: adaptado de Google Play Store (2022).

Desta forma, foram definidos os aplicativos de instituições financeiras utilizados no trabalho. Para tanto foi consultado um ranking disponibilizado no site do Banco Central do Brasil (BACEN), denominado "Ranking de Reclamações" (Figura 4). Este ranking é divulgado com periodicidade trimestral, sendo apresentado em duas listagens: (1) os 10 maiores Bancos e Financeiras em número de clientes; e (2) demais Bancos e Financeiras. A partir da primeira listagem, consultada no último trimestre de 2021, foram obtidos 10 Bancos e Financeiras para

análise. Com base nessa lista, foi realizada uma pesquisa na *Google Play Store*, em busca dos aplicativos de cada banco listado.

Figura 4 – Ranking de Reclamações do BACEN.



Top 10 - Bancos e Financeiras | Demais bancos e financeiras | Administradoras de consórcio (periodicidade semestral) | Reclamações mais frequentes por assunto | 3º trim/2021

Ranking de Bancos e Financeiras

Mensal/Bimestral/Trimestral | Semestral

2021 | 1º Trim | 2º Trim | 3º Trim | 4º Trim | 2022

Imprimir

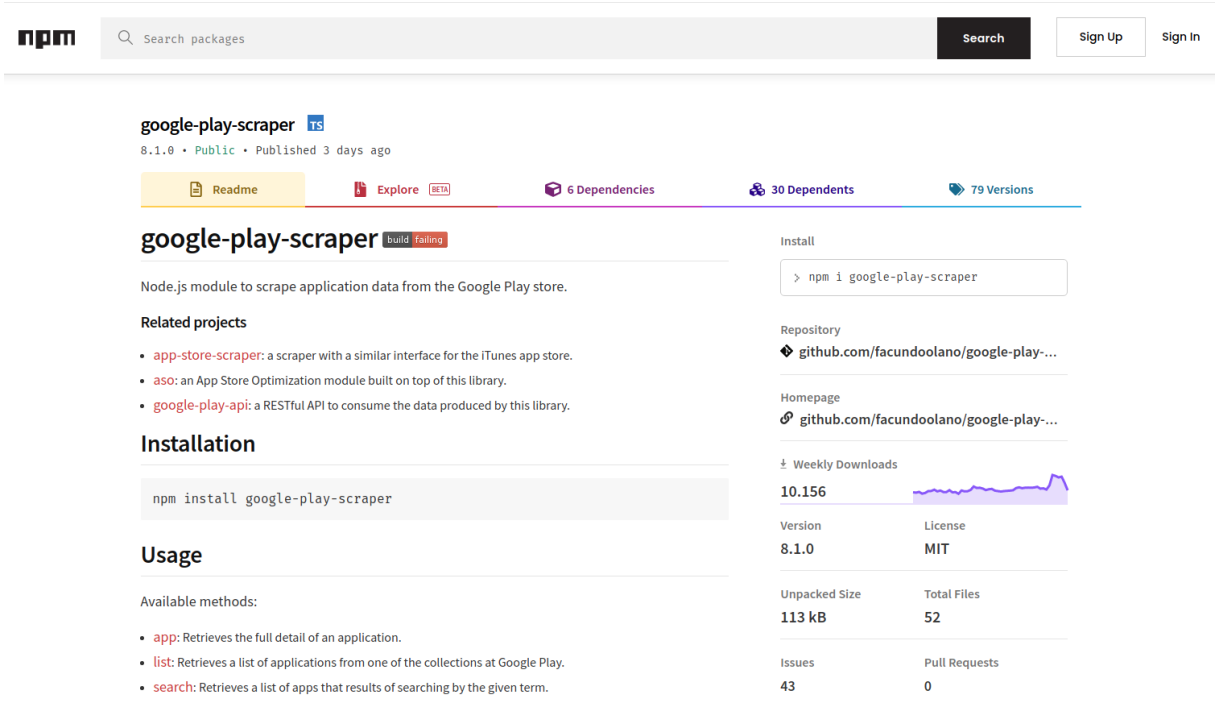
Posição	Instituição Financeira	Índice [1]	Reclamações reguladas procedentes [2]	Clientes [3]
1º	C6 BANK (conglomerado)	149,45	1.651	11.046.743
2º	BTG PACTUAL/BANCO PAN (conglomerado)	65,83	1.004	15.250.442
3º	INTER (conglomerado)	55,99	746	13.323.223
4º	BRADESCO (conglomerado)	36,03	3.613	100.264.792
5º	SANTANDER (conglomerado)	29,19	1.558	53.358.153
6º	CAIXA ECONÔMICA FEDERAL (conglomerado)	22,36	3.264	145.914.729
7º	BB (conglomerado)	16,79	1.180	70.259.170
8º	ITAU (conglomerado)	15,05	1.318	87.568.455
9º	VOTORANTIM (conglomerado)	13,90	256	18.414.652
10º	NUBANK (conglomerado)	0,13	3	22.267.718

Fonte: adaptado de Banco Central Do Brasil (2021).

A partir dessa pesquisa, foi elaborada uma tabela (Tabela 4) contendo dados que foram utilizados na definição destes aplicativos para estudo, sendo estes (1) quantidade de *downloads*; (2) quantidade de classificações por estrela; (3) quantidade de avaliações textuais; (4) quantidade de clientes; e (5) quantidade de reclamações no BACEN.

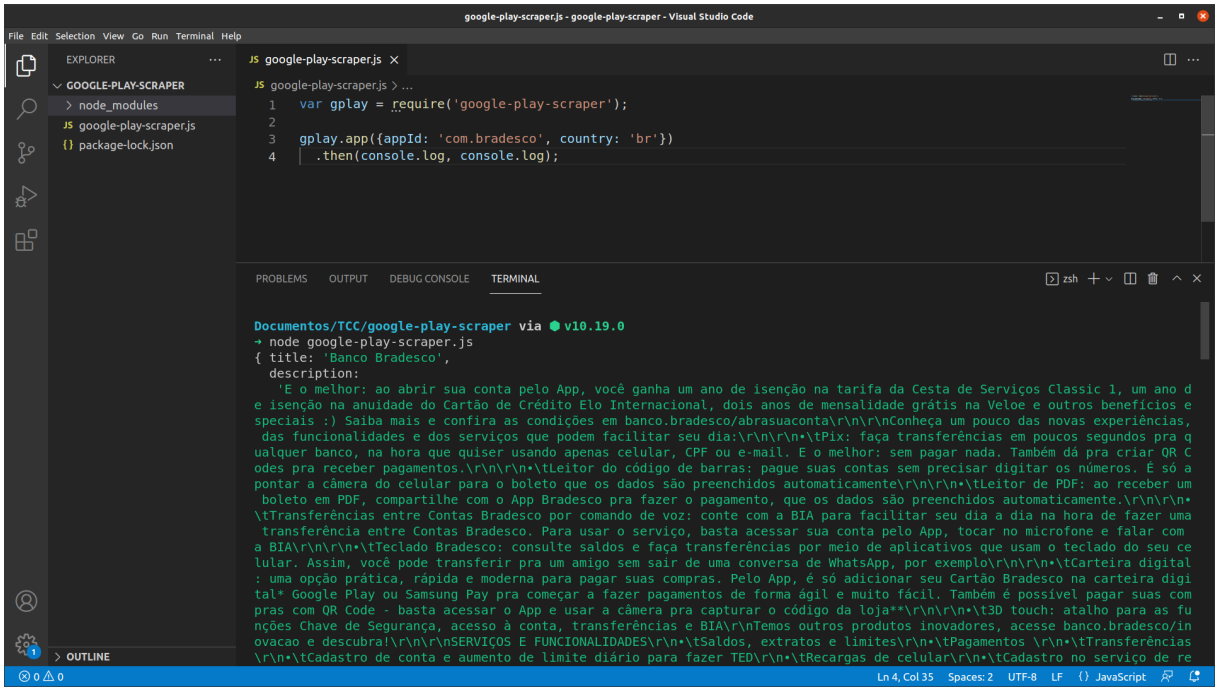
Os dados referentes à (1) quantidade de *downloads*, (2) quantidade de classificações e (3) quantidade de avaliações foram obtidos através do desenvolvimento de um programa em *Node.js* (Figura 6), realizado pelo autor deste trabalho, utilizando um módulo para extração de dados de aplicativos da *Google Play Store* disponível no repositório de pacotes do *Node Package Manager* (NPM), como mostra a Figura 5.

Figura 5 – Módulo *Node.js* para extração de dados de aplicativos da *Google Play Store*.



Fonte: adaptado de Banco Central Do Brasil (2021).

Figura 6 – Programa em *Node.js* utilizando módulo para extração de dados de aplicativos.



Fonte: elaborado pelo autor (2022).

Tabela 4 – Dados utilizados na definição dos aplicativos para estudo.

Instituição Financeira	Tipo de banco	Quantidade de *downloads*	Quantidade de classificações por estrela	Quantidade de avaliações textuais	Quantidade de clientes (*)	Quantidade de reclamações no BACEN
Banco do Brasil	Tradicional	73.521.112	4.524.326	1.361.274	69.010.996[(1)]	5.829
Bradesco	Tradicional	72.708.522	2.331.252	1.035.108	99.260.817[(1)]	10.693
BTG Pactual / Banco PAN	Tradicional	3.318.664	31.944	14.706	12.576.773[(1)]	3.061
Caixa Econômica Federal	Tradicional	125.983.253	2.968.755	1.447.968	145.684.233[(1)]	11.872
C6 Bank	Digital	20.896.295	335.836	173.740	11.046.743[(1)]	3.825
Inter	Digital	29.972.671	1.078.449	334.386	11.467.628[(1)]	1.776
Itaú	Tradicional	58.350.337	2.087.578	820.641	85.710.724[(1)]	6.850
Nubank	Digital	77.437.260	1.179.076	438.441	22.267.718[(1)]	38
Santander	Tradicional	52.382.128	2.473.340	876.691	52.415.407[(1)]	7.235
Votorantim	Tradicional	5.966.594	141.524	70.716	16.774.345[(1)]	674

Fonte: elaborado pelo autor (2022) e (1) adaptado de Banco Central Do Brasil (2021)
Nota: (*) Dados obtidos até o 3º trimestre de 2021.

Com base nos dados obtidos referentes aos aplicativos (Tabela 4), os bancos foram divididos de acordo com o seu tipo (tradicional ou digital), e foi analisado qual deles possui o maior valor em cada critério estabelecido. O Quadro 1 mostra qual o banco foi selecionado em cada critério.

Quadro 1 – Bancos selecionados em cada critério estabelecido.

Critério	**Banco tradicional**	**Banco digital**
Quantidade de downloads	Caixa Econômica Federal	Nubank
Quantidade de classificações por estrela	Banco do Brasil	Nubank
Quantidade de avaliações textuais	Caixa Econômica Federal	Nubank
Quantidade de clientes	Caixa Econômica Federal	Nubank
Quantidade de reclamações no BACEN	Caixa Econômica Federal	C6 Bank

Fonte: elaborado pelo autor (2022).

Com base no Quadro 1, os bancos Caixa Econômica Federal e Nubank aparecem com maior frequência em relação aos demais, sendo portanto as instituições selecionadas para ter o seu aplicativo de *mobile banking* explorado neste estudo.

4.2 Extração das postagens

A extração das postagens foi realizada através de um processo automatizado, utilizando como fontes as lojas de aplicativo *Google Play Store* e *App Store*, e a rede social *Twitter*. As lojas de aplicativos possibilitam formas dos usuários realizarem avaliações e classificações acerca dos aplicativos, e estas avaliações se tornam úteis para outros usuários, pesquisadores, desenvolvedores, proprietários, entre outros. Com base nestas avaliações e classificações os usuários podem escolher os melhores aplicativos, desenvolvedores podem obter *feedbacks* acerca das funcionalidades, e os proprietários das lojas podem identificar aplicativos ruins e mal intencionados. O *Twitter* atualmente é uma das redes sociais que mais se destaca, pelo fato de ser um meio de comunicação em que os usuários podem postar em sua *timeline* sobre qualquer assunto, limitados a 140 caracteres por postagem, o que proporciona conteúdos menores e mais claros, assim como uma maior absorção e compreensão, tendo em vista que a leitura é facilitada.

Os usuários utilizam as páginas dos aplicativos de instituições financeiras e redes sociais para se relacionar com o seu banco de forma mais rápida e prática. Buscam tirar dúvidas sobre funcionalidades, relatam problemas que estão enfrentando, solicitam apoio na realização de determinados serviços, tudo isso pelas postagens. Segundo CAVALCANTI (2013), empresas de todos os portes possuem presença em redes sociais, cujo objetivo é conseguir um relacionamento mais próximo com o cliente.

4.2.1 Extração de postagens de lojas de aplicativos

Foi realizada uma busca por ferramentas ou módulos que possibilitassem o acesso e extração das postagens nas lojas de aplicativos *Google Play Store* e *App Store*. Como resultado desta busca, foram encontrados dois módulos do NPM, o *google-play-scraper* e o *app-store-scraper*. Estes módulos fornecem um mecanismo para extração de dados de aplicativos da *Google Play Store* e da *App Store*, respectivamente.

Para a extração das postagens das lojas de aplicativos foram desenvolvidas duas *Application Programming Interface* (API) em *Node.js*, uma para extração de postagens dos aplicativos da *Google Play Store*, que utiliza o módulo *google-play-scraper*, e outra para extração de postagens dos aplicativos da *App Store*, que utiliza o módulo *app-store-scraper*.

Os módulos possuem métodos para determinadas finalidades, seja para obter detalhes do aplicativo, buscar um determinado aplicativo através de um termo, recuperar uma lista de aplicativos similares, obter avaliações de um aplicativo específico, entre outras. Para a extração das postagens das lojas de aplicativos utilizadas neste trabalho, foi utilizado o método *review* em ambos os módulos. Este método recupera uma página de avaliações (postagens) referentes a um aplicativo específico.

