



CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA
CURSO DE SISTEMAS DE INFORMAÇÃO

UM CHATBOT PARA A PROTEÇÃO CONTRA O ESTELIONATO EM PLATAFORMAS DE E-COMMERCE

CARLOS EDUARDO TARANTO WINTER
DAVI HEGGDORNE KLEIN

Orientador: Nilson Mori Lazzarin
CEFET/RJ Campus Nova Friburgo

NOVA FRIBURGO
JUNHO / 2025

**CARLOS EDUARDO TARANTO WINTER
DAVI HEGGDORNE KLEIN**

UM CHATBOT PARA A PROTEÇÃO CONTRA O ESTELIONATO EM PLATAFORMAS DE E-COMMERCE

Trabalho de Conclusão de Curso (Graduação) apresentado ao Curso de Sistemas de Informação do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, como requisito parcial para a obtenção do título de Bacharel em Sistemas de Informação.

Orientador: Nilson Mori Lazarin
CEFET/RJ Campus Nova Friburgo

CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA
CURSO DE SISTEMAS DE INFORMAÇÃO
NOVA FRIBURGO
JUNHO / 2025

UM CHATBOT PARA A PROTEÇÃO CONTRA O ESTELIONATO EM PLATAFORMAS DE E-COMMERCE

Monografia apresentada ao Curso de Sistemas de Informação do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, como requisito parcial para a obtenção do título de Bacharel.

Carlos Eduardo Taranto Winter e Davi Heggdorne Klein

Banca Examinadora:



Documento assinado digitalmente
Nilson Mori Lazarin
Data: 19/06/2025 09:09:40-0300
Verifique em <https://validar.iti.gov.br>

Presidente, Professor Me. Nilson Mori Lazarin (CEFET/RJ) (Orientador(a))



Documento assinado digitalmente
ELIEZER DUTRA GONCALVES
Data: 23/06/2025 17:06:39-0300
Verifique em <https://validar.iti.gov.br>

Professor Dr. Eliezer Dutra Gonçalves (CEFET/RJ)



Documento assinado digitalmente
BRUNO FERNANDES GUEDES
Data: 19/06/2025 12:05:53-0300
Verifique em <https://validar.iti.gov.br>

Professor Me. Bruno Fernandes Guedes (CEFET/RJ)



Documento assinado digitalmente
ANDRE QUEIROZ FERREIRA DE MELLO
Data: 24/06/2025 16:11:15-0300
Verifique em <https://validar.iti.gov.br>

Professor Me. André Queiroz Ferreira de Mello (CEFET/RJ)

NOVA FRIBURGO

JUNHO 2025

W785c Winter, Carlos Eduardo Taranto.
Um chatbot para a proteção contra o estelionato em
plataformas de E-commerce. / Carlos Eduardo Taranto Winter,
Davi Heggdorne Klein. – Nova Friburgo, RJ: 2025.
xii, 31f.: il. (color.) : em PDF.

Trabalho de Conclusão de Curso (Curso de Sistemas de
Informação) - Centro Federal de Educação Tecnológica Celso
Suckow da Fonseca, 2025.

Bibliografia : f. 29-31.

Orientador: Nilson Mori Lazzarin

1. Sistemas de Informação. 2. Segurança da informação.
3. Internet – Medidas de segurança. I. Klein, Davi Heggdorne
(co-autor). II. Lazzarin, Nilson Mori (Orientador). II. Título.

CDD 658.4038

Resumo

Com o crescimento do comércio eletrônico e o aumento dos golpes virtuais, torna-se essencial garantir a segurança dos consumidores. Este trabalho propõe o desenvolvimento de uma solução inovadora: um *chatbot*, denominado Ricky (*inteRnet domaln ChecK sYstem*), que promove a segurança em plataformas de *e-commerce*, permitindo a verificação da autenticidade de *sites* por meio da extração de informações administrativas do domínio e correlação com dados da Receita Federal. A ideia central é democratizar o acesso a informações confiáveis de forma prática e acessível, utilizando o *WhatsApp* como meio de interação com o usuário. A abordagem adotada concentra-se na aplicação de técnicas de extração e validação de dados para oferecer suporte na tomada de decisões de compra mais seguras, sendo a implementação do *chatbot* uma etapa prática para validação dessa proposta. Para avaliar a eficácia da solução, foi conduzido um estudo de caso exploratório com base no Modelo de Aceitação de Tecnologia (TAM), envolvendo 102 participantes. A coleta de dados foi realizada por meio de questionários estruturados que mensuraram a facilidade de uso percebida, utilidade percebida, confiança e intenção de uso da ferramenta. Os resultados demonstram um impacto positivo na experiência dos consumidores, com 95,9% dos participantes relatando que o Ricky auxiliou na tomada de decisão sobre compras online e 90,8% sentindo-se mais confiantes nas transações. Dessa forma, o estudo contribui para a mitigação de riscos no comércio digital, oferecendo uma solução inovadora e de fácil utilização para o público.

