# Desmistificando Fraudes: Análise de Dados e Tecnologia na Plataforma Beware para uma Defesa Eficaz

**Jéssica De Oliveira Pontes[1], Laiane Cristina De Souza[1], Rosemeiry De Castro Prado[1], Robson Parmezan Bonidia[2]**

[1] Departamento de Ciência de Dados – Faculdade de Tecnologia de Ourinhos
Av. Vitalina Marcusso, 1440, Campus Universitario – Ourinhos – SP – Brasil,

***Abstract.*** *Every year, millions fall victim to fraudulent actions and scams in the digital world. These deceptive strategies involve extensive tactics, including email phishing, spoofed online advertisements, and enhanced financial fraud. Taking advantage of the naivety, ignorance, or even unjustified self-confidence of their targets, scammers commit their criminal acts. In an interest to resolve this issue, the development of the Beware platform emerged. Its main objective is to provide users with knowledge and clarification on the numerous forms of fraud and major scams. This platform allows users to share their accounts of fraud and express their frustrations while collecting data for accurate analysis. In addition, the platform generates a dashboard that highlights the main fraud categories, the gender most vulnerable to scams, the affected age group, and the geographic distribution of fraudulent activities throughout Brazil. The work developed serves both as a practical tool for individuals to protect themselves against fraud and to obtain a broader knowledge of this issue, allowing the identification of areas with greater vulnerability and the adoption of preventive measures with greater results.*

***Resumo.*** *Todos os anos, milhões de pessoas são vítimas de ações fraudulentas e golpes que ocorrem no mundo digital. Essas estratégias enganosas envolvem uma extensa série de táticas, incluindo phishing por e-mail, anúncios on-line falsificados e fraudes financeiras aprimoradas. Aproveitando a ingenuidade, a ignorância ou mesmo a autoconfiança injustificada dos seus alvos, os golpistas cometem os seus atos criminosos. Num interesse para resolver esta questão, surgiu o desenvolvimento da plataforma Beware. Seu objetivo principal é fornecer aos usuários conhecimento e esclarecimentos sobre as inúmeras formas de fraude e golpes principais. Esta plataforma permite aos usuários compartilharem seus relatos pessoais com fraudes, bem como expressar suas frustrações, ao mesmo tempo em que coletam dados para uma análise precisa. Além disso, a plataforma gera um dashboard que aponta as categorias de fraude principais, o gênero mais vulnerável a golpes, a faixa etária afetada e a distribuição geográfica de atividades fraudulentas em todo o Brasil. O trabalho desenvolvido serve tanto como uma ferramenta prática para os indivíduos se protegerem contra a fraude, como um meio para obter um conhecimento mais amplo desta questão, permitindo a identificação de áreas com maior vulnerabilidade e a adoção de medidas preventivas com mais resultados.*

## 1. Introdução

O Brasil está entre os países com os maiores índices de risco de fraude, conforme o relatório recente da Visa referente a 2023. A partir da análise de mais de 2,7 bilhões de

transações realizadas globalmente pela Visa, somando um total de US$ 381 bilhões, o estudo revela que o índice de risco de fraude no Brasil alcançou 14,24%. Esse valor coloca o país logo atrás da China, que registrou um índice de 14,93% [VEJA, 2023].

No primeiro trimestre de 2023, ocorreram mais de 2,8 mil tentativas de fraudes financeiras por minuto em canais eletrônicos no Brasil. Isso equivale a aproximadamente 365 milhões de tentativas de golpes no mesmo período [ESTADAO, 2023]. No Brasil, segundo pesquisa realizada pela Federação Brasileira de Bancos [FEBRABAN 2012], de cada R$ 100,00 (cem reais) roubados de bancos, pelo menos R$ 95,00 (noventa e cinco reais) são de fraudes eletrônicos, realizadas por cartões ou internet banking [Beraldi (2014)]. A prioridade de proteger os consumidores de práticas enganosas torna-se cada vez mais crucial no panorama digital atual, onde a acessibilidade da informação coincide com o aumento de fraudes sofisticadas. Para resolver esta questão, a incorporação de tecnologias de ponta e estratégias assume um papel fundamental na minimização destes perigos potenciais. As fraudes não se restringem a transações financeiras; elas também ocorrem no consumo de energia, na aquisição de produtos, na utilização de benefícios sociais, no acesso a redes de computadores e até mesmo em transações contábeis para distorcer os resultados financeiros [Martins and Verardi Galegale (2022)].

Esse evento é devido ao crescimento exponencial das novas tecnologias e dispositivos como: smartphones, e-commerce, pagamentos sem contato, crimes cibernéticos – incluindo grandes violações de dados, computação em nuvem e moedas virtuais. À medida que o crime migra devido a essas tecnologias, isso ocorrerá mais rapidamente do que no passado, devido às novas tecnologias envolvidas. As formas tradicionais de fraude estão dando lugar a criminosos altamente versados em informática, os quais vivem em uma época de alta comunicação de tecnologia, com um estilo de vida voltado para a tecnologia e com uso intensivo das redes sociais [Martins and Verardi Galegale 2022]. Essas inovações transferiram o poder dos bancos para os consumidores, tornando as transações de compra e transferência mais descentralizadas e acessíveis ao público. No entanto, também aumentaram a vulnerabilidade a fraudes [Pereira and Murai 2021].