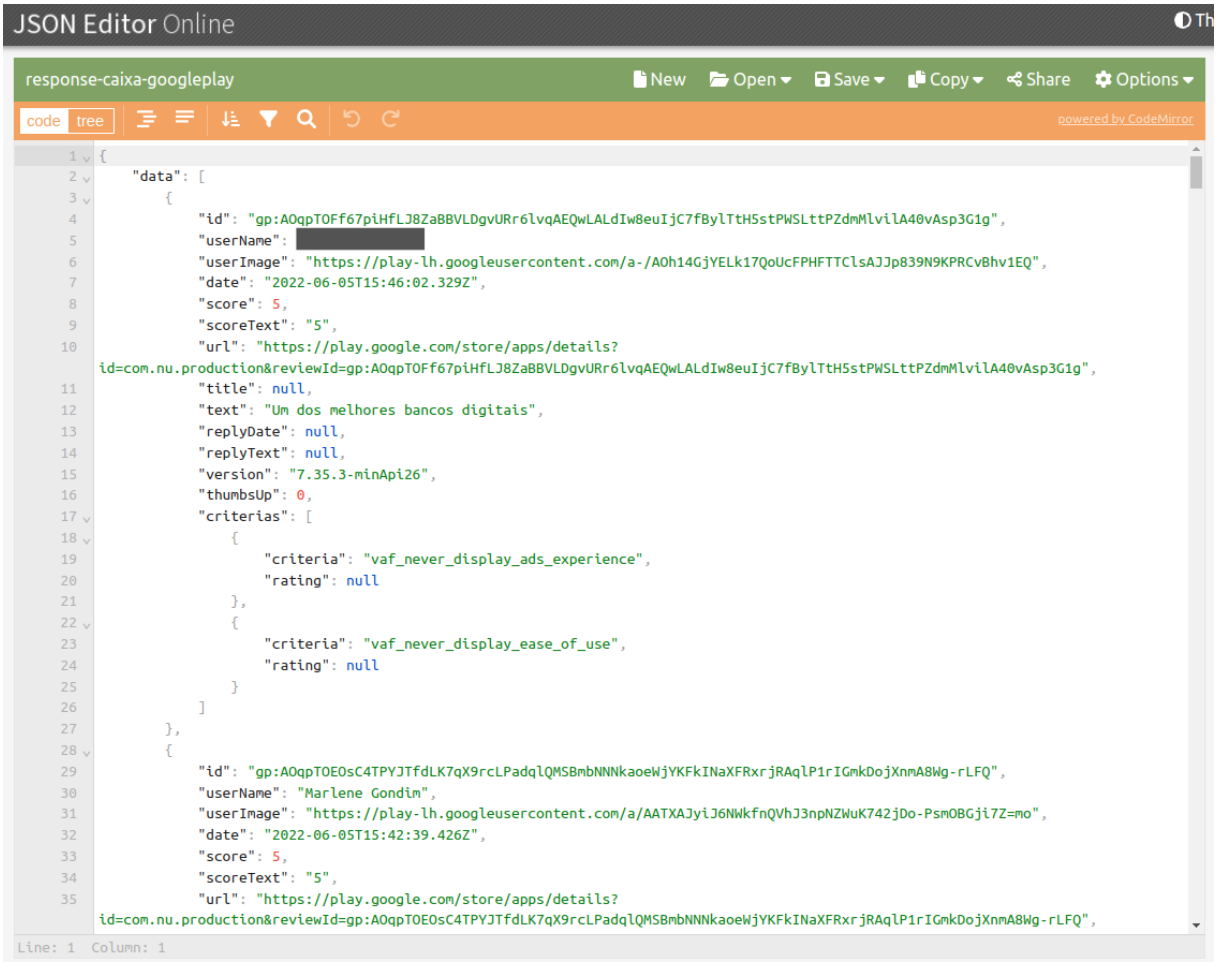
Para utilizá-lo no *google-play-scraper* é necessário passar como parâmetros o *num*, que corresponde à quantidade de avaliações a serem extraídas e o *appId*, que corresponde ao identificador exclusivo do aplicativo na *Google Play Store*, localizado na *Uniform Resource Locator* (URL) da página do aplicativo. Além destes parâmetros também são passados o *lang*, que corresponde ao idioma das avaliações buscadas; o *country*, que corresponde ao código do país para busca das avaliações; e o *sort*, que corresponde a forma como as avaliações serão classificadas, neste caso, através das mais recentes.

Já para utilizá-lo no *app-store-scraper* é necessário passar como parâmetros o *id*, que corresponde ao identificador exclusivo do aplicativo na *App Store*, localizado na URL da página do aplicativo e a *page*, que corresponde ao número da página de avaliação a ser recuperada, limitando-se a 10. Além destes parâmetros também são passados o *country*, que corresponde ao código do país para busca das avaliações; e o *sort*, que corresponde a forma como as avaliações serão classificadas, neste caso, através das mais recentes.

As APIs são responsáveis por receber estes parâmetros como entrada, em forma de *query params*, que são parâmetros ou *strings* de consulta definidos como pares de chave-valor que aparecem após o ponto de interrogação na URL. Segundo Rocha (2021), uma *string* de

consulta pode ser utilizada para diversas finalidades, porém um dos principais usos é manipular consultas do tipo *GET* que retornam uma lista de dados. Ao receber estes parâmetros os módulos são acionados, e é realizada a extração das postagens. O formato de saída das APIs é um *JavaScript Object Notation* (JSON), que possui as avaliações dos usuários acerca dos aplicativos, bem como as datas das postagens. O JSON é uma forma de notação de objetos *JavaScript* de modo que eles possam ser representados de uma forma comum a diversas linguagens Leite (2020). A Figura 7 mostra um exemplo de postagens extraídas do aplicativo Nubank na *Google Play Store* em formato JSON.

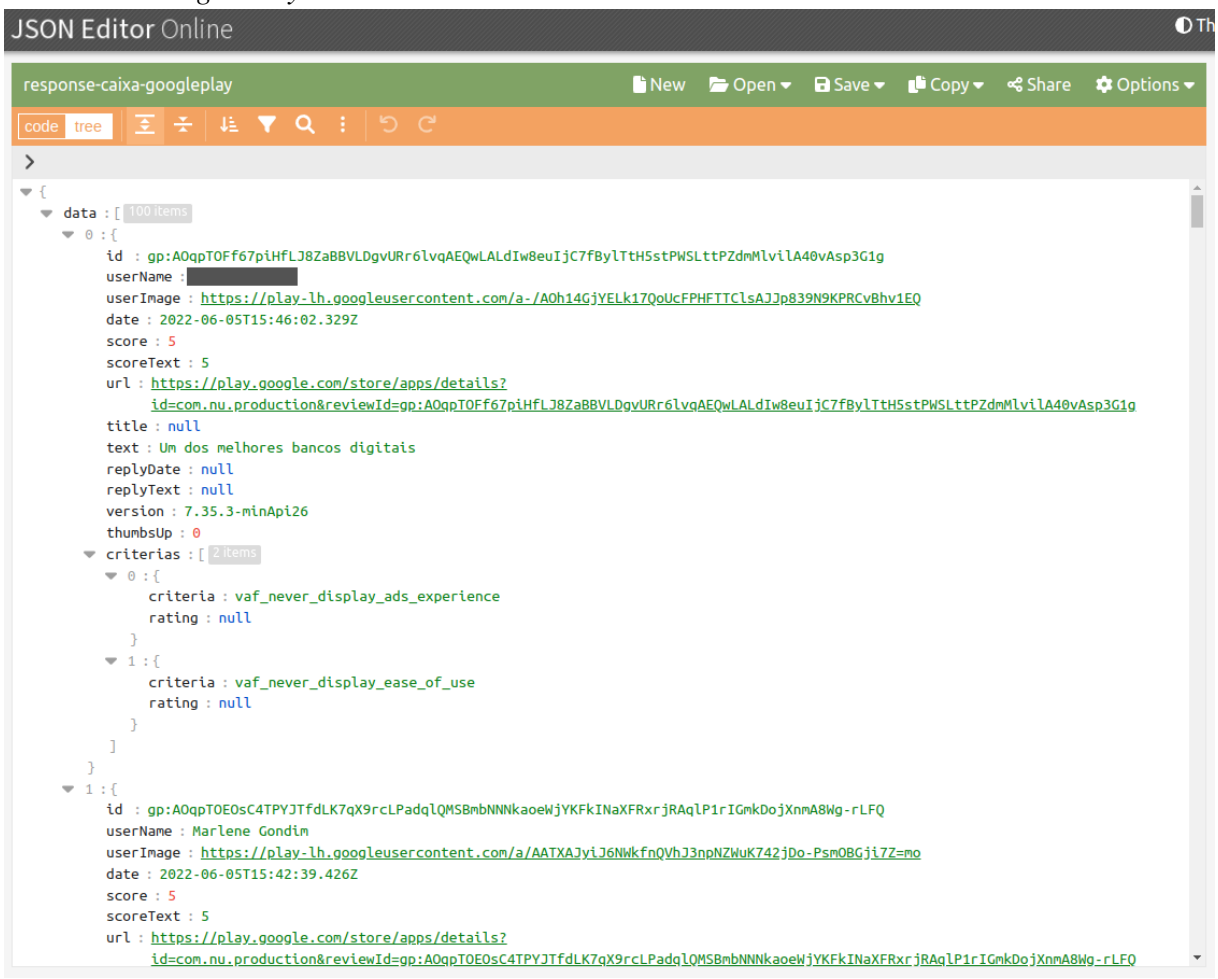
Figura 7 – Postagens extraídas do aplicativo Nubank na *Google Play Store* em formato JSON.



Fonte: elaborado pelo autor (2022).

Para melhor visualização, a Figura 8 apresenta uma exibição em itens. Em ambos formatos de visualização foi utilizada a plataforma JSON Editor Online.

Figura 8 – JSON em modo de exibição em itens de postagens extraídas do aplicativo Nubank na *Google Play Store*.



Fonte: elaborado pelo autor (2022).

4.2.2 Extração de postagens do Twitter

Inicialmente foi realizada uma busca por ferramentas que possibilitassem o acesso e extração das postagens no *Twitter*. Como resultado desta busca, foi encontrada uma API do próprio *Twitter* que permite acesso à recursos da rede social como *tweets*, mensagens diretas, listas e usuários de maneira exclusiva.

Para utilização desta API é necessário possuir uma conta ativa no *Twitter*, para ter acesso ao portal do desenvolvedor. O autor deste trabalho utilizou sua própria conta pessoal para tal acesso.

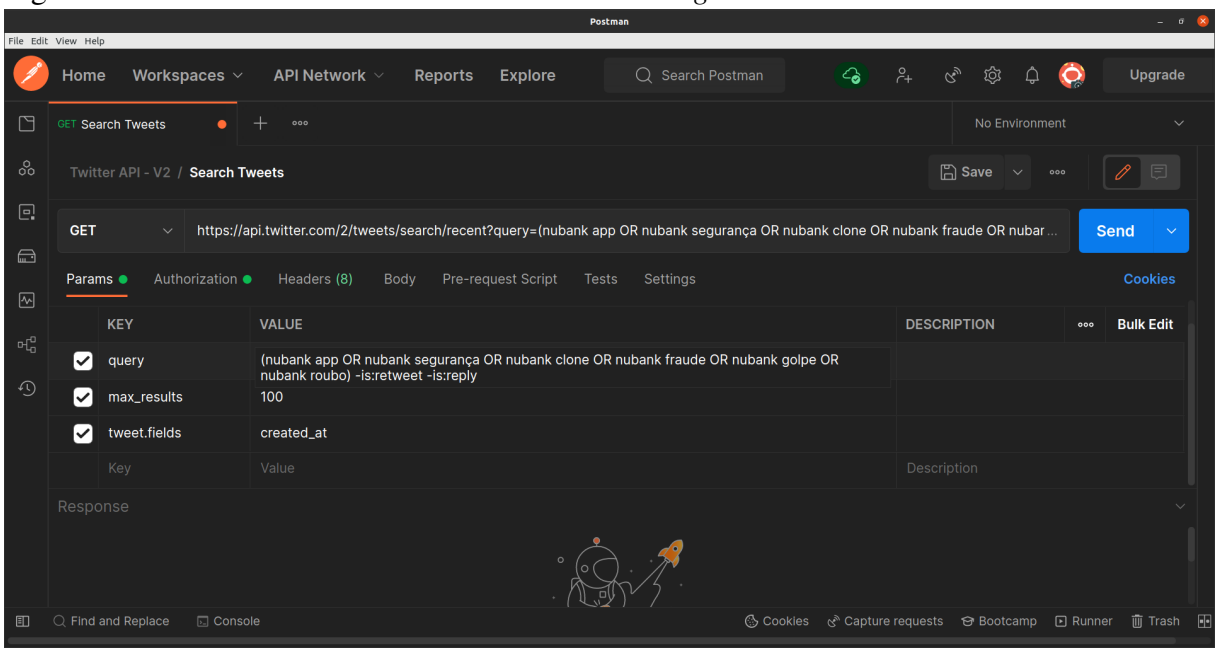
A API possui níveis de acesso, de acordo com a necessidade e a finalidade do uso por parte do desenvolvedor. O autor descreveu a finalidade da utilização da API, relatando que é voltada à pesquisa, informando o tema deste trabalho, e os principais objetivos de uso da API para contribuição com o trabalho, sendo estes realizar uma busca por *tweets* relacionados a páginas

bancárias e aplicativos bancários e, por meio dos textos presentes nesses *tweets*, identificar problemas relacionados à segurança. Esse processo foi iniciado através de um formulário presente no portal do desenvolvedor para solicitação de nível de acesso elevado, e continuou via e-mail após serem necessárias mais informações sobre o trabalho. Este nível permite acesso elevado a recursos da API, tais como buscas avançadas, múltiplos ambientes de aplicativos por projeto, e capacidade de recuperar até 2 milhões de *tweets* por mês.

Com o acesso foi criado um projeto, no portal do desenvolvedor, para buscar e extrair os *tweets*. A criação deste projeto é necessária pois através dele são obtidas as chaves e *tokens* de acesso aos recursos da API. Esse portal fornece um guia de referência para utilização dos recursos da API, logo, como a principal finalidade é buscar e extrair postagens dos *Twitter* relacionadas a aplicativos bancários, especificamente das instituições financeiras Caixa e Nubank, foi utilizado o recurso de busca por *tweets*.

Esse recurso permite buscar e obter os *tweets* mais recentes, dos últimos sete dias, com um limite máximo de 100 *tweets* por chamada à API. São utilizadas *string* de busca como parâmetro para realizar a consulta, associadas aos operadores de pesquisa *AND* e *OR*. As strings de busca utilizadas combinaram o nome do banco em questão (Caixa ou Nubank), juntamente com os termos segurança, app, clone, fraude, golpe e roubo. A escolha dos termos se deu através de uma busca manual por postagens do *Twitter*, na qual o autor identificou que dentre as postagens voltadas à segurança, estas eram as palavras mais mencionadas. Além das strings de busca e dos operadores de pesquisa, são definidos parâmetros de restrição para extração das postagens, ignorando casos de *retweets* e respostas a outros *tweets*. Na Figura 9 é exemplificada a chamada à API do *Twitter*, utilizando os parâmetros *query*, que contém a *string* de busca; e o parâmetro *max_results*, que corresponde à quantidade máxima de resultados que pode ser obtida.

Figura 9 – Chamada à API do *Twitter* utilizando *string* de busca.



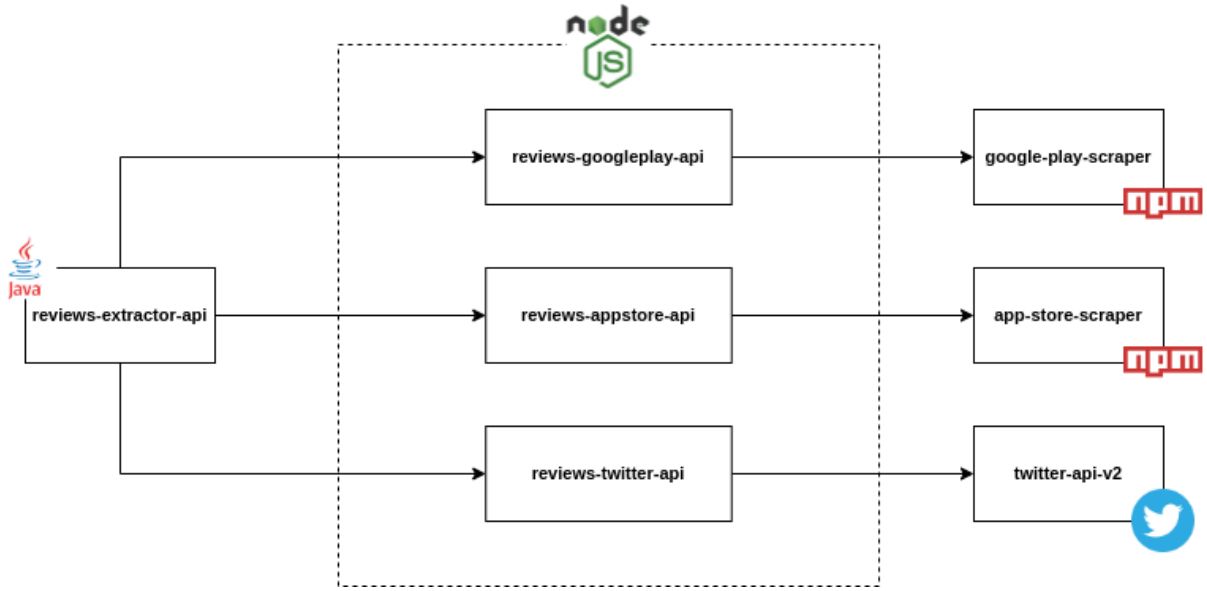
Fonte: elaborado pelo autor (2022).