Palavras-chave: ChatBot, Segurança, Internet.

Abstract

With the growth of *e-commerce* and the increase in online scams, ensuring consumer safety has become essential. This study proposes the development of an innovative solution: a *chatbot* named Ricky (inteRnet domain Check sYstem), designed to enhance security on *e-commerce* platforms by enabling the verification of website authenticity through the extraction of administrative domain information and correlation with data from Receita Federal (Brazilian Federal Revenue Service). The core idea is to democratize access to reliable information in a practical and accessible way, using *WhatsApp* as the interface for user interaction. The approach focuses on applying data extraction and validation techniques to support safer purchasing decisions, with the chatbot's implementation serving as a practical step toward validating this proposal. To assess the solution's effectiveness, an exploratory case study was conducted based on the Technology Acceptance Model (TAM), involving 102 participants. Data collection was carried out through structured questionnaires that measured perceived ease of use, perceived usefulness, trust, and intention to use the tool. The results show a positive impact on the consumer experience, with 95.9% of participants reporting that Ricky assisted in their decision-making regarding online purchases, and 90.8% feeling more confident in their transactions. Thus, this study contributes to risk mitigation in digital commerce by offering an innovative and user-friendly solution to the public.

Keywords: ChatBot. Security. Internet.

Sumário

1 – Introdução	1
1.1 Motivação	1
1.2 Problema	2
1.3 Contribuição	3
1.4 Organização do trabalho	3
2 – Fundamentação Teórica	4
2.1 Registro	4
2.1.1 Domínio de Internet	4
2.1.2 Cadastro de Pessoa Jurídica	5
2.2 Legislação	7
2.2.1 Código de Defesa do Consumidor (CDC)	8
2.2.2 Lei do E-commerce	8
2.3 Tecnologias de verificação	9
2.3.1 Selos de Reputação	9
2.3.2 Protocolo Whois	10
2.4 Tecnologias de comunicação	10
2.4.1 WhatsApp	11
2.4.2 Bot/ChatBot	11
3 – Trabalhos Relacionados	12
3.1 Abordagens na literatura	12
3.2 Ferramentas similares	13
3.3 Comparativo	14
4 – Proposta	17
4.1 Abordagem	17
4.2 Implementação	18
5 – Estudo de Caso	21
5.1 Objetivo do Estudo	21
5.2 Tipo e Design do Estudo	21
5.3 Questão de Pesquisa	21
5.4 Unidade de Análise	22
5.5 Público-Alvo	22
5.6 Procedimentos Metodológicos	22

5.6.1 Coleta de Dados	22
5.7 Lógica de Ligação dos Dados com as Proposições	23
5.8 Critérios de Interpretação dos Dados	23
5.9 Resultados	23
5.10 Análise das Questões de Pesquisa	25
5.11 Discussão	26
5.12 Considerações Finais	27
6 – Conclusão	28
6.1 Trabalhos Futuros	28
Referências	29

1 Introdução

Imagine a seguinte situação: um consumidor, ao navegar pelas redes sociais, encontra uma oferta imperdível de um *smartphone* de última geração, com um preço muito abaixo do mercado. Movido pela urgência e pela promessa de economia, ele clica no *link*, é direcionado a um *site* visualmente profissional e, confiando na aparência, realiza a compra. Poucos dias depois, percebe que foi vítima de um golpe: o *site* desapareceu, o produto nunca chegou e o prejuízo foi inevitável. Esse tipo de golpe tem se tornado cada vez mais comum com o avanço do comércio eletrônico. Estelionatários utilizam técnicas cada vez mais sofisticadas para criar páginas falsas, clonando visualmente lojas conhecidas ou inventando marcas inexistentes, dificultando a identificação de fraudes pelos consumidores. Diante desse cenário de crescente vulnerabilidade no ambiente digital, torna-se essencial desenvolver estratégias eficazes de proteção. Assim, este trabalho apresenta uma proposta para auxiliar na identificação de *sites* fraudulentos e na promoção da segurança dos usuários em transações online, por meio da análise de dados administrativos de domínios e da utilização de aplicativos de mensagens instantâneas.