Como diz Smith (2020), a integração de tecnologias emergentes e abordagens inovadoras desempenha um papel fundamental na mitigação dos riscos de fraudes online, podendo estas encontrar na educação uma solução abrangente para resolver a questão das fraudes, com foco na prevenção e na apropriação de conhecimentos que caminhem de encontro aos possíveis crimes.

Logo, ao aproveitar os recursos do *Botpress*, uma plataforma para desenvolvimento de *chatbots*, um ambiente interativo foi desenvolvido. Esse ambiente permite que os usuários busquem esclarecimentos, acessem informações pertinentes e troquem suas experiências pessoais com atividades fraudulentas. Esta solução incorpora diversas tecnologias e ferramentas de automação para fornecer uma abordagem abarcante.

Além de aproveitar a inteligência artificial ChatGPT3.5 para respostas precisas e atualizadas, o *Botpress* também incorporou uma base de conhecimento enriquecida com varreduras de sites públicos, onde o assistente virtual coleta e registra depoimentos de vivências pessoais com fraudes, incluindo dados demográficos como gênero, idade, categoria da fraude e localização geográfica.

A automação desempenha um papel crucial nesse procedimento, sendo que o *Botpress* automatiza a transferência desses depoimentos para o *Google Sheets*, onde são centralizados e organizados para análises posteriores. Além disso, a criação de um painel interativo utilizando o *Google Looker* facilita a visualização e exploração dos dados recolhidos, proporcionando valiosas reflexões sobre padrões e tendências associadas às fraudes.

Conforme sugerido por Johnson et al. (2018), a análise de sentimentos e o processamento de linguagem natural são essenciais para compreender as experiências dos usuários em relação a fraudes e golpes. Sendo esse, em uma extensão do projeto para futuras análises.

Essas ferramentas e abordagens, como destacado por Brown (2019), representam uma contribuição significativa para a conscientização e proteção dos consumidores contra fraudes e golpes online.

Este estudo representa uma colaboração para alertar e proteger os usuários contra esquemas fraudulentos, ao mesmo tempo que ilustra o potencial das tecnologias emergentes na abordagem desse desafio crescente e complexo. Além disso, procura-se trazer uma abordagem democrática em relação ao uso da ferramenta, de modo a socializá-la com todos cidadãos.

## 2. Trabalhos Relacionados

Durante uma pesquisa, foi identificado o Catálogo de Fraudes da Rede Nacional de Ensino e Pesquisa (RNP), lançado pelo Centro de Atendimento a Incidentes de Segurança [CAIS 2008] e atualmente mantido em parceria com o PoP-BA/RNP. Este catálogo tem como objetivo conscientizar a comunidade sobre os principais golpes em circulação na internet, identificando e divulgando fraudes reportadas pela comunidade ou detectadas por seus sensores.

Funcionando como um repositório de mensagens classificadas como fraudulentas, o catálogo serve como uma fonte de informação crucial para evitar a propagação de fraudes disseminadas por e-mail, além de fornecer orientações sobre como se proteger desses tipos de golpes. Para reportar uma mensagem suspeita ou fraudulenta, deve-se encaminhá-la para phishing@cais.rnp.br.

Em uma análise mais ampla do combate às fraudes digitais, foi encontrada uma forte relação com a plataforma Beware. Dedicada à análise e prevenção de fraudes, a plataforma Beware complementa as iniciativas do Catálogo de Fraudes da RNP ao

fornecer uma plataforma para a identificação de padrões de comportamento fraudulentos e métodos de proteção.

Ambos os recursos enfatizam a importância da conscientização e da educação na prevenção de fraudes. Assim, as práticas recomendadas pela Beware reforçam as diretrizes oferecidas pelo Catálogo de Fraudes, formando uma abordagem coesa e robusta contra fraudes digitais.

Foi identificado também, um estudo sobre golpes digitais e conscientização, realizado por Valério et al. (2023) que aborda o uso da gamificação como uma estratégia eficaz de conscientização sobre golpes digitais e seus padrões. Esse estudo investiga iniciativas anteriores que empregaram a gamificação na educação sobre segurança cibernética, utilizando plataformas como Kahoot! e o jogo Capture the Flag (CTF). Utilizando a metodologia de Pesquisa em Ciência do Design (Design Science Research - DSR), o estudo identificou cinco categorias comuns de golpes digitais e desenvolveu questionários na plataforma *QuizMaker* para instruir o público sobre esses golpes. A avaliação da eficácia desses questionários destacou áreas que poderiam ser aprimoradas, ressaltando a importância de revisões contínuas e do desenvolvimento de novos recursos educativos

Ambos os estudos têm como objetivo utilizar tecnologias avançadas para educar e proteger os usuários contra fraudes digitais, embora adotem abordagens distintas. O primeiro projeto, centrado na gamificação, desenvolve *quizzes* para conscientização sobre segurança cibernética, com base em tipos comuns de fraudes. Já a plataforma Beware integra diversas tecnologias para criar um ambiente interativo e automatizado, permitindo que os usuários relatem, consultem e aprendam sobre fraudes digitais. Utilizando *chatbots* e análises de dados, a Beware fornece informações em tempo real e insights sobre atividades fraudulentas, contribuindo para decisões estratégicas mais informadas.