O parâmetro *tweet.fields* é responsável por definir quais dados, além do próprio texto e *id* do *tweet*, virão na resposta da API. Neste caso, além do tweet, foi extraída também a data referente à sua criação.

4.2.3 Aplicação para centralizar extrações de postagens

Com o propósito de centralizar todas as chamadas às APIs de extração, foi desenvolvida uma aplicação *Java* que é responsável por expor todos os recursos de busca e extração, através de integrações com as APIs da *Google Play Store*, *App Store* e *Twitter*. Esta aplicação foi desenvolvida utilizando *Spring Boot*, um *framework Java* que torna fácil a criação de aplicações *Spring* auto suficientes e robustas, possibilitando a execução imediata (LIMA, 2021). Além de realizar a integração com as outras APIs, esta aplicação tratou da padronização das respostas obtidas, considerando apenas os textos e as datas das postagens extraídas. A Figura 10 apresenta um diagrama arquitetural especificando a forma de comunicação entre a aplicação, as APIs e seus módulos.

Figura 10 – Diagrama arquitetural dos componentes para extração das postagens.



Fonte: elaborado pelo autor (2022).

O diagrama foi planejado pelo autor deste trabalho baseando-se na arquitetura de microsserviços, um tipo de arquitetura de *software* que consiste em construir aplicações desmembrando-as em serviços independentes que se comunicam entre si usando APIs e promovem grande agilidade em times de desenvolvimento (KANCZUK, 2020). Cada um dos componentes arquiteturais é tratado como um micro serviço, e essa vertente valoriza a escalabilidade, a granularidade e a diversificação de tecnologia.

Segundo Duarte (2017), enquanto na arquitetura tradicional de *software*, chamada monolítica, quebramos uma grande aplicação em bibliotecas, cujos objetos são utilizados *in-process*, em uma aplicação modular como proposta na arquitetura de *microservices* cada módulo recebe requisições, as processa e devolve ao seu requerente o resultado, geralmente via *Hypertext Transfer Protocol* (HTTP).

4.2.4 Resultados das extrações

A Tabela 5 apresenta os resultados obtidos das extrações das postagens dos dois bancos, Caixa e Nubank, nas suas respectivas páginas nas lojas de aplicativo *Google Play Store* e *App Store*, e na rede social *Twitter*. Foram extraídas 3000 postagens do Nubank da *Google Play Store*, 500 da *App Store* e 342 do *Twitter*. Para a Caixa, foram extraídas 3000 postagens da *Google Play Store*, 500 da *App Store* e 265 do *Twitter*. O período de extração e classificação das postagens foi de 27 de abril de 2022 a 27 de maio de 2022.

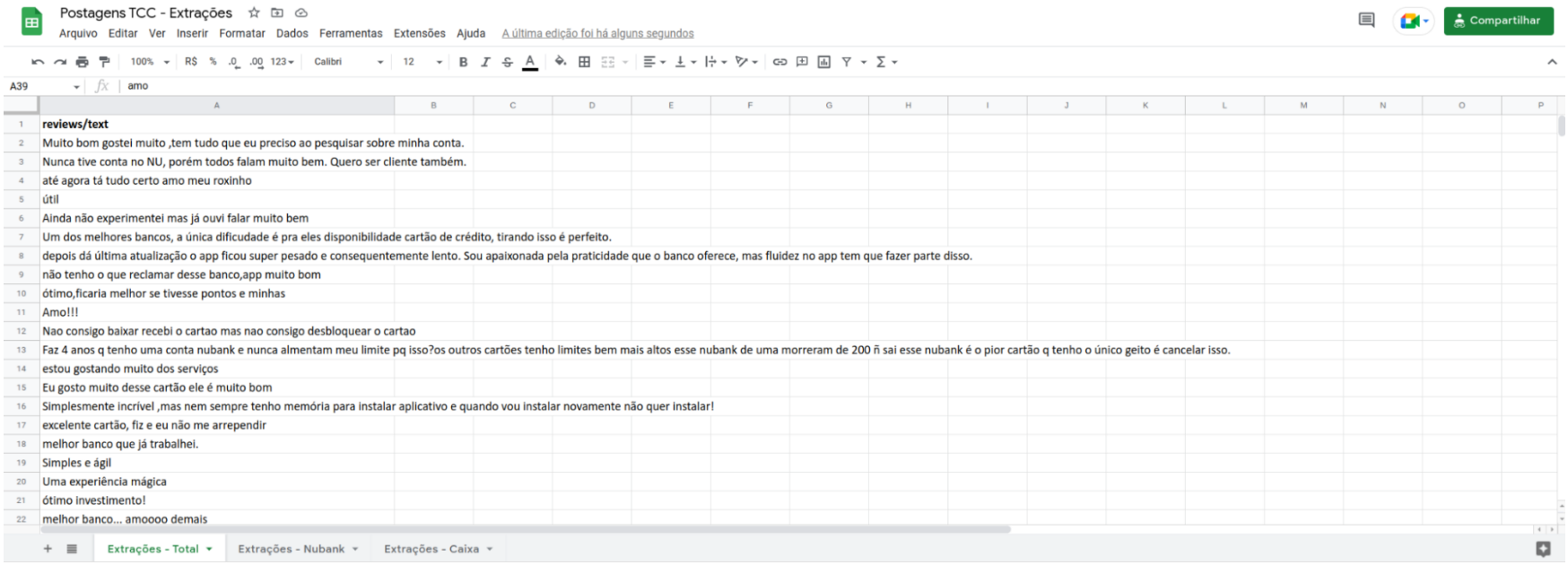
Para melhor organizar as postagens, as mesmas foram sendo coletadas e armazenadas em planilhas de acordo com a data de extração, conforme demonstrado na Figura 11.

Tabela 5 – Resultados obtidos das extrações de postagens da Caixa e Nubank.

Base de extração	CAIXA	NUBANK	TOTAL
GOOGLE PLAY STORE	3000	3000	6000 (78,8%)
APP STORE	500	500	1000 (13,2%)
TWITTER	265	342	607 (8%)
TOTAL DE POSTAGENS	3765	3842	7607 (100%)

Fonte: elaborado pelo autor (2022).

Figura 11 – Planilha com postagens extraídas.

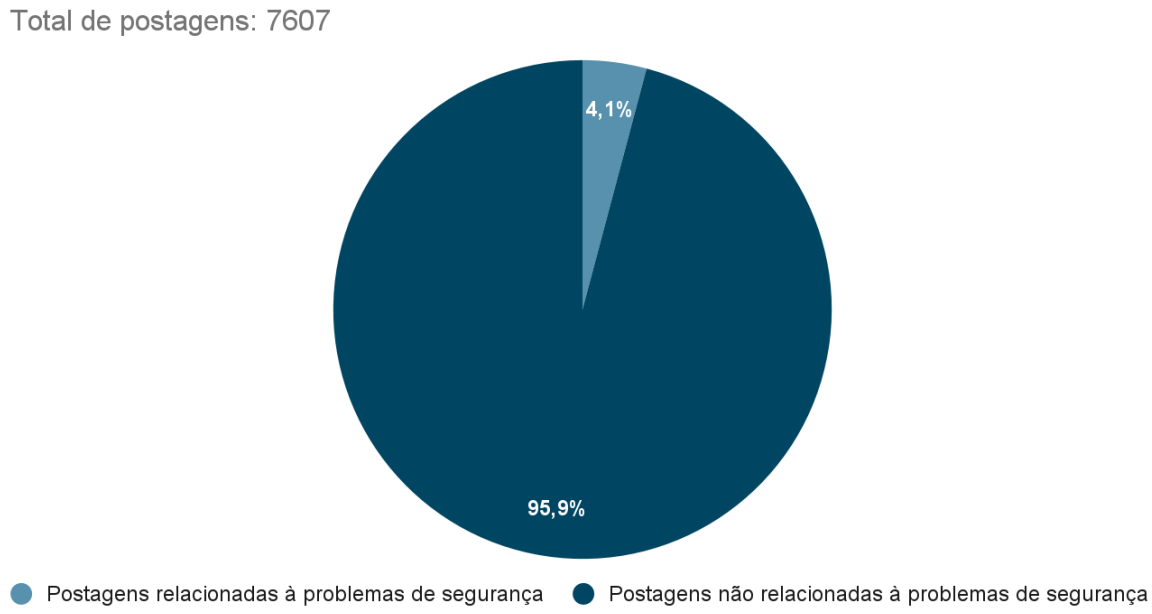


Fonte: elaborado pelo autor (2022).
Nota: Disponível em:<https://docs.google.com/spreadsheets/d/1C-T_KEyVI0XJAhkFvutWJd2ECgD8iuiSpT01jfmMTWc/edit?usp=sharing>

4.3 Classificação das postagens

Inicialmente, a partir das postagens extraídas e organizadas em planilhas, foi realizada uma classificação manual das 7607 postagens pelo autor deste trabalho, no período de 27 de abril de 2022 a 27 de maio de 2022. Foram classificadas manualmente como postagens relacionadas à problemas de segurança 315 postagens e foram descartadas 7292 postagens por não serem relacionadas a problemas de segurança, como mostra a Figura 12.

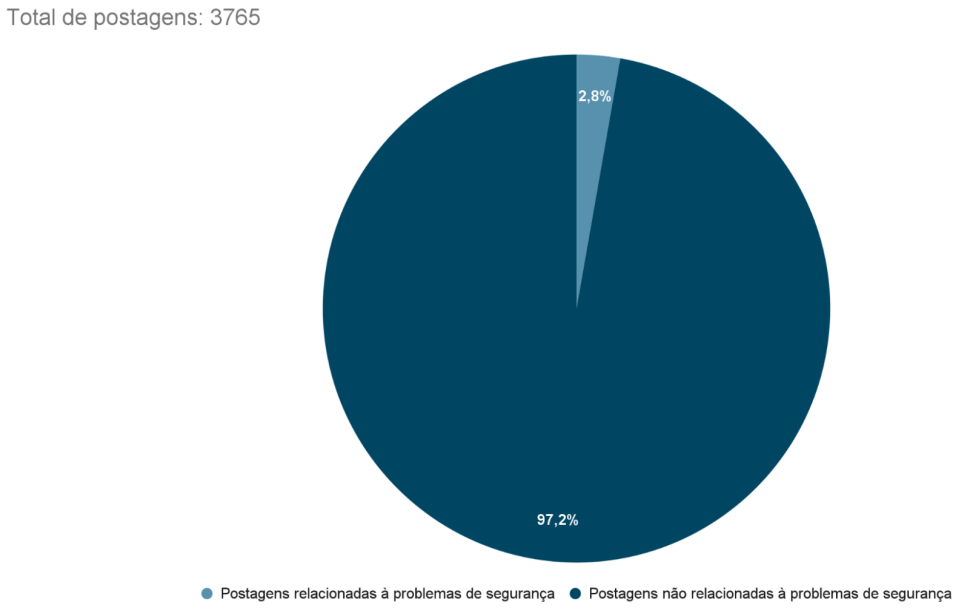
Figura 12 – Porcentagem de postagens de problemas de segurança classificadas manualmente.



Fonte: elaborado pelo autor (2022).

Para o aplicativo da Caixa, foram classificadas como postagens relacionadas à segurança 104 postagens e foram descartadas 3661 postagens, por não serem relacionadas à segurança, como é apresentado na Figura 13.

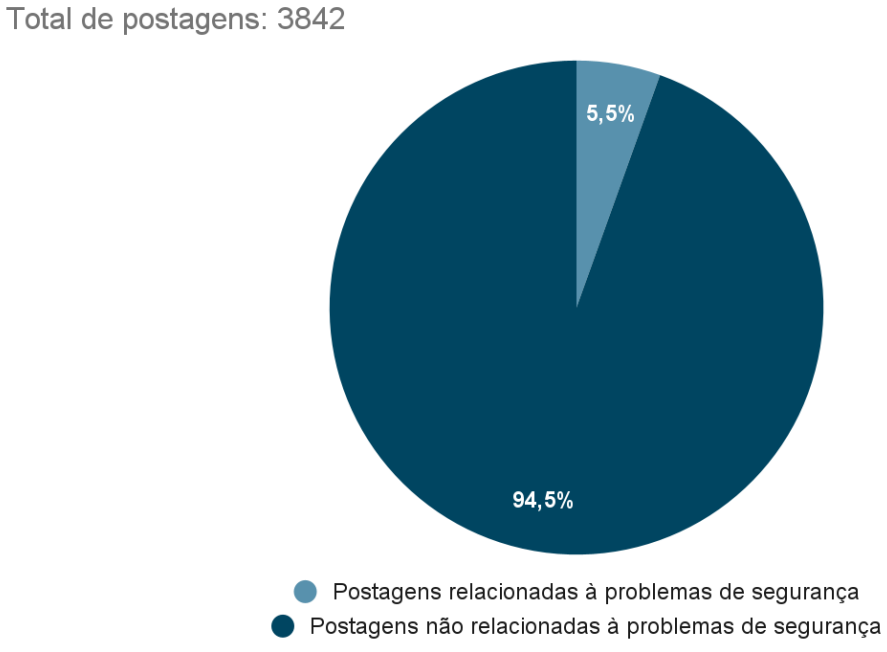
Figura 13 – Porcentagem de postagens de segurança do aplicativo da Caixa classificadas manualmente.



Fonte: elaborado pelo autor (2022).

Já para o aplicativo do Nubank, foram classificadas como postagens relacionadas à segurança 211 postagens e foram descartadas 3631 postagens, por não serem relacionadas à segurança, como mostra a Figura 14.

Figura 14 – Porcentagem de postagens de segurança do aplicativo do Nubank classificadas manualmente.



Fonte: elaborado pelo autor (2022).

Esta classificação teve como objetivo identificar quais das postagens extraídas estão relacionadas a problemas de segurança da informação, e classificá-las nas 4 categorias apresentadas no Quadro 2.