A legislação do *e-commerce*, representada pelo Decreto nº 7.962/2013 (BRASIL, 2013), enfrenta desafios devido à rápida evolução tecnológica e à complexidade das transações *online*, exigindo atualizações constantes. A fiscalização é dificultada pela natureza transnacional da internet, tornando os consumidores vulneráveis a práticas desleais. Além disso, a confiabilidade dos selos de reputação em *sites* de *e-commerce* é questionável, pois não refletem adequadamente a confiança e podem ser manipulados. Métodos estatísticos são usados para aprimorar esses sistemas, mas ainda apresentam limitações. Assim, mais pesquisas são necessárias para reduzir vieses e melhorar a avaliação da confiabilidade das empresas de comércio eletrônico (RODRIGUES, 2020; FEITOSA; GARCIA, 2016).

1.1 Motivação

De acordo com a Associação Brasileira de Comércio Eletrônico (ABCOMM), durante os anos de 2019 a 2024, o faturamento do comércio eletrônico no Brasil experimentou um impressionante crescimento de aproximadamente 127%. Paralelamente, o volume de pedidos *online* registrou um notável aumento de 93% durante esse mesmo intervalo de tempo, totalizando 414,86 milhões de transações em 2024 (ABCOMM, 2025).

Esse crescimento foi fortemente influenciado pela pandemia de COVID-19, que acelerou a digitalização das atividades comerciais e consolidou o *e-commerce* como uma alternativa viável e segura para consumidores e empresas durante as restrições de mobilidade. A pandemia impulsionou mudanças significativas no comportamento dos consumidores,

resultando em um aumento exponencial nas transações *online* e, ao mesmo tempo, expondo vulnerabilidades no ambiente digital (CRUZ, 2021). Mesmo após o fim das restrições, esse novo padrão de comportamento se manteve, com o comércio eletrônico seguindo em trajetória de crescimento, conforme indicam os dados da (ABCOMM, 2025).

Paralelamente a essa expansão, os ambientes digitais passaram a apresentar riscos crescentes aos consumidores. Observa-se um aumento no número de golpes virtuais, invasões por *hackers*, vazamentos de dados pessoais, clonagem de cartões e disseminação de vírus, entre outras ameaças (MOTA, 2021).

Segundo a pesquisa realizada pela Unico IDtech, metade dos consumidores brasileiros já foi vítima de fraude no *e-commerce* (IDTECH, 2022). Logo, no comércio eletrônico, o consumidor pode estar sujeito a várias formas de violação de seus direitos. Exemplos incluem produtos com defeitos, publicidade enganosa, recebimento de mercadorias diferentes das solicitadas, serviços de baixa qualidade e não cumprimento dos termos e cláusulas do contrato. Esses são alguns dos problemas enfrentados pelo consumidor (SILVA, 2023).

Em razão disso, o estelionato emerge como um dos crimes mais beneficiados pela facilidade na criação de páginas e conteúdos fraudulentos. A criação de páginas falsas, muitas vezes imitando identidades visuais e estruturas de plataformas de compras *online* bem estabelecidas, visa enganar consumidores desavisados.

O crescimento do comércio eletrônico trouxe benefícios significativos, mas também ampliou os riscos e desafios relacionados à segurança e à proteção dos consumidores. Muitos usuários não se sentem seguros ao realizar compras na internet devido à falta de informações claras e à dificuldade de verificar dados das lojas *online*. Esse cenário evidencia a vulnerabilidade dos consumidores diante da ausência de mecanismos eficazes que auxiliem na coleta e apresentação de informações confiáveis sobre os *sites* de *e-commerce*, facilitando a tomada de decisão e promovendo maior confiança no ambiente digital (MOREIRA, 2023; MOREIRA, 2022).

1.2 Problema

O crescimento do comércio eletrônico trouxe facilidade e conveniência aos consumidores, mas também aumentou o número de fraudes envolvendo *sites* falsos (MOTA, 2021). Muitos usuários não conseguem verificar a autenticidade das lojas *online*, tornando-se vulneráveis a golpes.

Um dos fatores que gera essa insegurança é o uso indevido de selos de reputação. Apesar de serem criados para transmitir confiança, esses selos podem ser facilmente copiados e inseridos em *sites* fraudulentos, sem qualquer comprovação real (FEITOSA; GARCIA, 2016).

Outro agravante é a falta de fiscalização efetiva. Embora a legislação exija informações claras, como CNPJ e endereço físico, muitos *sites* fornecem dados falsos ou omitem informações importantes. A fiscalização não consegue acompanhar o ritmo de criação de novas lojas, o que dificulta a proteção dos consumidores (RODRIGUES, 2020).

Assim, a dificuldade em validar informações, o uso enganoso de selos e a fiscalização insuficiente criam um ambiente de desconfiança no comércio eletrônico, evidenciando a necessidade de soluções práticas que ajudem o consumidor a verificar a legitimidade das lojas.