## 3. Desenvolvimento

O desenvolvimento da plataforma Beware é uma iniciativa estratégica e multifacetada para abordar de forma abrangente e proativa a crescente ameaça de fraudes e golpes online. Logo, foi utlizada a linguagem de programação JavaScript para automatizar integrações com outras plataformas, como *Google Sheets* e *Google Looker,* também interligando processos de desenvolvimento dentro do *Botpress*. Conforme destacado por Smith (2021), a automação de processos com JavaScript permite uma integração eficiente e robusta entre diferentes plataformas, melhorando significativamente a funcionalidade e a usabilidade de sistemas complexos.

### 3.1. Visão e Plano: A visão da plataforma

O Beware começou com uma análise aprofundada do cenário atual de fraudes e golpes online. Com base em pesquisas relevantes, foram identificadas lacunas significativas na capacidade dos consumidores de se protegerem contra estes ataques. O objetivo da

ferramenta era criar uma solução abrangente que fornecesse aos usuários conhecimento, educação e práticas para combater diversas formas de fraude.

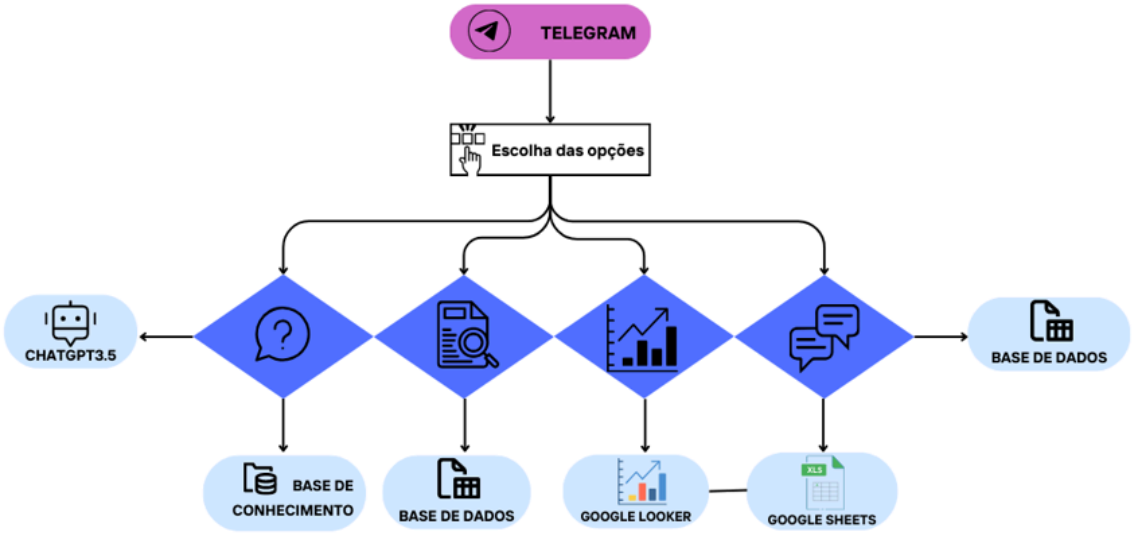


**Figura 1. Pipeline do processo do Beware. Fonte: Elaborado pelo Autor**.

## 3.2. O Botpress

O desenvolvimento da plataforma envolveu a utilização do *Botpress*, uma avançada ferramenta de criação de *chatbots*. Integrando essa tecnologia, criou-se um ambiente interativo que oferece diversas opções aos usuários. Eles podem escolher entre registrar relatos, consultar relatos de outros usuários, acessar o dashboard para visualizar interações no *chatbot* e esclarecer dúvidas sobre fraudes.

### 3.2.1. Realizar relato

A plataforma oferece uma funcionalidade para que os usuários possam compartilhar relatos detalhados sobre fraudes ou práticas enganosas das quais tenham sido vítimas ou tenham conhecimento. Ao enviar um relato, o usuário deve fornecer informações específicas, incluindo a descrição do tipo de fraude ou prática enganosa, estado ou região onde o incidente ocorreu, idade e gênero do usuário que está submetendo o relato. Esses dados são essenciais para que a plataforma possa realizar análises detalhadas e identificar padrões, tais como: identificar quais estados ou regiões são mais afetados por determinadas fraudes, analisar quais faixas etárias e gêneros são mais frequentemente alvo de práticas enganosas. Além disso, a coleta dessas informações contribui para a criação de relatórios e estatísticas que podem ser utilizados por autoridades competentes e instituições de proteção ao consumidor para desenvolver estratégias mais eficazes de combate a fraudes.