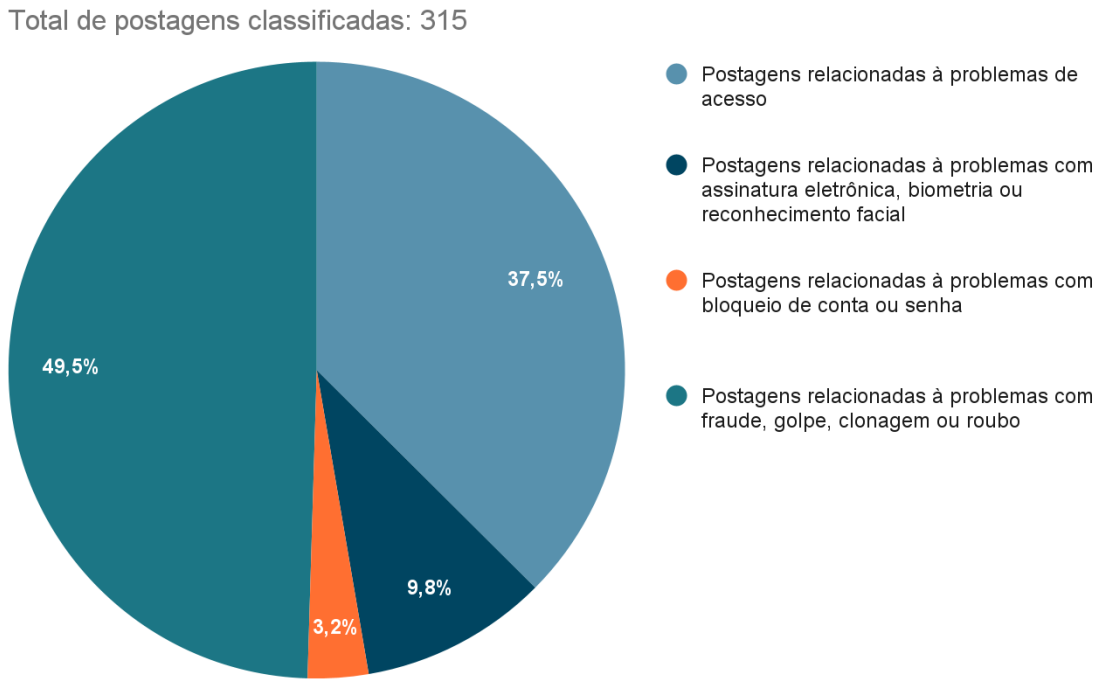
Quadro 2 – Tipos de postagens de segurança extraídas e principais categorias encontradas.

Categorias	**Definição**	**Exemplo**
Postagens relacionadas à problemas de acesso	Postagens que relatam problemas ao acessar os aplicativos, como problemas de login	*"Após a ultima atualização não consigo mais fazer login. Ao digitar minha senha o app entra na tela de "Estabelecendo conexão segura" e não sai mais. Estou impedida de realizar transações."*
Postagens relacionadas à problemas com assinatura eletrônica, biometria ou reconhecimento facial	Postagens que relatam problemas ao utilizar alternativas à autenticação por senha, como login e transações utilizando biometria	*"Muitas das vezes o app apresenta falhas, como por exemplo, não reconhece a biometria. E ultimamente, sobretudo há pouco mais de uma semana, não consigo abrir o app, e quando abre não consigo fazer nada. SEI QUE NÃO ADIANTA RECLAMAR AQUI, pois já fiz isso e nada resolveram. Mas, quem sabe tenho sorte desta vez, né?"*
Postagens relacionadas à problemas com bloqueio de conta ou senha	Postagens que relatam problemas de bloqueio ocasionados por falhas, como não reconhecimento de senha cadastrada	*"O pior App de Banco que já utilizei, muitas vezes fica fora do ar. Muito instável e lento, quase sempre não deixa utilizar a biometria, constantemente não reconhece a senha e de vez enquando a bloqueia."*
Postagens relacionadas à problemas com fraude, golpe, clonagem ou roubo	Postagens que relatam situações fraudulentas, clonagem, roubo ou golpe, como clonagem de cartão virtual e compras desconhecidas	*"Clonaram meu cartão DE NOVO, tentaram fazer compras totalmente aleatórias e a segurança do nubank falhou, eu vou eh cancelar essa conta."*

Fonte: elaborado pelo autor (2022).

A Figura 15 apresenta a porcentagem de postagens de problemas de segurança classificados por categoria manualmente.

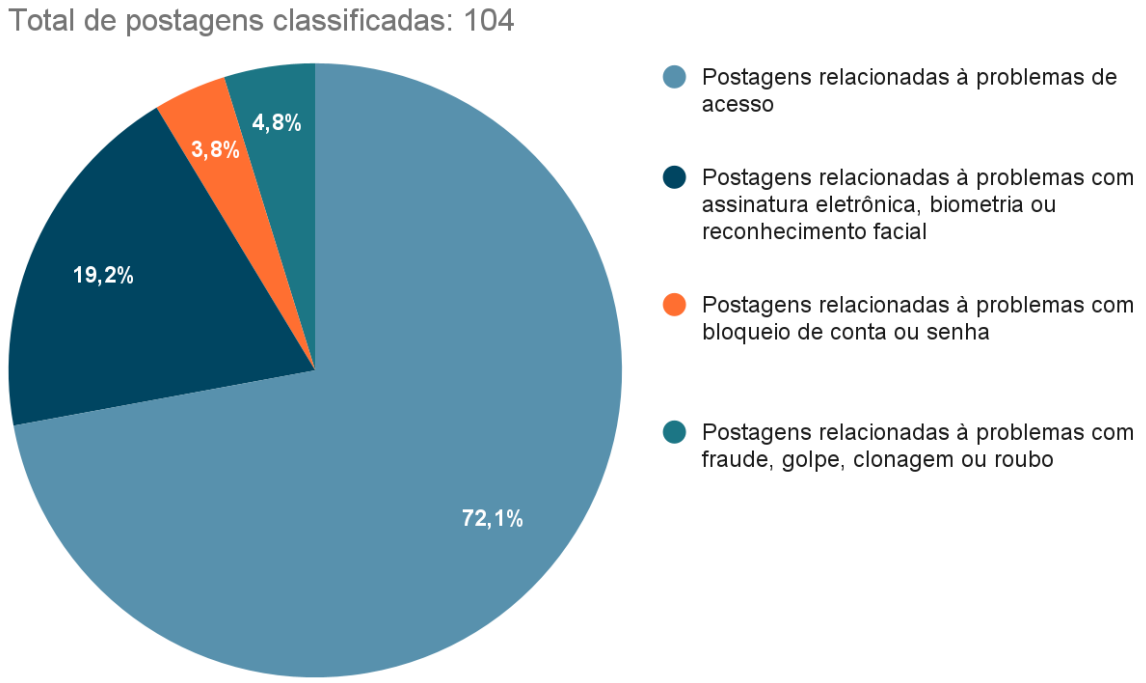
Figura 15 – Porcentagem de postagens de problemas de segurança classificados por categoria manualmente.



Fonte: elaborado pelo autor (2022).

A Figura 16 mostra a porcentagem de postagens de problemas de segurança do aplicativo da Caixa classificados por categoria manualmente.

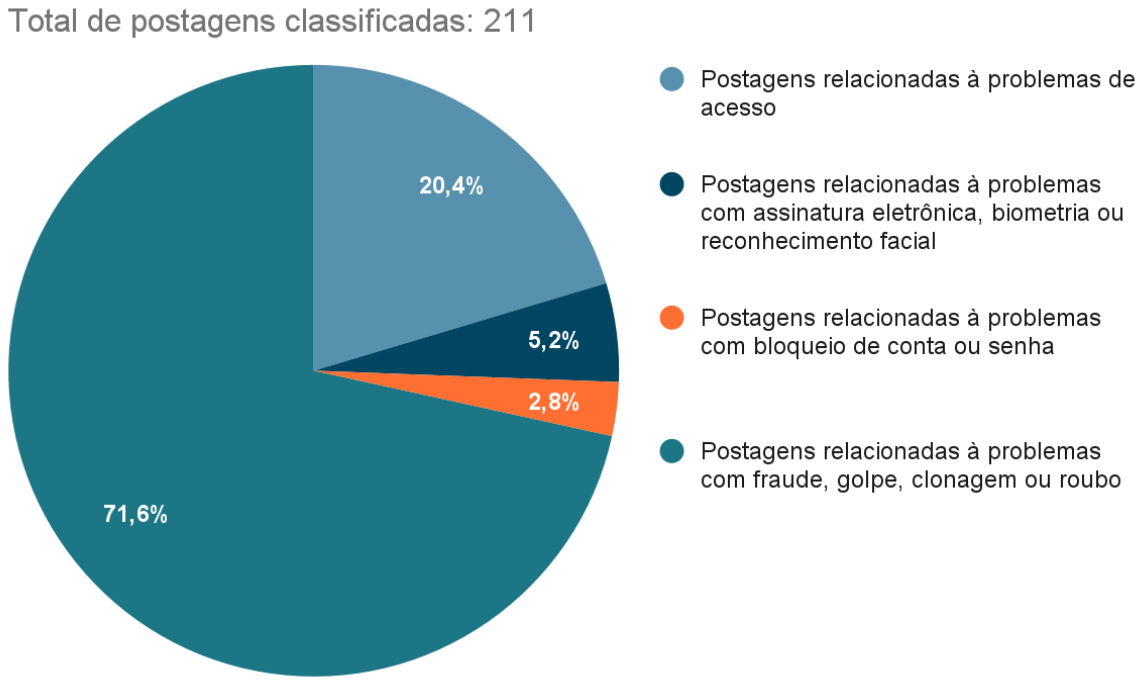
Figura 16 – Porcentagem de postagens de problemas de segurança do aplicativo da Caixa classificados por categoria manualmente.



Fonte: elaborado pelo autor (2022).

A Figura 17 mostra a porcentagem de postagens de problemas de segurança do aplicativo do Nubank classificados por categoria manualmente.

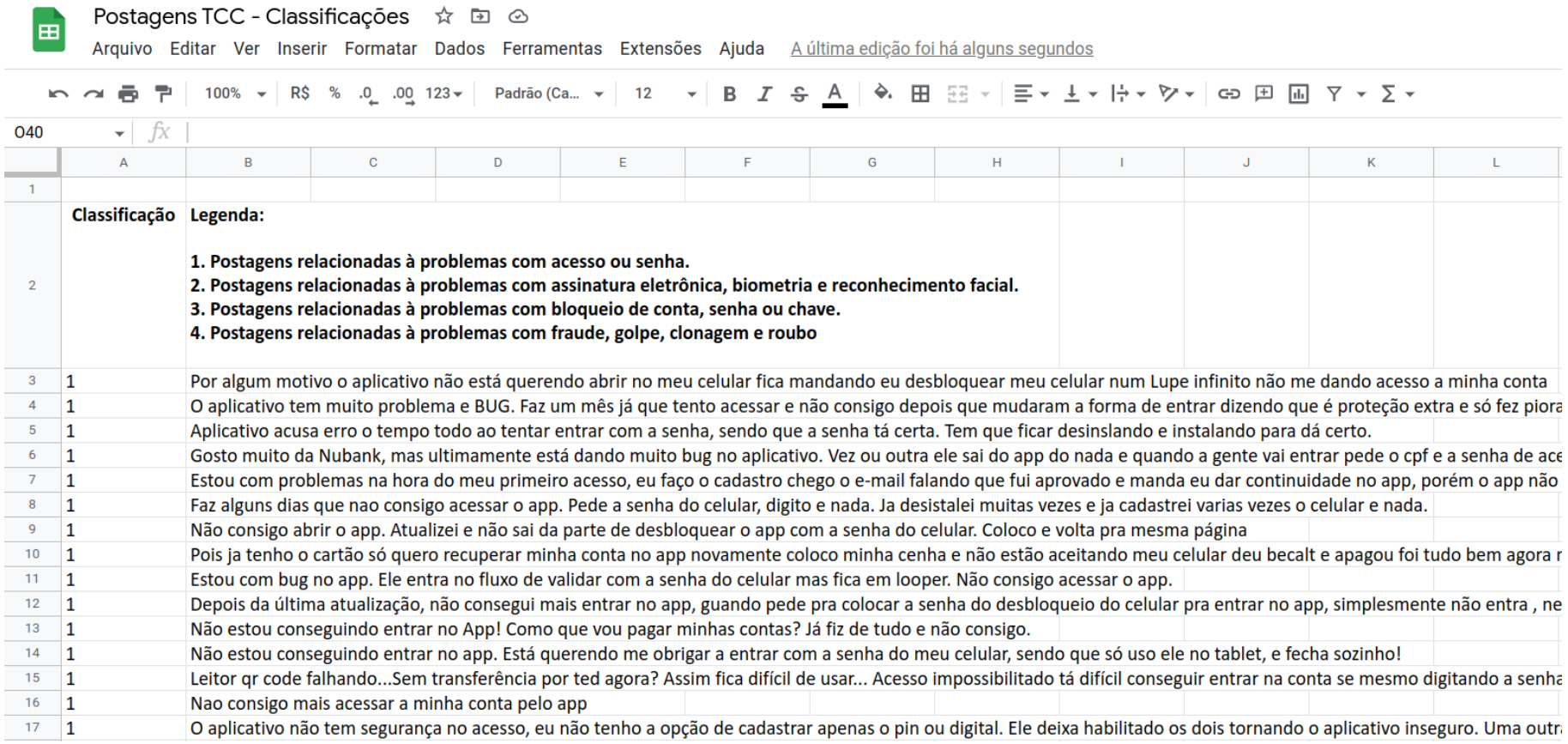
Figura 17 – Porcentagem de postagens de problemas de segurança do aplicativo do Nubank classificados por categoria manualmente.



Fonte: elaborado pelo autor (2022).

As postagens classificadas manualmente como relacionadas a problemas de segurança foram agrupadas em uma planilha. A Figura 18 apresenta um trecho da planilha com a classificação manual.

Figura 18 – Classificação manual das postagens extraídas.



Postagens TCC - Classificações

Arquivo Editar Ver Inserir Formatar Dados Ferramentas Extensões Ajuda A última edição foi há alguns segundos

	A	B
2	**Classificação**	**Legenda:** **1. Postagens relacionadas à problemas com acesso ou senha.** **2. Postagens relacionadas à problemas com assinatura eletrônica, biometria e reconhecimento facial.** **3. Postagens relacionadas à problemas com bloqueio de conta, senha ou chave.** **4. Postagens relacionadas à problemas com fraude, golpe, clonagem e roubo**
3	1	Por algum motivo o aplicativo não está querendo abrir no meu celular fica mandando eu desbloquear meu celular num Lupe infinito não me dando acesso a minha conta
4	1	O aplicativo tem muito problema e BUG. Faz um mês já que tento acessar e não consigo depois que mudaram a forma de entrar dizendo que é proteção extra e só fez piora
5	1	Aplicativo acusa erro o tempo todo ao tentar entrar com a senha, sendo que a senha tá certa. Tem que ficar desinslando e instalando para dá certo.
6	1	Gosto muito da Nubank, mas ultimamente está dando muito bug no aplicativo. Vez ou outra ele sai do app do nada e quando a gente vai entrar pede o cpf e a senha de ace
7	1	Estou com problemas na hora do meu primeiro acesso, eu faço o cadastro chego o e-mail falando que fui aprovado e manda eu dar continuidade no app, porém o app não
8	1	Faz alguns dias que nao consigo acessar o app. Pede a senha do celular, digito e nada. Ja desistalei muitas vezes e ja cadastrei varias vezes o celular e nada.
9	1	Não consigo abrir o app. Atualizei e não sai da parte de desbloquear o app com a senha do celular. Coloco e volta pra mesma página
10	1	Pois ja tenho o cartão só quero recuperar minha conta no app novamente coloco minha cenha e não estão aceitando meu celular deu becalt e apagou foi tudo bem agora r
11	1	Estou com bug no app. Ele entra no fluxo de validar com a senha do celular mas fica em looper. Não consigo acessar o app.
12	1	Depois da última atualização, não consegui mais entrar no app, guando pede pra colocar a senha do desbloqueio do celular pra entrar no app, simplesmente não entra , ne
13	1	Não estou conseguindo entrar no App! Como que vou pagar minhas contas? Já fiz de tudo e não consigo.
14	1	Não estou conseguindo entrar no app. Está querendo me obrigar a entrar com a senha do meu celular, sendo que só uso ele no tablet, e fecha sozinho!
15	1	Leitor qr code falhando...Sem transferência por ted agora? Assim fica difícil de usar... Acesso impossibilitado tá difícil conseguir entrar na conta se mesmo digitando a senha
16	1	Nao consigo mais acessar a minha conta pelo app
17	1	O aplicativo não tem segurança no acesso, eu não tenho a opção de cadastrar apenas o pin ou digital. Ele deixa habilitado os dois tornando o aplicativo inseguro. Uma outr

Fonte: elaborado pelo autor (2022).
Nota: Disponível em: <https://docs.google.com/spreadsheets/d/1oPZOCaeQH8jjMHorFpZPNPR9ZkzZ-7U52hIYAcOVYjk/edit?usp=sharing>

A classificação manual serviu de base para o desenvolvimento do algoritmo para classificação automática. A partir das postagens obtidas através dela foi implementado um algoritmo (Figura 19) para obter a frequência de palavras presentes nas postagens, com o objetivo de identificar padrões e regras relacionadas à segurança, e aplicá-las no algoritmo de classificação automática.