1.3 Contribuição

Este trabalho propõe uma metodologia prática e acessível para auditoria de *sites* de *e-commerce*, com foco na democratização do acesso à verificação de informações administrativas de domínios. A metodologia desenvolvida integra a extração de dados de registro de domínios, por meio do protocolo *WHOIS*, com a validação cruzada junto à base da Receita Federal, oferecendo uma análise estruturada e confiável ao usuário. A implementação de um *chatbot* em plataformas de mensagens instantâneas, como o *WhatsApp*, serve como uma aplicação prática para validar a eficácia da metodologia proposta, proporcionando uma experiência de uso acessível e inclusiva. Dessa forma, o trabalho contribui para a mitigação de riscos no comércio eletrônico ao estruturar um processo inovador e eficiente de verificação de legitimidade de *sites*, aplicável em diferentes contextos tecnológicos.

1.4 Organização do trabalho

O Capítulo 2 trata da fundamentação teórica, explicando os conceitos técnicos essenciais para a compreensão da ideia. Em seguida, o Capítulo 3 discute os trabalhos e ferramentas relacionadas, fornecendo um panorama do estado da arte e das soluções existentes. No Capítulo 4, são detalhados os aspectos técnicos da ferramenta desenvolvida, bem como as tecnologias utilizadas neste trabalho. O Capítulo 5 descreve o estudo de caso utilizado para validar a ferramenta, incluindo a análise e discussão dos resultados obtidos. Por fim, o Capítulo 6 conclui o trabalho e sugere direções para pesquisas e desenvolvimentos futuros.

2 Fundamentação Teórica

Este capítulo dedica-se à exploração da fundamentação teórica essencial para entender os conceitos subjacentes ao estudo proposto. Aqui, serão abordados os principais conceitos e modelos que formam a base para a análise e desenvolvimento da ferramentas de auditoria e segurança em plataformas de *e-commerce*.

2.1 Registro

Nesta seção, são apresentados os principais elementos relacionados ao registro de domínios e à identificação formal de empresas na internet. Entender esses aspectos é essencial para avaliar a legitimidade de sites de e-commerce e garantir maior segurança ao consumidor. Para isso, exploram-se os conceitos de domínio de internet e Cadastro Nacional da Pessoa Jurídica (CNPJ).

2.1.1 Domínio de Internet

Nos primórdios da Internet, o acesso a computadores e serviços online exigia a utilização direta de endereços IP — sequências numéricas difíceis de memorizar. À medida que a rede crescia, tornou-se necessário criar um sistema que facilitasse a navegação para os usuários. Surge então o Sistema de Nomes de Domínio (DNS – Domain Name System), que traduziu nomes simples e compreensíveis, como *www.exemplo.com*, para seus respectivos endereços IP, permitindo uma navegação mais prática e intuitiva.

O DNS foi estruturado de maneira hierárquica e distribuída, funcionando como uma árvore invertida. No topo dessa hierarquia está a raiz, representada por um ponto (“.”), de onde partem os domínios de topo (Top-Level Domains – TLDs). Estes domínios podem ser genéricos, como *.com*, *.org* e *.net*, ou códigos de países (ccTLDs), como *.br* (Brasil) e *.uk* (Reino Unido).

Cada TLD é administrado por uma entidade específica, responsável pela gestão e registro dos domínios sob sua extensão. O NIC.br (Núcleo de Informação e Coordenação do Ponto BR) é a entidade responsável pela coordenação e implementação de iniciativas estratégicas para a Internet no Brasil. Entre suas principais atribuições está a administração do Registro.br, o departamento encarregado do registro de domínios na Internet com a terminação *.br*, conhecido como *Top-Level Domain* (TLD) do Brasil. Desde 1995, o Registro.br exerce diversas funções delegadas pelo Comitê Gestor da Internet no Brasil, incluindo o registro de nomes de domínio, bem como a administração e publicação do DNS para este TLD (SILVA *et al.*, 2012).

Para registrar um domínio sob o .br, é necessário ser uma pessoa física (CPF) ou jurídica (CNPJ) legalmente estabelecida no Brasil, com cadastro regular no Ministério da Fazenda. O processo é realizado pelo *site*¹ e inicia-se com a verificação da disponibilidade do domínio desejado (ver Figura 1a).

Se disponível, o usuário pode prosseguir com o registro, fornecendo os dados obrigatórios. Para cadastros com CPF, são exigidos nome, e-mail, endereço e telefone brasileiro. No caso de CNPJ, também é necessário informar a razão social da empresa e o CPF do responsável (ver Figura 1b).