### 3.2.2. Base de Conhecimento e ChatGPT3.5

O *Botpress* permite incorporar uma base de conhecimento para automatizar a extração de dados de páginas da *web*, utilizando a técnica de web *scraping*. Esta técnica envolve a pesquisa e a coleta de informações dessas páginas, transformando os dados em formatos estruturados para responder eficientemente às perguntas dos usuários [Silva et al. 2021]. Além disso, é possível criar documentos em PDF*(Portable Document Format)* com estruturas de dados que o *chatbot* pode consultar para responder aos usuários. Foi o caso deste projeto, no qual foi criada uma base de dados em PDF*(Portable Document Format)* contendo informações e dicas da Federação Brasileira de Bancos (FEBRABAN). Caso a resposta não seja encontrada inicialmente, o sistema recorre à inteligência artificial do ChatGPT-3.5. Um aspecto fundamental para obter uma resposta satisfatória é formular a pergunta de forma precisa [Sant´Ana 2023].

### 3.2.3. Consulta de outros relatos

Ao interagir com o *chatbot*, o usuário tem como opção visualizar relatos de outros usuários. O *Botpress* possui uma base de dados própria que armazena esses relatos, permitindo que os usuários consultem informações sobre fraudes em diversas categorias. Dessa forma, é possível comparar situações, se informar sobre fraudes recentes, obter respostas precisas e atualizadas, buscar esclarecimentos, acessar informações relevantes.

### 3.2.4. Automação e Google Sheets

A automação é um componente vital da plataforma, simplificando o processo de transferência e organização de depoimentos de usuários no Planilhas Google. O Google Planilhas é reconhecido pela sua simplicidade e atualização em tempo real. Ele se atualiza automaticamente quando os usuários interagem com o *chatbot*, mantendo um registro das alterações [Rebman Jr. et al. 2023]. Essa abordagem facilita a análise dos dados coletados para identificar padrões e tendências, incluindo atividades fraudulentas.

### 3.2.5. Painel Interativo e Google Looker

O *Google Looker* é uma plataforma inovadora de análise de dados que oferece recursos interativos e informativos de visualização. Ele proporciona uma compreensão abrangente e precisa das informações coletadas, facilitando a descoberta de *insights*

valiosos relacionados às atividades fraudulentas. Além disso, o *Google Looker Studio* permite gerenciar, analisar e apresentar informações operacionais de forma visual e em tempo real, contribuindo para uma melhor tomada de decisão e resposta mais ágil [Asher and Rachmawati 2024].

## 4. A Integração com Telegram

A eficácia e a funcionalidade da plataforma *Beware* dependem significativamente da integração com serviços como *Telegram*. Esse componente é essencial para facilitar a coleta, organização e análise de dados, garantindo uma experiência de usuário perfeita em diversas plataformas e ferramentas de análise. Conforme destacado por Johnson (2022), a integração de múltiplos serviços de comunicação é crucial para a centralização e eficiência na gestão de dados complexos.

O Telegram é uma plataforma de troca de mensagens em tempo real e para a escolha do uso do telegrama como um elemento interativo, os seguintes parâmetros foram considerados: gratuidade, ferramentas e flexibilidade para a programação de *chatbots.*

A integração do *Botpress* com o Telegram é relativamente direta e envolve alguns passos básicos, enumerados a seguir:

### 4.1. Criação de um Bot no Telegram

Primeiro, torna-se necessário criar um *bot* no Telegram para que haja a interação com o *BotFather*bot (*bot* oficial do Telegram) para criar e gerenciar *bots*. Basta iniciar uma conversa com o *BotFather* e seguir as instruções para criar o *bot,* recebendo um *token* de acesso.

### 4.2. Instalação do módulo do Telegram no Botpress

No *Botpress*, é preciso habilitar a integração. Após habilitado, passa-se o *token* do *bot,* obtido do *BotFather.*

### 4.3. Teste e Integração:

Depois da configuração pronta, realiza-se o teste para a verificação da integração. Assim, envia-se uma mensagem para o *bot* que é criado no Telegram, verificado se o *Botpress* está recebendo e respondendo às mensagens corretamente. Uma vez configurada e testada, a integração permitirá criar e gerenciar fluxos de conversa no *Botpress.*

## 5. Análise de dados e Insights

*O Botpress* conta também com um recurso importante: o *Analytics*, uma ferramenta que fornece *insights* valiosos sobre o desempenho e a interação do *bot* com os usuários. Ele permite monitorar e analisar diversos aspectos do comportamento do *bot*, ajudando a entender melhor como os usuários estão interagindo e identificando as áreas para as melhorias.