Figura 19 – Algoritmo de frequência de palavras implementado em Python.

```
import matplotlib.pyplot as plt
import nltk

dataList = data['stopwords_reviews'].to_list()

words = []

for i in range(len(dataList)):
    for j in range(len(dataList[i])):
        words.append(dataList[i][j])

fdist = nltk.FreqDist(words).most_common(10)

fdist = pd.Series(dict(fdist))

fig, ax = plt.subplots(figsize=(10,10))

barplot = sns.barplot(x=fdist.index, y=fdist.values, ax=ax)
plt.title('Frequency Word')
plt.xticks(rotation=30);
```

[51] ✓ 0.2s

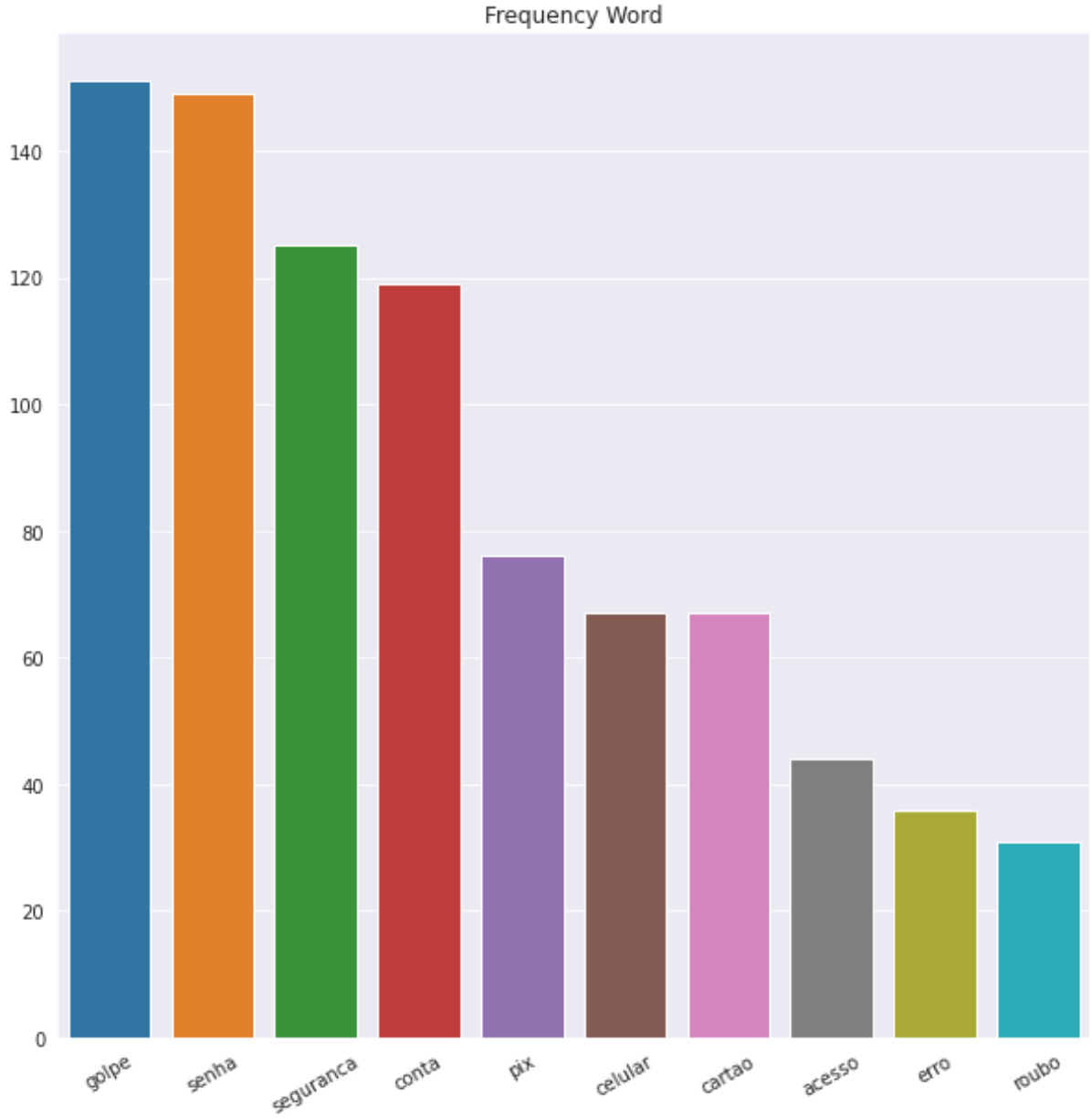
Fonte: elaborado pelo autor (2022).
Nota: Disponível em: <https://github.com/souzamoab/reviews-classifier-algorithm>

A partir das postagens, foram obtidas com a utilização do algoritmo as 10 palavras mais mencionadas após passarem por algumas etapas de pré-processamento que serão definidas no próximo tópico. A Figura 20 apresenta o resultado da execução do algoritmo, com as palavras mais frequentes das postagens.

4.4 Pré-processamento das postagens

Neste ponto foram realizadas as implementações das etapas de pré-processamento, utilizando a linguagem *Python*. Para implementação destas etapas no algoritmo foram utilizadas as bibliotecas *spaCy* e Natural Language Toolkit (NLTK), bibliotecas *Python* usadas para

Figura 20 – Palavras mais frequentes em todas as categorias de postagens.



Fonte: elaborado pelo autor (2022).

trabalhar com dados de linguagem humana para aplicação em PLN. Estas bibliotecas possuem estruturas para construção de programas de PLN em Python e fornecem classes e interfaces para representar os dados necessários para o processamento da linguagem natural, bem como executar processos como tokenização e classificação textual, que serão descritos a seguir.

- **Limpeza do texto:** esta etapa foi implementada em Python utilizando o *spaCy* para carregamento dos seus *pipelines* treinados em português. Também foi utilizado o módulo de expressões regulares (*Regular Expressions*), para realizar operações de remoção de caracteres especiais e *emojis*;
- **Tokenização:** esta etapa foi implementada utilizando o pacote *tokenize* da biblioteca

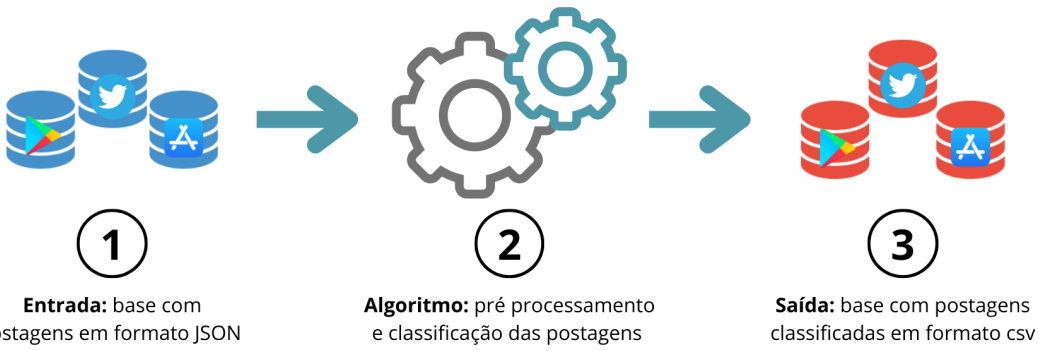
NLTK;

- **Remoção de stopwords:** esta etapa foi implementada utilizando o módulo de *stopwords* do NLTK e do *spaCy*;
- **Lematização e stemização:** estas etapas foram implementadas utilizando os módulos de lematização (*WordNetLemmatizer*) e stemização (*RSLPStemmer*), do NLTK.

4.5 Algoritmo para classificação de postagens

Foi desenvolvido um algoritmo de classificação em Python que utiliza um mecanismo de correspondência baseado em regras, padrões e *strings* de busca. Esse mecanismo é o *PhraseMatcher*, que está presente no *spaCy*. Ele permite combinar com eficiência grandes listas de frases, e aceita padrões de correspondência na forma de objetos que possuem sequências de *tokens*. A Figura 21 apresenta o processo de execução do algoritmo.

Figura 21 – Processo de execução do algoritmo de classificação automática das postagens.



Fonte: elaborado pelo autor (2022).

O *PhraseMatcher* utiliza padrões para realizar as correspondências entre os *tokens*, ou seja, utiliza de palavras ou termos pré-definidos para efetuar buscas e correspondências nas postagens extraídas. Como padrões foram utilizadas as palavras obtidas no algoritmo de frequência apresentado anteriormente. Para uma melhor eficiência, as palavras obtidas passaram por um processo de stemização, e foram reduzidas aos seus radicais, facilitando a correspondência

com as postagens extraídas usando o *PhraseMatcher*. Dessa forma o algoritmo utiliza estes padrões para realizar a classificação de acordo com as 4 categorias apresentadas anteriormente. Na Figura 22 é apresentado o algoritmo desenvolvido.

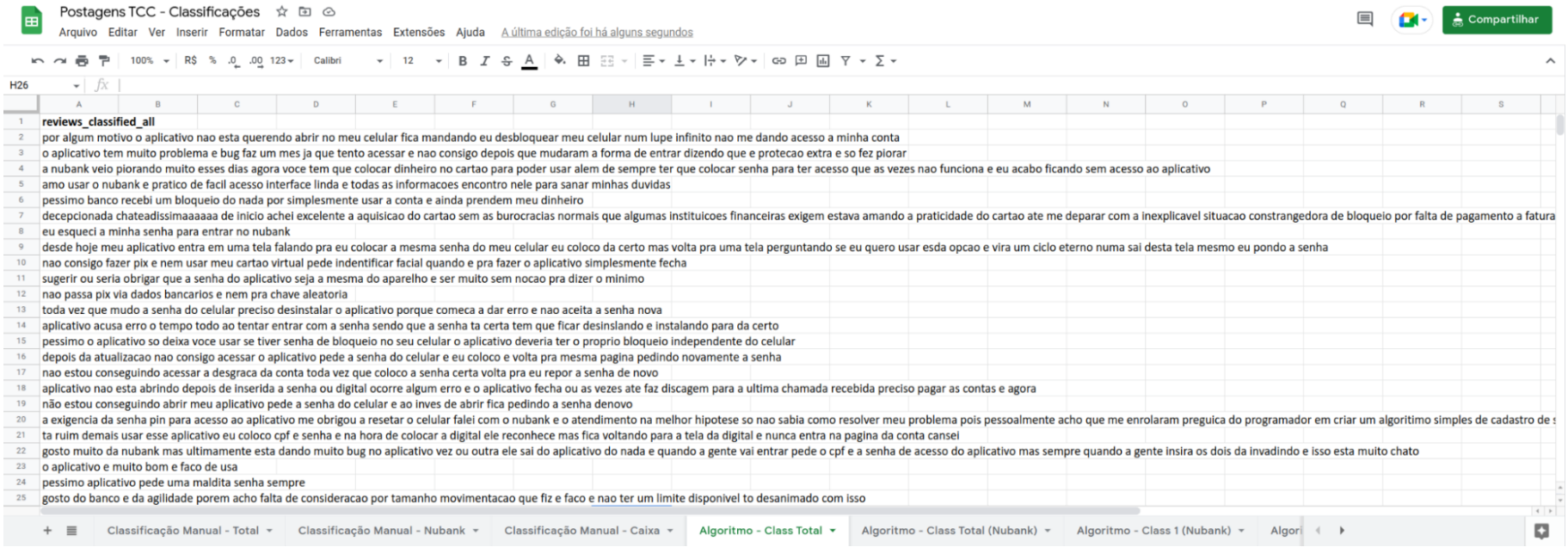
Figura 22 – Algoritmo classificador de postagens.

```
import spacy
from spacy.matcher import PhraseMatcher

nlp = spacy.load('pt_core_news_sm')

def securityReviewsClassifier(text):
    securityReviews = []
    doc = nlp(text)

    securityTerms = mostCommonStem
    patterns = [nlp(term) for term in securityTerms]

    matcher = PhraseMatcher(nlp.vocab)
    matcher.add("SECURITY_PATTERN", patterns)

    matches = matcher(doc)

    for i in range(0,len(matches)):
        token = doc[matches[i][1]:matches[i][2]]
        securityReviews.append(str(token))

    return securityReviews
```

Fonte: elaborado pelo autor (2022).
Nota: Disponível em: <https://github.com/souzamoab/reviews-classifier-algorithm>

A seguir, na Figura 23, é apresentada a saída do algoritmo em formato *.csv* contendo as postagens classificadas em cada critério.

Figura 23 – Saída do algoritmo classificador de postagens de segurança.



Fonte: elaborado pelo autor (2022).
Nota: Disponível em: <https://docs.google.com/spreadsheets/d/1oPZOCaeQH8jjMHorFpZPNPR9ZkzZ-7U52hIYAcOVYjk/edit?usp=sharing>

4.6 Análise das postagens

Com base nas 7607 postagens extraídas, o algoritmo realizou uma classificação automática para obter as postagens relacionadas a problemas de segurança. Foram classificadas pelo algoritmo como postagens relacionadas à problemas de segurança 568 postagens e foram descartadas 7039 postagens por não serem relacionadas a problemas de segurança, como mostra a Figura 24.

Figura 24 – Porcentagem de postagens de problemas de segurança classificadas automaticamente pelo algoritmo.

Fonte: elaborado pelo autor (2022).