Além de identificar *sites* brasileiros, o domínio .br possui grande importância na organização da Internet nacional, oferecendo diversas subcategorias que atendem a diferentes contextos de atuação. Existem, por exemplo, categorias específicas como gov.br para órgãos governamentais, edu.br para instituições de ensino, org.br para organizações sem fins lucrativos e art.br para atividades culturais. Essa diversidade facilita a identificação do propósito de cada *site*, contribuindo para a segurança e a confiança dos usuários. Dados atualizados sobre as categorias de domínios podem ser consultados diretamente no *site* do Registro.br².



(a) Verificação de disponibilidade (dia 08/06/2024)

② DADOS PESSOAIS DO ADMINISTRADOR DA CONTA

Nome completo (pessoa física) *

E-mail *

CEP *

Endereço * Número *

Complemento UF * Cidade *

DDD * Telefone * Ramal

③ DADOS DO TITULAR DO DOMÍNIO

☒ Quero utilizar os mesmos dados do administrador da conta

Razão social *

Responsável *

Informe nome do detentor do CPF ou responsável do CNPJ (por exemplo: sócio, presidente, diretor, etc.)

(b) Inserção dos dados necessários (dia 08/06/2024)

Figura 1 – Registro de domínio - Processo de verificação e inserção de dados.

2.1.2 Cadastro de Pessoa Jurídica

Ao se deparar com uma loja virtual desconhecida, uma dúvida comum que surge é: essa empresa realmente existe? Para ajudar na resposta, um recurso essencial é o CNPJ (Cadastro Nacional da Pessoa Jurídica).

¹ Disponível em: <<https://registro.br>>. Acesso em: 12 jan. 2025.

² Disponível em: <<https://registro.br/dominio/estatisticas/>>. Acesso em: 27 abr. 2025.

O CNPJ (Cadastro Nacional da Pessoa Jurídica) é um registro administrado pela Receita Federal do Brasil, utilizado para identificar empresas e outras entidades jurídicas. É composto por um número único de identificação, atribuído a cada pessoa jurídica registrada no Brasil. O CNPJ é utilizado como instrumento de controle fiscal, permitindo que as autoridades tributárias acompanhem as atividades econômicas das empresas e garantam o cumprimento das obrigações fiscais (GERMANI, 2007).

Para se cadastrar como pessoa jurídica e obter um CNPJ, são necessários alguns dados, incluindo RG, dados de contato e endereço residencial para a pessoa responsável, bem como tipo de ocupação, forma de atuação e endereço comercial para o negócio. Esses requisitos podem variar conforme o tipo de empreendimento, como MEI (Microempreendedor Individual), ME (Microempresa), EPP (Empresa de Pequeno Porte), entre outros.

Para consultar informações de uma empresa usando seu CNPJ, é possível acessar o *site* da Receita Federal, entrar na seção de consulta de pessoa jurídica e digitar os 14 dígitos do CNPJ. O portal exibirá uma página com todos os dados da empresa, incluindo o nome empresarial e a descrição da atividade.

Na figura 2 é apresentado como realizar uma consulta de CNPJ no *site* da Receita Federal.

Emissão de Comprovante de Inscrição e de Situação Cadastral

Cidadão,

Esta página tem como objetivo permitir a emissão do Comprovante de Inscrição e de Situação Cadastral de Pessoa Jurídica pela Internet em consonância com a [Instrução Normativa RFB nº 2.119, de 06 de dezembro de 2022](#).

Digite o número de CNPJ da empresa e clique em "Consultar".

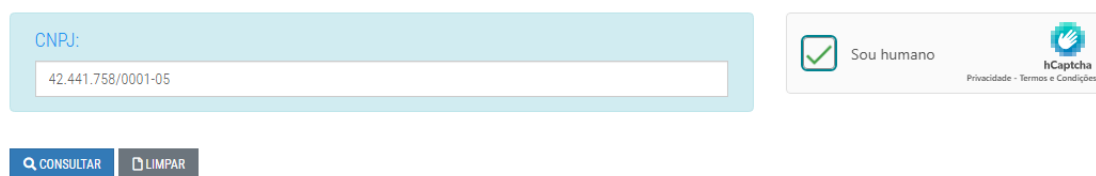


Figura 2 – Consulta de CNPJ - Inserção do CNPJ (dia 28/04/2025) <https://solucoes.receita.fazenda.gov.br/servicos/cnpjreva/cnpjreva_solicitacao.asp>

Ao final da consulta, é exibido o Cadastro Nacional da Pessoa Jurídica, conforme ilustrado na Figura 3