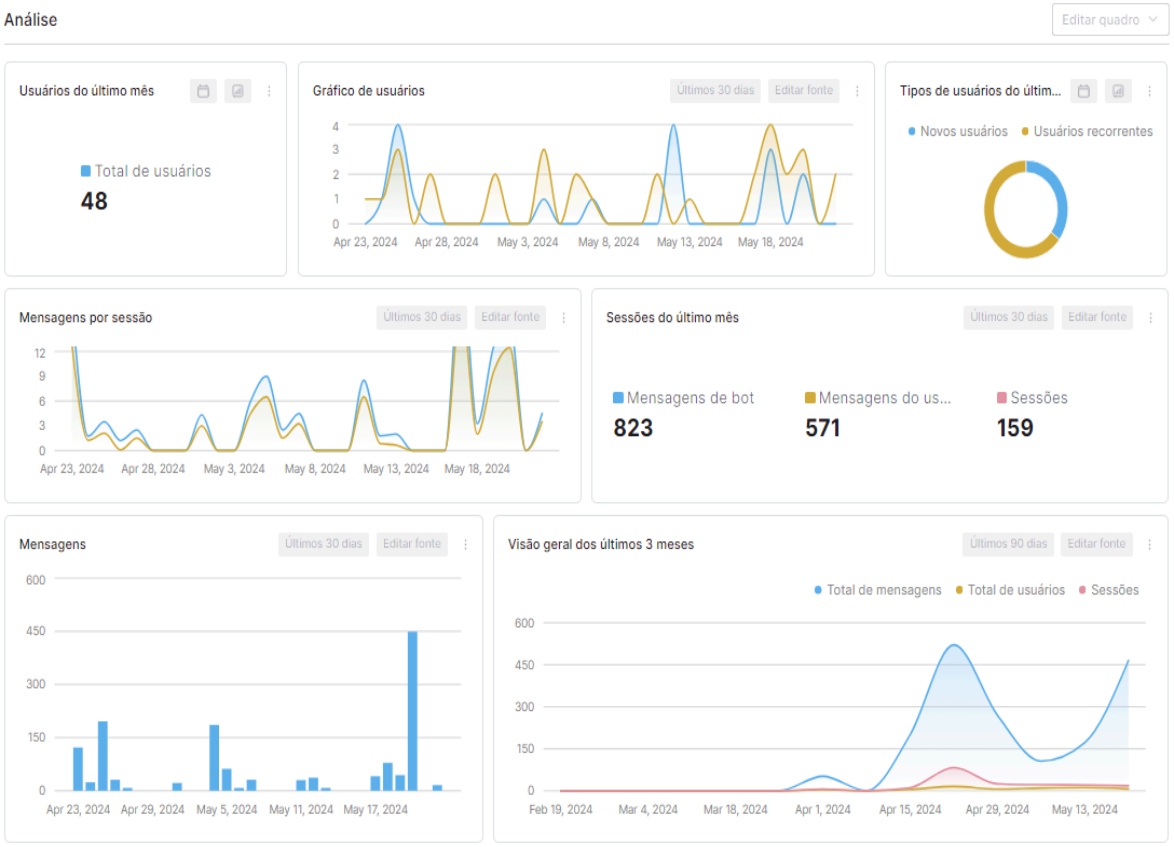


**Figura 2. Interface do Analytics no Botpress do projeto Beware. Fonte: Elaborado pelo autor.**

## 5.1. Dados de Engajamento

O *Analytics* do *Botpress* coleta informações sobre o engajamento dos usuários com o *bot*, incluindo o número de mensagens enviadas e recebidas, conversas iniciadas e finalizadas, e o tempo médio de interação. Essas métricas são cruciais para avaliar o nível de atividade e interesse dos usuários no bot.

## 5.2. Fluxo de Conversa

A ferramenta acompanha o fluxo de conversa dos usuários, permitindo visualizar a trajetória que eles percorrem durante a interação. Essa funcionalidade é essencial para identificar padrões de comportamento e compreender como os usuários estão navegando pelo *bot*.

## 5.3. Análise de Intenções e Entidades

O *Analytics* do *Botpress* analisa as intenções e entidades detectadas durante as conversas. Isso oferece *insights* sobre os temas mais discutidos e as necessidades dos usuários, possibilitando a personalização e otimização das respostas do *bot.*

### 5.4. Acompanhamento de Metas e Conversões

Os usuários podem definir metas específicas para o *bot*, como a conclusão de um pedido ou preenchimento de formulário, e monitorar o progresso em direção a essas metas usando o *Analytics* do *Botpress*. Essa funcionalidade é fundamental para medir o sucesso do *bot* em alcançar seus objetivos e identificar áreas para melhorias.

### 5.5. Visualização de Dados

Por fim, o *Analytics* do *Botpress* oferece diversas ferramentas de visualização de dados, como gráficos e tabelas, facilitando a interpretação dos dados coletados. Isso permite identificar tendências e padrões rapidamente, auxiliando na tomada de decisões embasadas nos dados obtidos.

## 6. Resultados

## 6.1. Interface

A plataforma Beware utiliza a interface do Telegram devido à sua robusta integração, proporcionando uma experiência de usuário fluida e eficiente. A escolha do Telegram permite que os usuários interajam facilmente com a plataforma, beneficiando-se de uma comunicação rápida e segura.