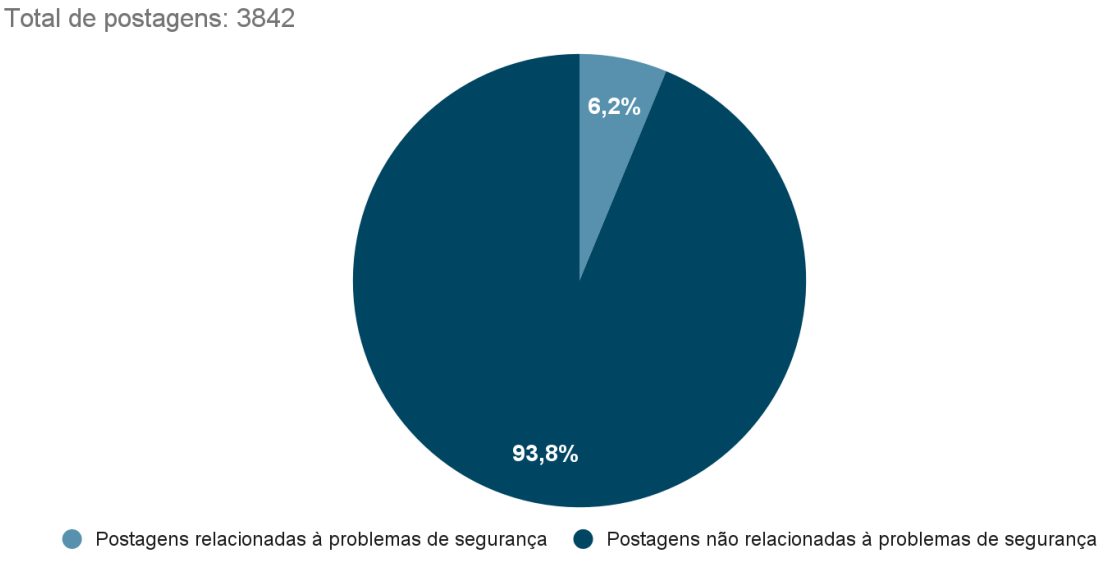
Para o aplicativo da Caixa, foram classificadas pelo algoritmo como postagens relacionadas à problemas de segurança 328 postagens e foram descartadas 3437 postagens por não serem relacionadas a problemas de segurança, como é apresentado na Figura 25.

Figura 25 – Porcentagem de postagens de segurança do aplicativo da Caixa classificadas pelo algoritmo.

Fonte: elaborado pelo autor (2022).

Para o aplicativo do Nubank, foram classificadas pelo algoritmo como postagens relacionadas à problemas de segurança 240 postagens e foram descartadas 3602 postagens por não serem relacionadas a problemas de segurança, como é apresentado na Figura 26.

Figura 26 – Porcentagem de postagens de segurança do aplicativo do Nubank classificadas pelo algoritmo.



Fonte: elaborado pelo autor (2022).

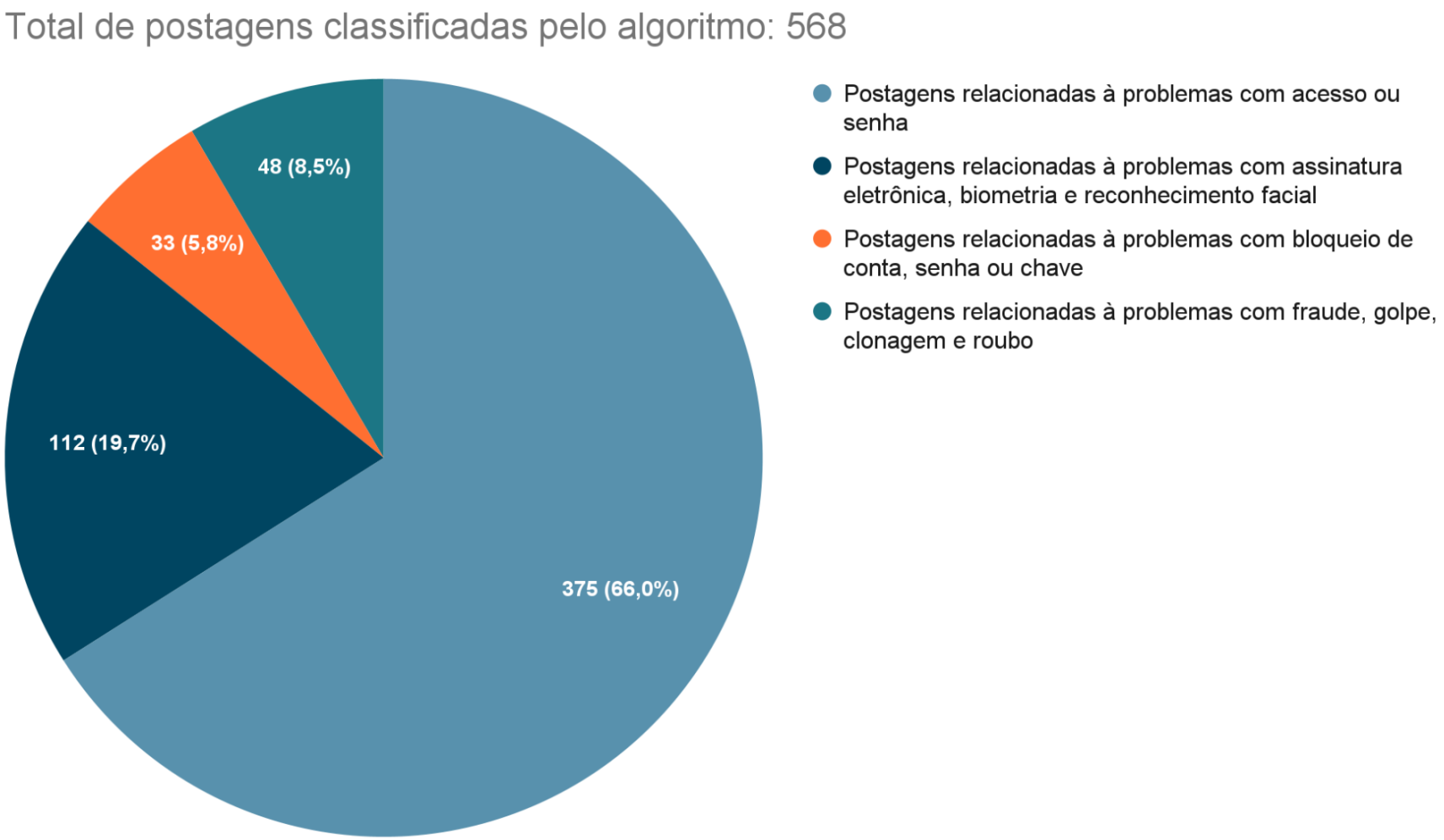
Após a análise das postagens, foi identificado que o aplicativo da Caixa apresentou

uma quantidade maior de problemas relacionados à segurança, comparando-se ao aplicativo do Nubank. A seguir são apresentados os resultados das extrações e da classificação das postagens pelo algoritmo de acordo com as categorias de problemas levantadas.

4.7 Resultados

Como mencionado nos tópicos anteriores, foram desenvolvidas três APIs e uma aplicação centralizadora para extração das postagens, e também um algoritmo utilizado para classificação automática das postagens, que passaram por pré-processamentos até que fossem classificadas como postagens de segurança. Além disso, este algoritmo realiza uma classificação com o objetivo de categorizar os problemas em 4 categorias: (1) Postagens relacionadas à problemas com acesso ou senha; (2) Postagens relacionadas à problemas com assinatura eletrônica, biometria e reconhecimento facial; (3) Postagens relacionadas à problemas com bloqueio de conta, senha ou chave; e (4) Postagens relacionadas à problemas com fraude, golpe, clonagem e roubo. A Figura 27 apresenta a quantidade e a porcentagem de problemas de segurança classificados por categoria pelo algoritmo.

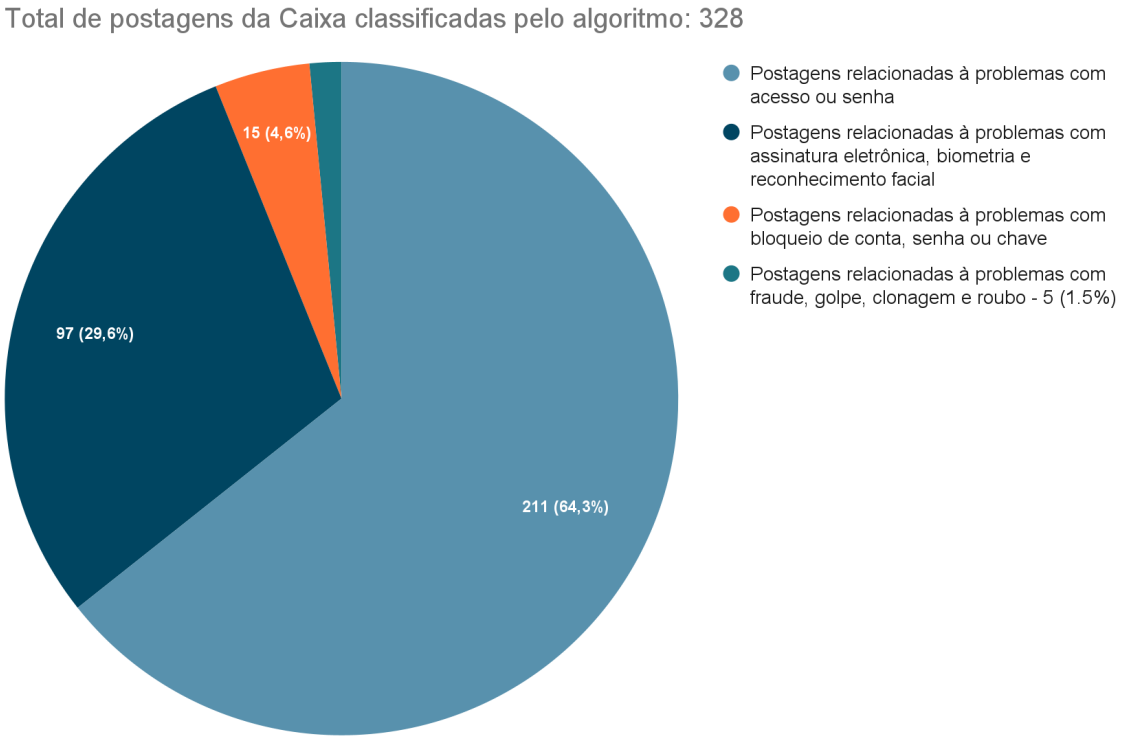
Figura 27 – Quantidade e porcentagem de postagens de problemas de segurança classificados por categoria pelo algoritmo.



Fonte: elaborado pelo autor (2022).

A Figura 28 apresenta a quantidade e a porcentagem de problemas de segurança do aplicativo da Caixa classificados por categoria pelo algoritmo.

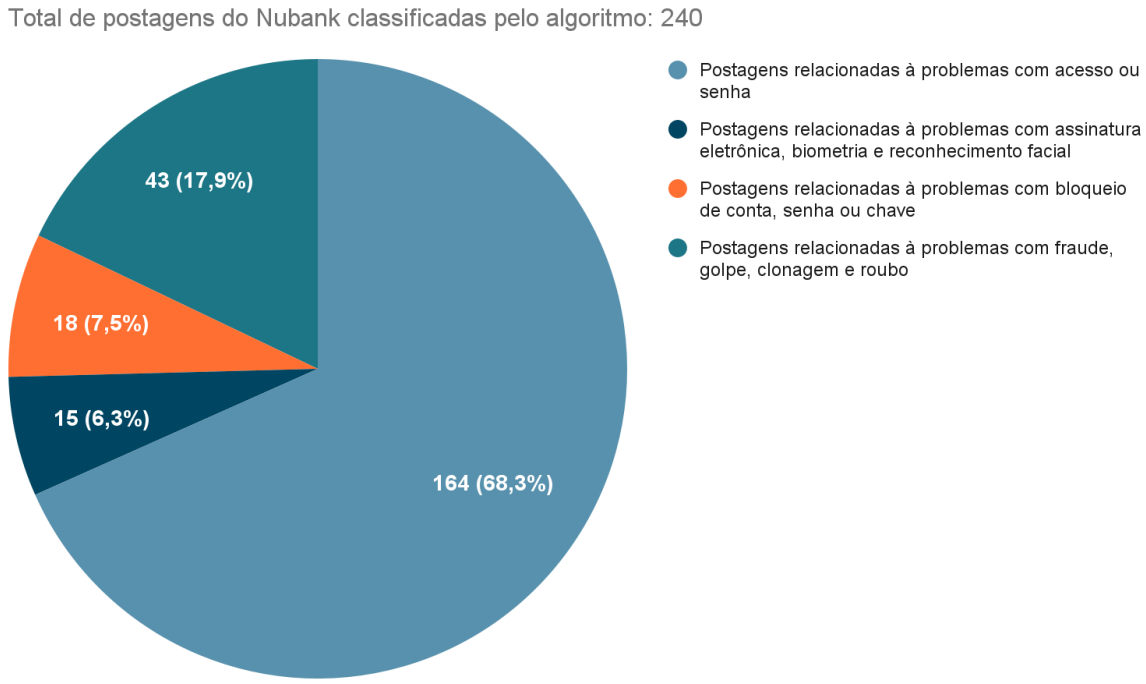
Figura 28 – Quantidade e porcentagem de postagens de problemas de segurança do aplicativo da Caixa classificados por categoria pelo algoritmo.



Fonte: elaborado pelo autor (2022).

A Figura 29 apresenta a quantidade e a porcentagem de problemas de segurança do aplicativo do Nubank classificados por categoria pelo algoritmo.

Figura 29 – Quantidade e porcentagem de postagens de problemas de segurança do aplicativo do Nubank classificados por categoria pelo algoritmo.



Fonte: elaborado pelo autor (2022).

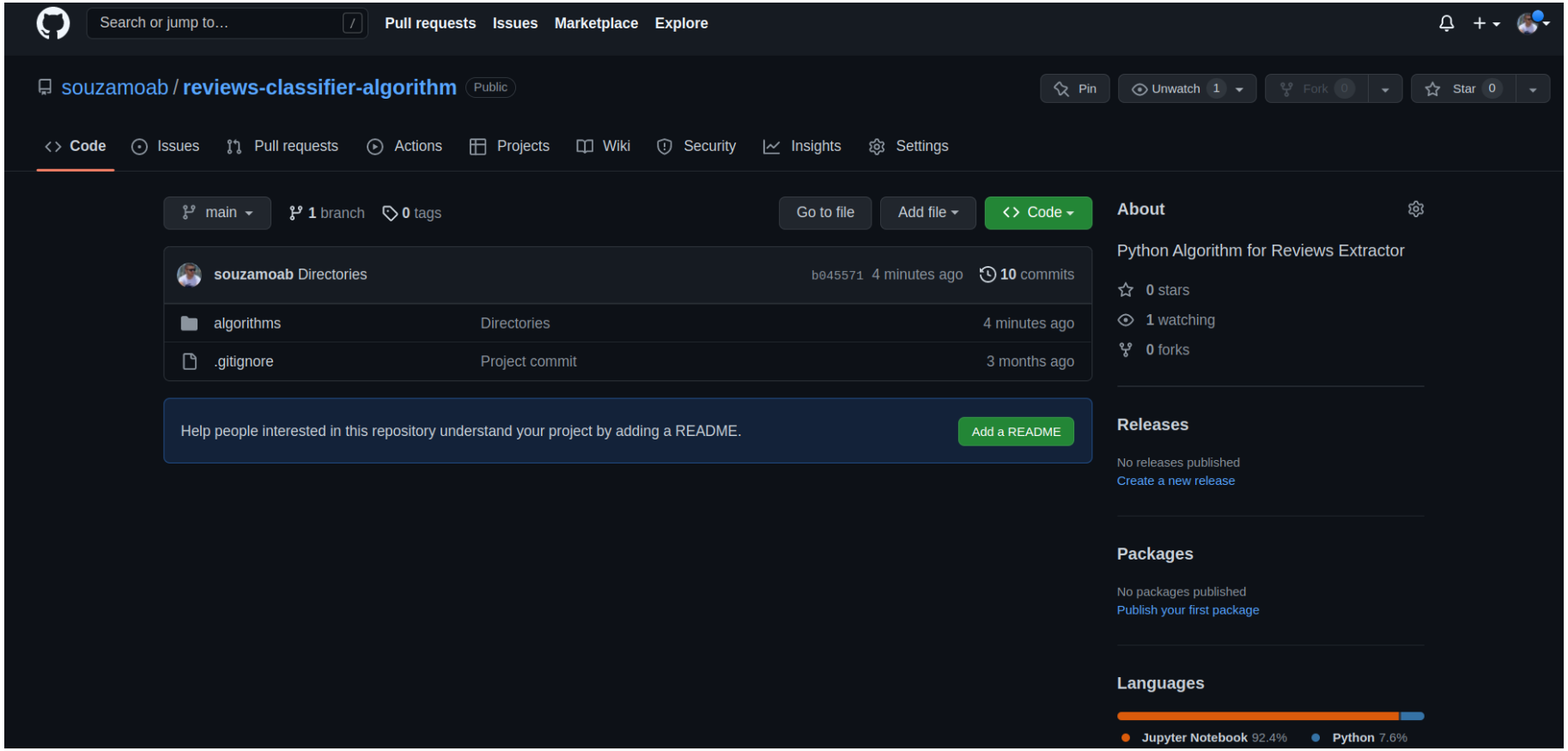
5 CONCLUSÃO

A partir dos estudos realizados e desenvolvidos neste trabalho, foi possível cumprir com os objetivos definidos, investigando a opinião dos usuários sobre a segurança da informação no uso de aplicativos bancários e identificando os principais problemas relacionados à segurança da informação. Foi desenvolvido e apresentado um algoritmo para identificação e classificação automática de problemas de segurança a partir de postagens, e foi feito um mapeamento e categorização dos principais problemas encontrados.