 REPÚBLICA FEDERATIVA DO BRASIL CADASTRO NACIONAL DA PESSOA JURÍDICA			
NÚMERO DE INSCRIÇÃO 42.441.758/0001-05 MATRIZ		COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO CADASTRAL	
		DATA DE ABERTURA 09/07/1976	
NOME EMPRESARIAL CENTRO FED DE ED TECNOLÓGICA CELSO SUCKOW DA FONSECA RJ			
TÍTULO DO ESTABELECIMENTO (NOME DE FANTASIA) *****			PORTE DEMAIS
CÓDIGO E DESCRIÇÃO DA ATIVIDADE ECONÔMICA PRINCIPAL 84.11-6-00 - Administração pública em geral			
CÓDIGO E DESCRIÇÃO DAS ATIVIDADES ECONÔMICAS SECUNDÁRIAS Não informada			
CÓDIGO E DESCRIÇÃO DA NATUREZA JURÍDICA 110-4 - Autarquia Federal			
LOGRADOURO AV MARACANA		NÚMERO 229	COMPLEMENTO *****
CEP 20.271-110	BAIRRO/DISTRITO MARACANA	MUNICÍPIO RIO DE JANEIRO	UF RJ
ENDEREÇO ELETRÔNICO		TELEFONE	
ENTE FEDERATIVO RESPONSÁVEL (EFR) UNIÃO			
SITUAÇÃO CADASTRAL ATIVA		DATA DA SITUAÇÃO CADASTRAL 04/07/1998	
MOTIVO DE SITUAÇÃO CADASTRAL			
SITUAÇÃO ESPECIAL *****		DATA DA SITUAÇÃO ESPECIAL *****	

Aprovado pela Instrução Normativa RFB nº 2.119, de 06 de dezembro de 2022.

Emitido no dia 28/04/2025 às 00:01:30 (data e hora de Brasília).

Página: 1/1

Figura 3 – Comprovante de Inscrição e de Situação Cadastral - Inserção do CNPJ (dia 28/04/2025) <https://solucoes.receita.fazenda.gov.br/servicos/cnpjreva/cnpjreva_solicitacao.asp>

2.2 Legislação

O ambiente digital também é regido por normas que visam proteger os direitos do consumidor. Esta seção aborda as principais legislações brasileiras aplicáveis ao comércio eletrônico, destacando os dispositivos que tratam da transparência nas transações online, da responsabilização dos fornecedores e dos direitos dos consumidores frente a práticas abusivas.

2.2.1 Código de Defesa do Consumidor (CDC)

O Código de Defesa do Consumidor (Lei nº 8.078/1990) é um dos pilares legais que visa proteger os direitos dos consumidores no Brasil, sendo aplicável também às transações realizadas no comércio eletrônico. Ele estabelece normas que garantem o acesso a informações claras e precisas sobre produtos e serviços, bem como a reparação de danos causados ao consumidor. A Lei aborda questões como a oferta de produtos e serviços, a proteção contra práticas abusivas, e assegura o direito à informação e à escolha do consumidor, além de garantir a devolução de valores pagos em caso de desistência da compra (BRASIL, 1990). De acordo com o Art. 6º do CDC, são direitos básicos do consumidor:

- I. a proteção da vida, saúde e segurança contra riscos causados por práticas no fornecimento de produtos e serviços;
- II. a educação e divulgação sobre o consumo adequado dos produtos e serviços;
- III. a informação adequada e clara sobre os diferentes produtos e serviços;
- IV. discriminação, no preço, de quaisquer despesas adicionais ou acessórias, tais como as de entrega ou seguros;
- V. a facilitação da defesa dos seus direitos, especialmente quando lesados por práticas comerciais abusivas ou desleais.

2.2.2 Lei do E-commerce

A Lei do *E-commerce*, baseada no Decreto Federal nº 7.962/2013 (BRASIL, 2013), complementa o Código de Defesa do Consumidor, regulamentando as transações *online* e focando em três áreas principais: informações claras e acessíveis, atendimento ao cliente eficiente e direito de devolução. As empresas devem fornecer dados completos sobre produtos, preços, formas de pagamento e políticas de devolução de maneira visível e compreensível (SOBHIE; OLIVEIRA, 2013).

De acordo com o Art. 2º do decreto supracitado, os sítios eletrônicos ou demais meios eletrônicos utilizados para oferta ou conclusão de contrato de consumo devem disponibilizar, em local de destaque e de fácil visualização, as seguintes informações:

- I. nome empresarial e número de inscrição do fornecedor, quando houver, no Cadastro Nacional de Pessoas Físicas ou no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda;
- II. endereço físico e eletrônico, e demais informações necessárias para sua localização e contato;
- III. características essenciais do produto ou do serviço, incluídos os riscos à saúde e à segurança dos consumidores;
- IV. discriminação, no preço, de quaisquer despesas adicionais ou acessórias, tais como

as de entrega ou seguros;

- V. condições integrais da oferta, incluídas modalidades de pagamento, disponibilidade, forma e prazo da execução do serviço ou da entrega ou disponibilização do produto; e
- VI. informações claras e ostensivas a respeito de quaisquer restrições à fruição da oferta.