A conversa começa de maneira simples: o usuário envia uma mensagem de saudação ou um comando específico para o *chatbot,* que então oferece várias opções, como registrar um relato, consultar relatos existentes, ou obter informações sobre Fraudes.

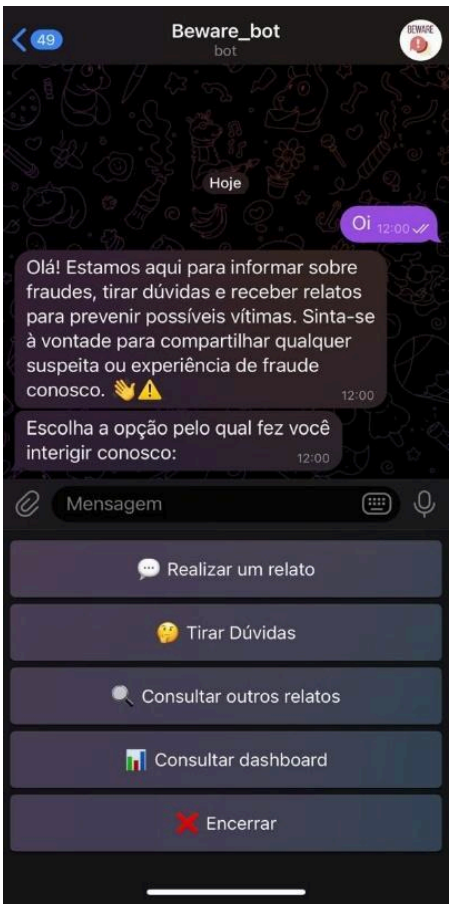


**Figura 3. Interface do chatbot ao interagir. Fonte: Elaborado pelo autor**

Essa integração facilita a coleta, organização e análise de dados, garantindo que os usuários possam acessar informações relevantes e compartilhar experiências de forma prática e intuitiva. A integração com plataformas de comunicação populares como o Telegram é essencial para aumentar a acessibilidade e a eficiência dos serviços digitais [Brown 2023].

## 6.2. Beware

A crescente ameaça de fraudes e golpes online levou ao desenvolvimento da plataforma Beware, uma solução inovadora para ajudar usuários a identificar, relatar e consultar informações sobre fraudes. Este estudo examina a criação, implementação e impacto da Beware, destacando suas funcionalidades principais e a experiência dos usuários.

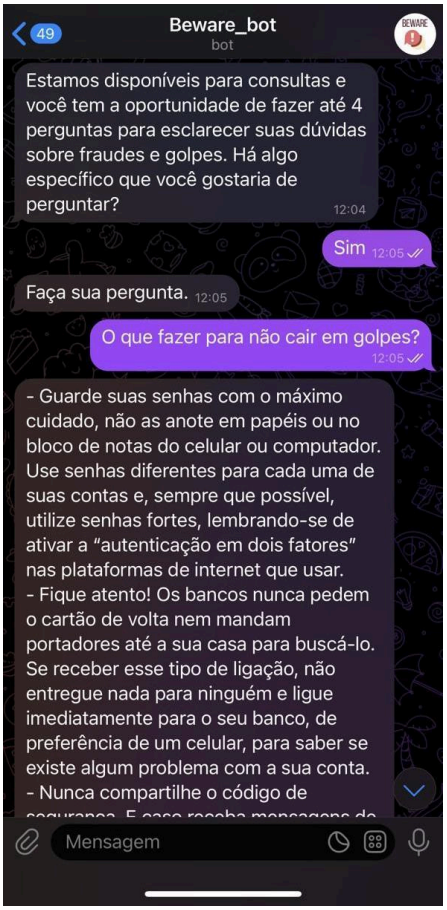


**Figura 4. Interface do chatbot ao obter resposta de alguma dúvida. Fonte: Elaborado pelo autor**

A utilização da Beware demonstrou diversos benefícios, como maior engajamento dos usuários devido à integração com o Telegram, eficiente coleta e organização de dados sobre fraudes, e aumento da conscientização dos usuários sobre ameaças, melhorando sua capacidade de evitá-las. A eficácia da Beware é atribuída à sua integração com plataformas de comunicação populares, que melhora a confiabilidade e eficiência das soluções de combate a fraudes, resultando em maior participação e *feedback* positivo.

## 6.3. Dashboard Beware

O *dashboard* foi criado no *Google Looker Studio*, onde os relatos direcionados para o *Google Sheets* são integrados a este painel interativo para análise de dados. Foram utilizadas diferentes visualizações gráficas para apresentar os dados dos usuários:

1. Origem dos Usuários por Regiões do Brasil: Gráfico de barras mostrando a quantidade de usuários por região.

2. Faixa Etária: Gráfico de barras exibindo a distribuição dos usuários por faixas etárias.
3. Gênero: Gráfico de rosca representando a proporção de usuários por gênero.
4. Categoria da Fraude: Gráfico de rosca ilustrando as diferentes categorias de fraudes detectadas.
5. Quantidade de Interações até o Momento: Contador numérico mostrando a evolução das interações ao longo do tempo.