5.1 Resultados do trabalho

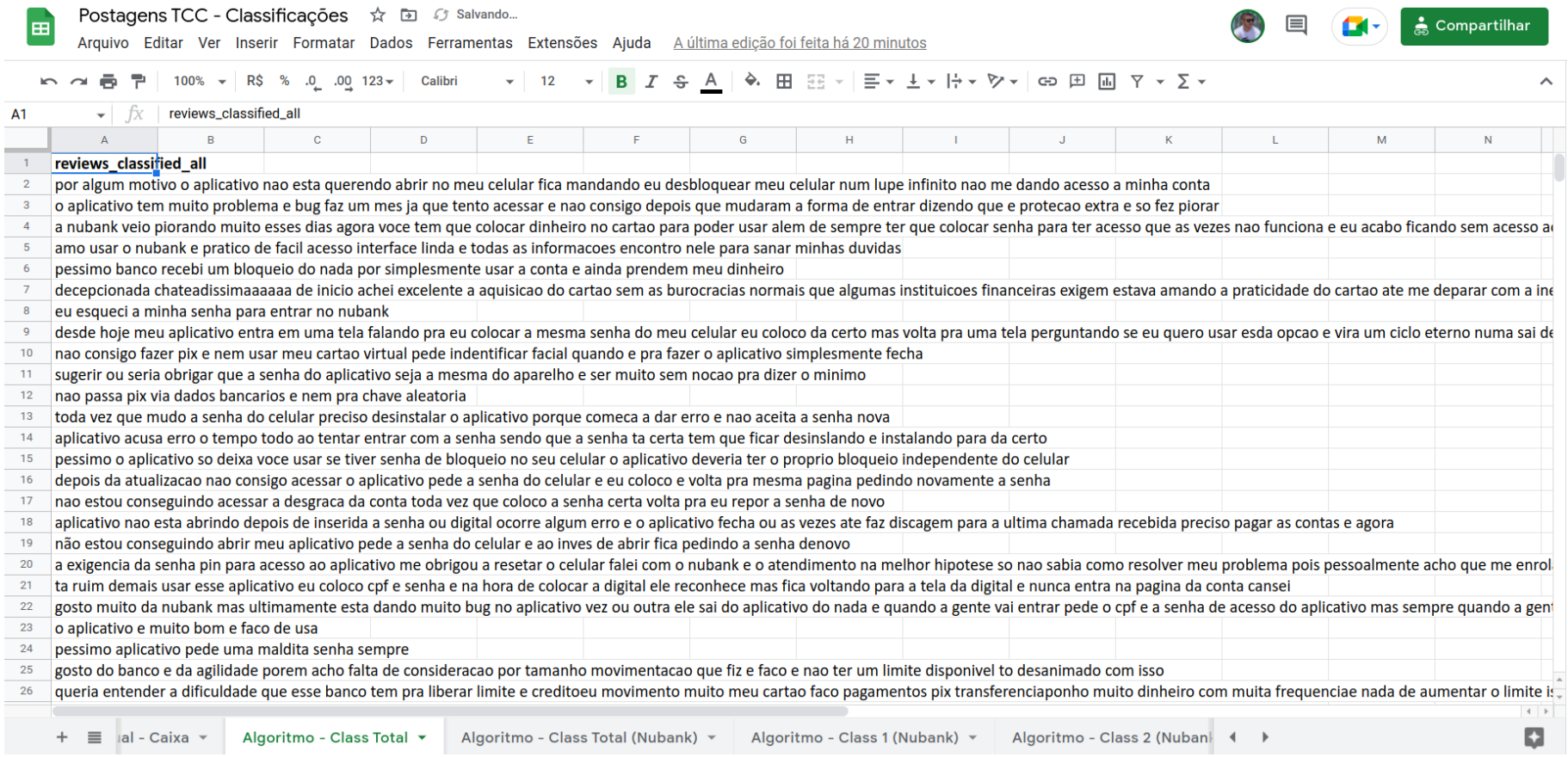
Este trabalho apresentou o quão amplo é trabalhar com processamento de linguagem natural e com áreas de avaliação textual, e a diversidade de soluções que elas oferecem. Desse modo, este trabalho contribuiu para os estudos acerca dessas áreas através dos seguintes resultados: (1) realização de análise da segurança da informação nos aplicativos das instituições financeiras Caixa e Nubank, a partir das postagens dos usuários nas lojas de aplicativos *Google Play Store* e *App Store*, e da rede social *Twitter*; (2) desenvolvimento de algoritmo de classificação automática de postagens relacionadas à segurança da informação em aplicativos de instituições financeiras, disponibilizado em repositório público (Figura 30); e (3) base de dados de postagens relacionadas à segurança da informação em aplicativos de instituições financeiras classificada (Figura 31).

Figura 30 – Repositório público do algoritmo classificador de postagens.



Fonte: elaborado pelo autor (2022).
Nota: Disponível em: <https://github.com/souzamoab/reviews-classifier-algorithm>

Figura 31 – Base de dados de postagens classificada.



Fonte: elaborado pelo autor (2022).
Nota: Disponível em: <https://docs.google.com/spreadsheets/d/1oPZOCaeQH8jjMHorFpZPNPR9ZkzZ-7U52hIYAcOVYjk/edit?usp=sharing>

5.2 Limitações

Durante a etapa de extração das postagens houve limitações na extração a partir da App Store e da rede social *Twitter*. Enquanto o módulo para extração de postagens da *Google Play Store* permitia extrações em massa, o módulo da *App Store* possuía um limite de extração de apenas 500 postagens. Já a API do *Twitter* permitia extrair no máximo 100 postagens a cada chamada, não podendo ultrapassar esse limite. Portanto, a partir do módulo da *App Store* foram extraídas as 500 postagens disponíveis, e a partir da API do *Twitter* foram realizadas cinco chamadas consecutivas, agrupando os resultados e eliminando as postagens repetidas.

Além disso, não foi desenvolvida ou utilizada nenhuma ferramenta de validação do algoritmo. A mesma foi realizada manualmente pelo autor deste trabalho, que informalmente confirmou a classificação correta das postagens pelo algoritmo, sendo esta uma forma de validação humana.

Por fim, poderiam ter sido investigados mais aspectos, como sentimentos dos usuários através de uma análise de sentimentos, o tipo de postagem e a funcionalidade através da metodologia MALTU, entre outros. Isto forneceria uma análise mais detalhada das postagem e tornaria a avaliação textual mais completa.

5.3 Trabalhos futuros

Como trabalhos futuros é fundamental que sejam implementadas melhorias nos processos de identificação e classificação das postagens de segurança, em busca de torná-los mais eficientes. Para isso, uma opção a ser adotada estratégias que utilizem técnicas de *Machine Learning*, tais como modelos de aprendizado para PLN, treinados em uma linguagem que sejam genéricos o suficiente para serem aplicados de forma satisfatória.

Outro ponto fundamental é a aplicação de uma validação do algoritmo, seja através de humanos ou através do desenvolvimento de um algoritmo validador. Junto a isso, realizar uma análise da validação com as métricas de avaliação (acurácia, precisão, *recall*, entre outras) para mensurar a eficácia do algoritmo.

Realizar uma análise mais detalhada das postagens para fornecer um resultado de avaliação da UX por sentimentos, pela metodologia MALTU (tipo de postagem e funcionalidade), a fim de fornecer uma avaliação textual completa, também é essencial.

Também é essencial realizar uma avaliação temporal, como no trabalho de Silva *et*

al. (2019), a partir das datas das postagens para identificação dos períodos de maior frequência de problemas de segurança.

Também é de suma importância expandir a pesquisa para mais bancos e fontes de dados (outras redes sociais) e realizar uma investigação com um volume maior de postagens, pois quanto maior esse número maior será a precisão e confiança da pesquisa.

Por fim, também é ideal desenvolver uma interface gráfica que consuma as APIs desenvolvidas e apresente as opções de entrada e resultados de forma visual, para facilitar a utilização das funcionalidades de extração e classificação das postagens.

REFERÊNCIAS

ALBASHRAWI, M.; MOTIWALLA, L. Understanding mobile banking usage: An integrative perspective. In: **Proceedings of the 2017 ACM SIGMIS Conference on Computers and People Research**. New York, NY, USA: Association for Computing Machinery, 2017. (SIGMIS-CPR '17), p. 63–70. ISBN 9781450350372. Disponível em: <https://doi.org/10.1145/3084381.3084405>.

ALMENARA, I. **Lançado em 2019, Android 10 ainda é o sistema mais popular do Google.** 2021. Disponível em: <https://canaltech.com.br/android/lancado-em-2019-android-10-ainda-e-o-sistema-do-google-mais-popular-202543/>. Acesso em: 15 jan. 2022.

ALTHOBAITI, M. M.; MAYHEW, P. Security and usability of authenticating process of online banking: User experience study. In: **2014 International Carnahan Conference on Security Technology (ICCST)**. [S.l.: s.n.], 2014. p. 1–6.

ANDRESS, J. **The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice**. 2. ed. [S.l.]: Elsevier, 2014.

ARISYA, K. F.; RULDEVIYANI, Y.; PRAKOSO, R.; FADHILAH, A. L. Measurement of information security awareness level: A case study of mobile banking (m-banking) users. In: **2020 Fifth International Conference on Informatics and Computing (ICIC)**. [S.l.: s.n.], 2020. p. 1–5.

BANCO CENTRAL DO BRASIL. 2021. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/rankingreclamacoes>. Acesso em: 18 jan. de 2022.

BARBOSA, S.; SILVA, B. **Interação Humano-Computador**. Elsevier Brasil, 2010. ISBN 9788535211207. Disponível em: <https://books.google.com.br/books?id=qk0skwr_cewC>.

BLASI, L.; SAVOLA, R.; ABIE, H.; ROTONDI, D. Applicability of security metrics for adaptive security management in a universal banking hub system. In: **Proceedings of the Fourth European Conference on Software Architecture: Companion Volume**. New York, NY, USA: Association for Computing Machinery, 2010. (ECSA '10), p. 197–204. ISBN 9781450301794. Disponível em: <https://doi.org/10.1145/1842752.1842792>.

BOLLINI, M. **Por que o Brasil lidera a digitalização bancária na América Latina**. 2021. Disponível em: <https://www.consumidormoderno.com.br/2021/06/04/brasil-lidera-digitalizacao-bancaria-america-latina/>. Acesso em: 04 jan. 2022.

BOTACIN, M.; KALYSCH, A.; GRéGIO, A. The internet banking [in]security spiral: Past, present, and future of online banking protection mechanisms based on a brazilian case study. In: **Proceedings of the 14th International Conference on Availability, Reliability and Security**. New York, NY, USA: Association for Computing Machinery, 2019. (ARES '19). ISBN 9781450371643. Disponível em: <https://doi.org/10.1145/3339252.3340103>.

CARMINATI, M.; POLINO, M.; CONTINELLA, A.; LANZI, A.; MAGGI, F.; ZANERO, S. Security evaluation of a banking fraud analysis system. **ACM Trans. Priv. Secur.**, Association for Computing Machinery, New York, NY, USA, v. 21, n. 3, apr 2018. ISSN 2471-2566. Disponível em: <https://doi.org/10.1145/3178370>.

CARNEIRO, L. **Mais de 34 milhões de brasileiros não tinham acesso a serviço bancário até 2018**. 2021. Disponível em: <https://valorinveste.globo.com/mercados/brasil-e-politica/noticia/2021/08/19/mais-de-34-milhoes-de-brasileiros-nao-tinham-acesso-a-servico-bancario-ate-2018.ghtml>. Acesso em: 18 dez. 2021.

CASELLA, G. **Liberdade Financeira: dicas para você alcançar a sua investindo**. 2017. Disponível em: <https://www.btgpactualdigital.com/blog/investimentos/liberdade-financeira-dicas-para-voce-alcancar-sua-investindo/amp>. Acesso em: 04 jan. 2022.

CAVALCANTI, G. K. M. As marcas no twitter: Uma anÁlise de perfis e repercussÃo de empresas no microblog. **Ciências Sociais Aplicadas em Revista**, v. 12, n. 22, p. 53–69, set. 2013. Disponível em: <https://e-revista.unioeste.br/index.php/csaemrevista/article/view/8636>.

CHEN, S.; SU, T.; FAN, L.; MENG, G.; XUE, M.; LIU, Y.; XU, L. Are mobile banking apps secure? what can be improved? In: **Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering**. New York, NY, USA: Association for Computing Machinery, 2018. (ESEC/FSE 2018), p. 797–802. ISBN 9781450355735. Disponível em: <https://doi.org/10.1145/3236024.3275523>.

CHIORAZZO, V.; D'APICE, V.; DEYOUNG, R.; MORELLI, P. Is the traditional banking model a survivor? **Journal of Banking Finance**, v. 97, p. 238–256, 2018. ISSN 0378-4266. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0378426618302322>.

CROSSLER, R. E.; JOHNSTON, A. C.; LOWRY, P. B.; HU, Q.; WARKENTIN, M.; BASKERVILLE, R. Future directions for behavioral information security research. **Computers Security**, v. 32, p. 90–101, 2013. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404812001460>.

DAHLMAN, C.; MEALY, S.; WERMELINGER, M. Harnessing the digital economy for developing countries. **OECD Development Centre Working Papers**, OECD Publishing, Paris, n. 334, 2016.

DUARTE, L. **Introdução à Arquitetura de Micro Serviços**. 2017. Disponível em: <https://www.luiztools.com.br/post/introducao-arquitetura-de-micro-servicos/>. Acesso em: 07 jun. 2022.

FREITAS, L. M.; SILVA, T. H. O. da; MENDES, M. S. Evaluation of spotify: An evaluation textual experience using the maltu methodology. In: **Proceedings of the 15th Brazilian Symposium on Human Factors in Computing Systems**. New York, NY, USA: Association for Computing Machinery, 2016. (IHC '16). ISBN 9781450352352. Disponível em: <https://doi.org/10.1145/3033701.3033752>.