Embora a Lei do *E-commerce* estabeleça requisitos claros para a divulgação de informações em *sites* de comércio eletrônico, essas exigências podem ser contornadas por empresas que fornecem dados incompletos ou enganosos. Por exemplo, algumas lojas virtuais exibem um CNPJ verdadeiro de outra empresa, induzindo o consumidor ao erro, ou omitem o endereço físico, dificultando a localização e contato em caso de problemas. Há também casos em que o *site* copia políticas de devolução de empresas renomadas, mas não oferece suporte real ao consumidor. A falta de fiscalização rigorosa pode permitir que tais práticas continuem, colocando os consumidores em risco de serem enganados ao realizar compras *online* (RODRIGUES, 2020).

2.3 Tecnologias de verificação

A verificação da confiabilidade de sites e empresas na internet é um desafio crescente. Esta seção apresenta algumas das principais tecnologias utilizadas para ajudar consumidores a avaliar a reputação e legitimidade de lojas virtuais, incluindo selos de reputação e o protocolo Whois.

2.3.1 Selos de Reputação

Os sistemas de reputação são mecanismos utilizados em ambientes *online* para coletar e apresentar informações sobre a reputação de empresas ou vendedores, com base nas experiências dos consumidores. Esses sistemas agregam *feedbacks* e avaliações de clientes, ajudando a construir a confiança dos consumidores em relação aos vendedores e empresas com os quais pretendem negociar. Além disso, algumas certificadoras de reputação verificam se os *sites* cumprem determinados padrões de qualidade e boas práticas de atendimento ao consumidor, como a política de devolução de produtos, a transparência nas informações comerciais e o atendimento eficiente. Em alguns casos, também exigem a apresentação de certificados de segurança digital, como SSL, para garantir a proteção dos dados pessoais dos consumidores. Ao prover informações que podem reduzir a incerteza na percepção dos consumidores, os sistemas de reputação promovem a criação de confiança ao fornecer percepções de diversos consumidores sobre o comportamento das empresas. Esses sistemas visam minimizar o problema de assimetria de informação entre compradores e vendedores, incentivando um comportamento que induz à confiança (FEITOSA; GARCIA, 2016).

Para obter um selo de reputação, é necessário submeter sua empresa à análise da

entidade certificadora escolhida. Durante esse processo, a certificadora avaliará diversos aspectos e métricas da empresa. Dependendo do tipo de selo e dos resultados dessa avaliação, sua empresa pode ser aprovada ou reprovada, recebendo diferentes níveis de selo de reputação (COSTA, 2011).

Exemplos de Selos de Reputação:

- I. eBit: Concedido pela certificadora NielsenIQ eBit, é um dos selos de reputação mais conhecidos no Brasil, avalia empresas com base em *feedbacks* de consumidores que realizaram compras *online*. As lojas são classificadas em categorias como bronze, prata, ouro e diamante, de acordo com a qualidade de suas avaliações³.
- II. Reclame Aqui (RA1000): Selo de excelência do portal Reclame AQUI, concedido a empresas que apresentam altos índices de solução de problemas, bom atendimento e avaliações positivas dos consumidores⁴.
- III. Google Avaliações: Utilizado por consumidores para avaliar empresas diretamente no Google, criando uma reputação pública com base na experiência dos clientes⁵.
- IV. Trustpilot: Gerenciado pela plataforma global de avaliações Trustpilot que gera selos baseados na qualidade e quantidade de *feedbacks* de clientes, reforçando a credibilidade internacional de uma empresa⁶.

2.3.2 Protocolo Whois

O protocolo *WHOIS* é um sistema que permite a consulta de informações relacionadas ao registro de domínios na internet. Ele fornece detalhes administrativos, técnicos e de registro, como o nome do registrante, dados de contato, organização responsável, datas de criação e expiração do domínio, além de informações sobre os servidores DNS associados. Essa ferramenta é amplamente utilizada para verificar a autenticidade de *sites*, identificar proprietários de domínios e monitorar atividades suspeitas na internet (DAIGLE, 2004).

2.4 Tecnologias de comunicação

A comunicação eficiente entre consumidores e sistemas automatizados é um pilar das soluções modernas de segurança digital. Nesta seção, serão abordadas as tecnologias mais utilizadas para interação com o usuário, como o WhatsApp e os chatbots, destacando sua aplicabilidade e impacto na experiência do consumidor.

³ Disponível em: <<https://www.ebit.com.br/>>. Acesso em: 28 abr. 2025.