Essas visualizações facilitam a análise detalhada dos dados dos usuários. Com esses dados, outros usuários podem obter uma visão mais abrangente sobre a expansão das fraudes, fornecendo insights valiosos para que as empresas tomem medidas adequadas em resposta a esses fatos.

A interatividade do dashboard permite que as informações sejam atualizadas em tempo real, possibilitando uma rápida identificação de padrões emergentes e mudanças nas tendências.

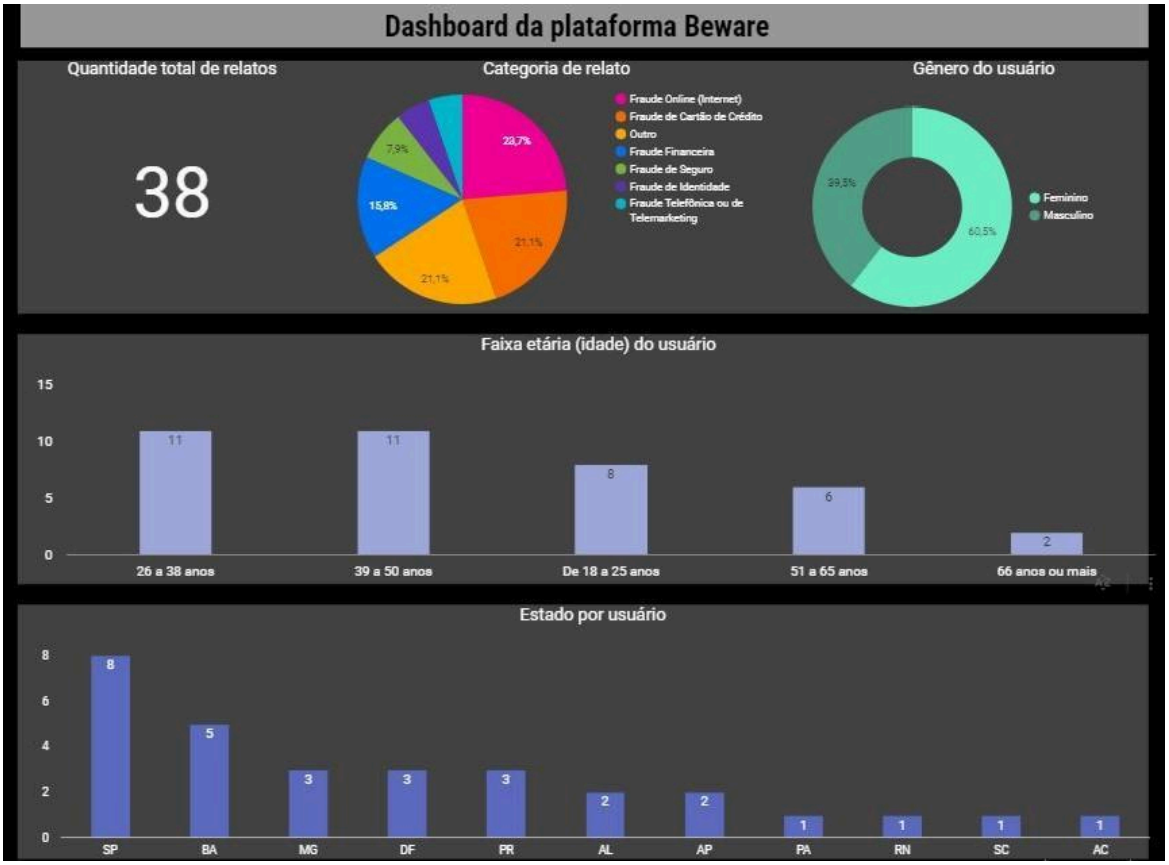


**Figura 5. Análise de interação pelo Google Looker. Fonte: Elaborado pelo Autor**

Essa capacidade de monitoramento dinâmico é essencial para antecipar e mitigar novas ameaças, além de permitir uma resposta proativa e mais eficaz. Dessa forma, o painel não só facilita a compreensão dos dados, mas também otimiza a tomada de decisões estratégicas. Uma das principais funcionalidades do dashboard é atuar como um recurso para a tomada de decisões. Ao exibir informações essenciais de maneira transparente e de fácil assimilação, os dashboards capacitam gestores e responsáveis pela tomada de decisões a reconhecer os pontos críticos, permitindo decisões mais bem fundamentadas e estratégicas (de Góis Silva).

### 6.4. Plataforma Beware: Onde Encontrá-la

O acesso à plataforma Beware ocorrerá por meio do Telegram, onde os usuários poderão interagir com o @Beware_chatBot.