GOLDSTEIN, J.; CHERNOBAI, A.; BENAROCH, M. An event study analysis of the economic impact of it operational risk and its subcategories. **Journal of the Association for Information Systems**, v. 12, 09 2011.

GOOGLE PLAY STORE. 2022. Disponível em: <https://play.google.com/store/apps/category/FINANCE?hl=pt_BR&gl=US>. Acesso em: 18 jan. de 2022.

HONOHAN, P. Financial development, growth and poverty: How close are the links? **World Bank Policy Research Working Paper**, OECD Publishing, n. 3203, p. 1–31, 2004. Disponível em: <https://openknowledge.worldbank.org/handle/10986/14439>.

INDURKHYA, N.; DAMERAU, F. J. **Handbook of Natural Language Processing**. 2nd. ed. [S.l.]: Chapman amp; Hall/CRC, 2010. ISBN 1420085921.

KANCZUK, D. **O que são microsserviços e como funcionam?** 2020. Disponível em: <https://blog.geekhunter.com.br/arquitetura-de-microsservicos-x-arquitetura-monolitica/>. Acesso em: 07 jun. 2022.

KLEINA, N. **Android 11 é a versão mais usada do sistema do Google em 2022**. 2022. Disponível em: <https://www.tecmundo.com.br/software/239024-android-11-versao-usada-sistema-do-google-2022.htm>. Acesso em: 02 jul. 2022.

KRITZINGER, E.; SMITH, E. Information security management: An information security retrieval and awareness model for industry. **Computers Security**, v. 27, n. 5, p. 224–231, 2008. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404808000321>.

LEITE, G. **O que é JSON?** 2020. Disponível em: <https://www.alura.com.br/artigos/o-que-e-json>. Acesso em: 29 jun. 2022.

LEITE, V. **O que é um Banco Digital? Qual a diferença para um banco tradicional?** 2019. Disponível em: <https://blog.nubank.com.br/banco-digital-o-que-e/>. Acesso em: 29 nov. 2021.

LI, F.; LU, H.; HOU, M.; CUI, K.; DARBANDI, M. Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. **Technology in Society**, v. 64, p. 101487, 2021. ISSN 0160-791X. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0160791X20312902>.

LIMA, C. **O que é o Spring Boot?** 2021. Disponível em: <https://www.treinaweb.com.br/blog/o-que-e-o-spring-boot>. Acesso em: 07 jun. 2022.

LIMA, M. de; LINHARES, T. **PLN – Processamento de Linguagem Natural para Iniciantes**. 2021. Disponível em: <https://insightlab.ufc.br/pln-processamento-de-linguagem-natural-para-iniciantes>. Acesso em: 03 jul. 2022.

MENDES, M. S. **MALTU - Um modelo para avaliação da interação em sistemas sociais a partir da linguagem textual do usuário.** Tese (Doutorado em Ciência da Computação) — Universidade Federal do Ceará (UFC), Fortaleza, 2015.

MONTINI, A. **Digitalização dos bancos: quais são as tendências e os desafios?** 2021. Disponível em: <https://noomis.febraban.org.br/especialista/alessandra-montini/digitalizacao-dos-bancos-quais-sao-as-tendencias-e-os-desafios>. Acesso em: 08 jun. 2022.

MTAMBALIKA, A.; MANDA, T. D.; GOMBACHIKA, H.; KUNYENJE, G. Branchless banking in rural malawi: Potential customers' perspective on bank-led mobile banking. In: **2016 IST-Africa Week Conference**. [S.l.: s.n.], 2016. p. 1–11.

NOURALLAH, M.; STRANDBERG, C.; ÖHMAN, P. Understanding the relationship between trust and satisfaction on mobile bank application. In: **Proceedings of the 2019 3rd International Conference on E-Commerce, E-Business and E-Government**. New York, NY, USA: Association for Computing Machinery, 2019. (ICEEG 2019), p. 58–61. ISBN 9781450362375. Disponível em: <https://doi.org/10.1145/3340017.3340033>.

OUTEIRO, A. de S.; SANTOS, P. dos. **Liberdade financeira ao alcance de todos.** [S.l.]: Brasil: Editora Senac São Paulo, 2019.

PALMER, D. D. **Text preprocessing**. 2. ed. [S.l.]: Chapman and Hall/CRC, 2010.

PEREIRA, R. **Bancos digitais aumentam presença no Brasil durante pandemia**. 2021. Disponível em: <https://economia.uol.com.br/noticias/estadao-conteudo/2021/01/10/brasileiros-se-voltam-para-bancos-digitais.htm>. Acesso em: 18 dez. 2021.

PINHEIRO, N. **Introdução ao Processamento de Linguagem Natural — Natural Language Processing(NLP)**. 2021. Disponível em: <https://medium.com/data-hackers/introdu\%C3\%A7\%C3\%A3o-ao-processamento-de-linguagem-natural-natural-language-processing-nlp-be907cd06c71>. Acesso em: 12 jun. 2022.

POON, W. Users adoption of e-banking services: the malaysian perspective. In: **Proceedings of the 2019 3rd International Conference on E-Commerce, E-Business and E-Government**. New York, NY, USA: [s.n.], 2008. (ICEEG 2019), p. 58–61. Disponível em: <https://doi.org/10.1145/3340017.3340033>.

REZENDE, S. O.; MARCACINI, R. M.; MOURA, M. F. O uso da mineração de textos para extração e organização não supervisionada de conhecimento. **Revista de Sistemas de Informação da FSMA**, v. 7, p. 7–21, 2011. ISSN 19835604. Disponível em: <http://www.fsma.edu.br/si/7edicao.html>.

ROCHA, L. **A importância do suporte à Query Strings em uma API REST**. 2021. Disponível em: <https://www.linkedin.com/pulse/import\%C3\%A2ncia-do-suporte-\%C3\%A0-query-strings-em-uma-api-rest-lucas-rocha/?originalSubdomain=pt>. Acesso em: 04 jun. 2022.

RODRIGUES, J. **O que é o Processamento de Linguagem Natural?** 2017. Disponível em: <https://medium.com/botsbrasil/o-que-\%C3\%A9-o-processamento-de-linguagem-natural-49ece9371cff>. Acesso em: 12 jun. 2022.

SCACCIA, K. **Pré-processamento de Texto para NLP e Fundamentos**. 2022. Disponível em: <https://dataml.com.br/pre-processamento-de-texto-para-nlp-e-fundamentos/>. Acesso em: 12 jun. 2022.

SHAIKH, A. A.; KARJALUOTO, H. The effects of mobile banking application user satisfaction and system usage on bank-customer relationships. In: **Proceedings of the 20th International Academic Mindtrek Conference**. New York, NY, USA: Association for Computing Machinery, 2016. (AcademicMindtrek '16), p. 177–183. ISBN 9781450343671. Disponível em: <https://doi.org/10.1145/2994310.2994330>.

SILVA, P. B. d. S.; SILVA, T. H. O. d.; MENDES, M. S.; FURTADO, M. E. S. Temporal analysis of posts related to use: Case study of use of an academic management system. In: **Proceedings of the 18th Brazilian Symposium on Human Factors in Computing Systems**. New York, NY, USA: Association for Computing Machinery, 2019. (IHC '19). ISBN 9781450369718. Disponível em: <https://doi.org/10.1145/3357155.3358482>.

SOARES, H.; MACHADO, R.; SALGADO, B.; SOARES, R.; CARDOSO, J. L.; COSTA, L. F. Information security aspects of public software. In: **Proceedings of the Fifth International Conference on Management of Emergent Digital EcoSystems**. New York, NY, USA: Association for Computing Machinery, 2013. (MEDES '13), p. 336–339. ISBN 9781450320047. Disponível em: <https://doi.org/10.1145/2536146.2536190>.

WEERASINGHE, D.; RAKOCEVIC, V.; RAJARAJAN, M. Security framework for mobile banking. In: **Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia**. New York, NY, USA: Association for Computing Machinery, 2010. (MoMM '10), p. 421–424. ISBN 9781450304405. Disponível em: <https://doi.org/10.1145/1971519.1971591>.

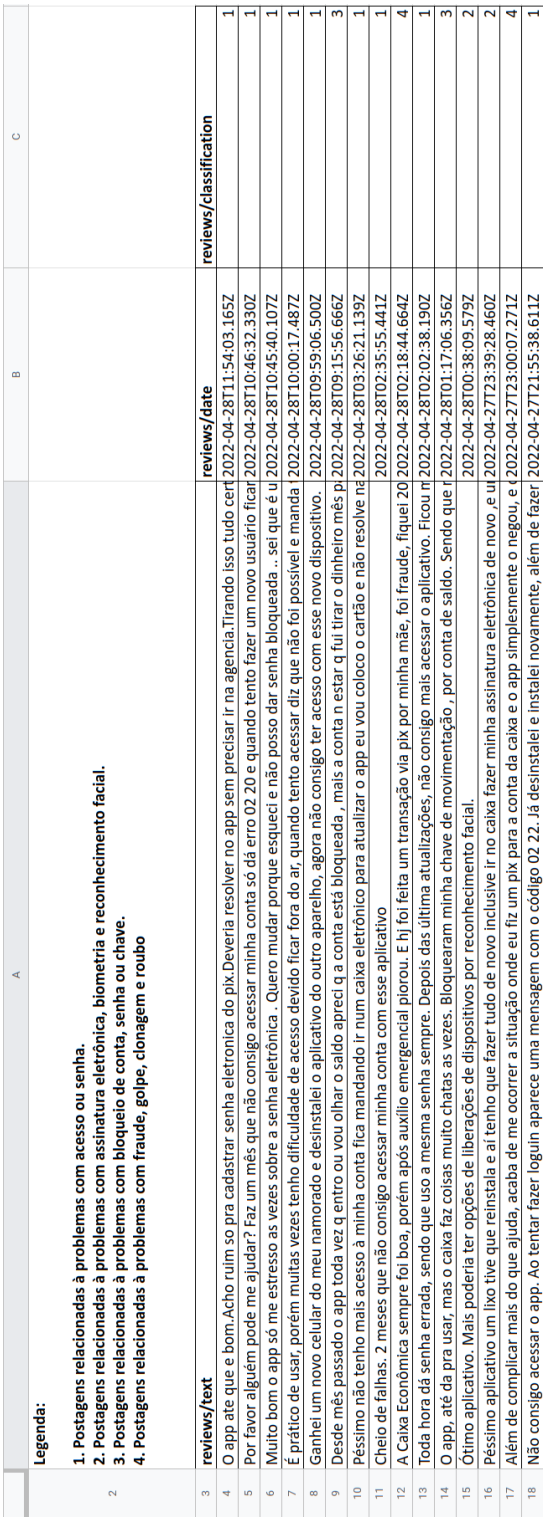
YILDIRIM, N.; VAROL, A. A research on security vulnerabilities in online and mobile banking systems. In: **2019 7th International Symposium on Digital Forensics and Security (ISDFS)**. [S.l.: s.n.], 2019. p. 1–5.

YOON, H. S.; Barker Steege, L. M. Development of a quantitative model of the impact of customers' personality and perceptions on internet banking use. **Computers in Human Behavior**, v. 29, n. 3, p. 1133–1141, 2013. ISSN 0747-5632. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0747563212002737>.

ZOMAI, M. A.; ALFAYYADH, B.; JØSANG, A.; MCCULLAGH, A. An experimental investigation of the usability of transaction authorization in online bank security systems. In: **AISC**. [S.l.: s.n.], 2008.

ZURIARRAIN, J. M. **Android já é o sistema operacional mais usado do mundo**. 2017. Disponível em: <https://brasil.elpais.com/brasil/2017/04/04/tecnologia/1491296467_396232.html>. Acesso em: 02 jul. 2022.

APÊNDICE A – CLASSIFICAÇÃO DAS POSTAGENS DA GOOGLE PLAY STORE



	A	B	C
2	**Legenda:** **1. Postagens relacionadas à problemas com acesso ou senha.** **2. Postagens relacionadas à problemas com assinatura eletrônica, biometria e reconhecimento facial.** **3. Postagens relacionadas à problemas com bloqueio de conta, senha ou chave.** **4. Postagens relacionadas à problemas com fraude, golpe, clonagem e roubo**		
3	**reviews/text**	**reviews/date**	**reviews/classification**
4	O app ate que e bom.Acho ruim so pra cadastrar senha eletronica do pix.Deveria resolver no app sem precisar ir na agencia.Tirando isso tudo cert	2022-04-28T11:54:03.165Z	1
5	Por favor alguém pode me ajudar? Faz um mês que não consigo acessar minha conta só dá erro 02 20 e quando tento fazer um novo usuário ficar	2022-04-28T10:46:32.330Z	1
6	Muito bom o app só me estresso as vezes sobre a senha eletrônica . Quero mudar porque esqueci e não posso dar senha bloqueada .. sei que é u	2022-04-28T10:45:40.107Z	1
7	É prático de usar, porém muitas vezes tenho dificuldade de acesso devido ficar fora do ar, quando tento acessar diz que não foi possível e manda t	2022-04-28T10:00:17.487Z	1
8	Ganhei um novo celular do meu namorado e desinstalei o aplicativo do outro aparelho, agora não consigo ter acesso com esse novo dispositivo.	2022-04-28T09:59:06.500Z	1
9	Desde mês passado o app toda vez q entro ou vou olhar o saldo apreci q a conta está bloqueada , mais a conta n estar q fui tirar o dinheiro mês p	2022-04-28T09:15:56.666Z	3
10	Péssimo não tenho mais acesso à minha conta fica mandando ir num caixa eletrônico para atualizar o app eu vou coloco o cartão e não resolve na	2022-04-28T03:26:21.139Z	1
11	Cheio de falhas. 2 meses que não consigo acessar minha conta com esse aplicativo	2022-04-28T02:35:55.441Z	1
12	A Caixa Econômica sempre foi boa, porém após auxílio emergencial piorou. E hj foi feita um transação via pix por minha mãe, foi fraude, fiquei 20	2022-04-28T02:18:44.664Z	4
13	Toda hora dá senha errada, sendo que uso a mesma senha sempre. Depois das última atualizações, não consigo mais acessar o aplicativo. Ficou m	2022-04-28T02:02:38.190Z	1
14	O app, até da pra usar, mas o caixa faz coisas muito chatas as vezes. Bloquearam minha chave de movimentação , por conta de saldo. Sendo que r	2022-04-28T01:17:06.356Z	3
15	Ótimo aplicativo. Mais poderia ter opções de liberações de dispositivos por reconhecimento facial.	2022-04-28T00:38:09.579Z	2
16	Péssimo aplicativo um lixo tive que reinstala e ai tenho que fazer tudo de novo inclusive ir no caixa fazer minha assinatura eletrônica de novo ,e u	2022-04-27T23:39:28.460Z	2
17	Além de complicar mais do que ajuda, acaba de me ocorrer a situação onde eu fiz um pix para a conta da caixa e o app simplesmente o negou, e (	2022-04-27T23:00:07.271Z	4
18	Não consigo acessar o app. Ao tentar fazer loguin aparece uma mensagem com o código 02 22. Já desinstalei e instalei novamente, além de fazer	2022-04-27T21:55:38.611Z	1

Fonte: elaborado pelo autor (2022).

APÊNDICE B – EXEMPLOS DE POSTAGENS DOS USUÁRIOS

Fonte: elaborado pelo autor (2022).