## 7. Conclusão

A crescente ameaça de fraudes e golpes online exige soluções inovadoras e abrangentes. A plataforma Beware foi desenvolvida para atender a essa demanda, oferecendo aos usuários uma ferramenta para identificar, relatar e consultar informações sobre fraudes. Utilizando tecnologias avançadas, como os *chatbots* via *Botpress*, a inteligência artificial ChatGPT-3.5 e os painéis interativos com o *Google Looker*, a Beware proporciona uma experiência interativa e informativa.

Por meio da coleta e análise de dados demográficos e relatos de fraudes, a Beware ajuda os indivíduos a se protegerem contra possíveis golpes e oferece uma visão detalhada das tendências e padrões fraudulentos. A integração com o Telegram facilita a comunicação e o acesso às informações, tornando a plataforma acessível e eficiente.

Iniciativas como o Catálogo de Fraudes da RNP complementam os esforços da Beware, enfatizando a importância da conscientização e educação na prevenção de fraudes.

A Beware pode representar um avanço significativo na proteção dos consumidores contra fraudes online, destacando o papel crucial da tecnologia e da colaboração no combate a esse problema complexo e em constante evolução, além de possibilitar o acesso gratuito e a democratização de ferramentas à sociedade.

## Referências

Asher, J., & Rachmawati, E. P. (2024). Visualisasi Data Operasi SAR BASARNAS Di Indonesia Menggunakan Google Looker Studio. *Indonesian Journal of Computer Science*, 13(2).

Beraldi, F. (2014). *Atualização dinâmica de modelo de regressão logística binária para detecção de fraudes em transações eletrônicas com cartão de crédito* (Doctoral dissertation, Universidade de São Paulo).

Brown, L. (2023). *Digital Communication Integration*: Enhancing User Engagement. TechConnect Publishing, (p.102)

de Góis Silva[1], L. R. USO DE DASHBOARDS NA ANÁLISE DE DADOS: UM ESTUDO DE CASO.

Estadão. (2023). Brasil tem aumento nas tentativas de fraude; veja dicas para se proteger. E-Investidor.

https://einvestidor.estadao.com.br/ultimas/brasil-dados-tentativas-fraude-dicas-se-proteger/

Johnson, A., et al. (2018). Natural Language Processing for Fraud Detection. *Proceedings of the International Conference on Artificial Intelligence*, 42(3), 211-224.

Johnson, M. (2022). *Data Integration and User Experience:* Strategies for Modern Platforms. DataTech Publishing, (p.78).

Martins, E., & Verardi Galegale, N. (2022). Detecção de fraudes no segmento de crédito financeiro utilizando aprendizado de máquina*:* uma revisão da literatura. *Revista E-TECH: Tecnologias Para Competitividade Industria*l - ISSN - 1983-1838, 15(3)

Pereira, R. D., & Murai, F. (2021, July). Quao efetivas sao Redes Neurais baseadas em Grafos na Detecçao de Fraude para Dados em Rede?. *In Anais do X Brazilian Workshop on Social Network Analysis and Mining* (pp. 205-210). SBC.

Bird, Steven, et al.(2009) *Natural language processing with Python.* O'Reilly Processamento de Linguagem Natural em Python Media, Inc.

Rebman Jr, C. M., Booker, Q. E., Wimmer, H., Levkoff, S., McMurtrey, M., & Powell, L. M. (2023). An Industry Survey of Analytics Spreadsheet Tools Adoption: Microsoft Excel vs Google Sheets. *Information Systems Education Journal*, 21(5), 29-42.

Sant´Ana, F. P., Sant´Ana, I. P., & Sant´Ana, C. de C. (2023). Uma utilização do Chat GPT no ensino. *Com a Palavra, O Professor,* 8(20), 74–86.

Silva, K., Tierno, R., Branchine, S., Vilaça, D., & Oliveira, F. (2021). Desenvolvimento de ferramenta de chatbot como solução para a comunicação do IFB. *In Anais Estendidos do XVII Simpósio Brasileiro de Sistemas de Informação*, p. 185-188.

Smith, J. (2020). Emerging Technologies in Fraud Prevention. *Journal of Cybersecurity*, 15(2), 123-135.

Smith, J. (2021). Advanced JavaScript Integrations: Enhancing System Functionality. *TechPres*, p.45.

Valério, R. A., Dias, A. P. V., de Souza, P. C., Vecchiato, D. A., da Silva, A. M., & Araújo, N. V. (2023, November). Desvendando as Artimanhas Virtuais: um projeto sobre a tipificação de golpes digitais e a promoção da conscientização popular. In Anais da XII Escola Regional de Informática de Mato Grosso (pp. 231-235). SBC

VEJA. Brasil é o segundo país com maior índice de fraudes. Veja, 2023. Disponível em: https://veja.abril.com.br/economia/brasil-e-o-segundo-pais-com-maior-indice-de-fraudes#:~:text=%C3%8Dndice%20no%20Brasil%20atingiu%2014,segundo%20relat%C3%B3rio%20elaborado%20pela%20Visa&text=O%20Brasil%20figura%20entre%20os,referente%20ao%20ano%20de%202023.