⁴ Disponível em: <<https://www.reclameaqui.com.br/como-funciona/selo/>>. Acesso em: 28 abr. 2025.

⁵ Disponível em: <<https://support.google.com/merchants/answer/14629804?hl=pt-BR>>. Acesso em: 28 abr. 2025.

⁶ Disponível em: <<https://www.trustpilot.com/>>. Acesso em: 28 abr. 2025.

2.4.1 WhatsApp

O *WhatsApp* é uma das plataformas de comunicação mais populares do mundo, com bilhões de usuários ativos. Sua simplicidade e integração com dispositivos móveis o tornam amplamente utilizado em diversos contextos, desde interações pessoais até serviços empresariais. No Brasil, está presente em 98% dos celulares, consolidando-se como o principal aplicativo de mensagens (GLOBAL, 2024).

Sua importância no cenário atual é enorme, especialmente para o comércio eletrônico e para a segurança digital. O *WhatsApp* é amplamente utilizado como ferramenta de atendimento ao cliente, vendas, suporte técnico e envio de informações importantes, oferecendo comunicação rápida e direta com os consumidores. Além disso, sua popularidade entre diferentes faixas etárias e classes sociais facilita a democratização do acesso a serviços digitais, tornando-o uma plataforma estratégica para a implementação de soluções inovadoras.

Além disso, tem sido usado na segurança digital para disseminação de informações e interações automatizadas via *bots*, facilitando o acesso a dados relevantes (BATISTA; SOUZA *et al.*, 2023).

2.4.2 Bot/ChatBot

Os *chatbots* são sistemas computacionais projetados para interagir com usuários por meio de mensagens automatizadas. Em essência, eles funcionam como assistentes virtuais que fornecem respostas e informações pré-programadas em tempo real (VALENTINI *et al.*, 2021). A principal função do *chatbot* é simplificar a comunicação entre o usuário e o sistema. Esse papel é especialmente relevante em aplicativos de mensagens instantâneas, já que aproxima a interação do usuário de uma experiência mais próxima e simples.

Um exemplo de *chatbot* é a Bia (acrônimo de Bradesco Inteligência Artificial), do Bradesco, ela está disponível para ajudar clientes a tirar dúvidas e realizar consultas de saldo, encontrar agências, verificar a cotação do dólar, conferir lançamentos da conta, e checar o limite do cartão, entre outros serviços, bastando enviar uma mensagem (BATISTA; SOUZA *et al.*, 2023).

Outro exemplo é a Lu, assistente virtual da Magazine Luiza, que atua em diversas plataformas digitais oferecendo suporte ao consumidor, esclarecimento de dúvidas, acompanhamento de pedidos e recomendações de produtos, consolidando-se como uma importante ferramenta de atendimento no e-commerce brasileiro (NAMA, 2018).

3 Trabalhos Relacionados

Neste capítulo, serão apresentados os trabalhos relacionados que embasaram o desenvolvimento desta ideia. Ao analisar estudos prévios, buscamos compreender o contexto e as abordagens utilizadas em pesquisas similares, visando aprimorar nossa compreensão do tema e identificar lacunas que nosso trabalho pretende preencher.

3.1 Abordagens na literatura

Em (CARVALHO; LAZARIN, 2023) é proposto o desenvolvimento de uma extensão para navegadores voltada à auditoria de dados administrativos de *sites* de *e-commerce*. Essa ferramenta utiliza informações obtidas pelo protocolo *WhoIs* e pela Receita Federal, como CNPJ, dados do responsável pelo domínio, endereço e telefone, para verificar a legitimidade do *site* acessado. A extensão apresenta essas informações de forma organizada e destaca inconsistências por meio de um sistema de cores, facilitando a identificação de possíveis riscos pelo usuário.

No trabalho de (RODRIGUEZ-ARRASTIA *et al.*, 2022), é abordado o uso do *SafeBot*, um *chatbot* projetado para apoiar as decisões clínicas de estudantes de enfermagem em situações simuladas de emergência. Os participantes relataram que a ferramenta contribuiu para organizar informações de maneira clara e eficiente, facilitando a tomada de decisão em cenários críticos. As avaliações destacaram aspectos positivos como usabilidade, precisão e rapidez na apresentação de informações relevantes. Como sugestões de melhoria, os estudantes recomendaram maior interatividade e a inclusão de conteúdos mais detalhados para atender diferentes contextos clínicos. Concluiu-se que o *SafeBot* pode atuar como um recurso complementar para apoiar práticas seguras e melhorar o desempenho em situações de alta pressão.

Em seu estudo, (FILHO; ROSSI, 2020) apresenta uma abordagem baseada em *chatbot* para apoiar o processo de gerenciamento de incidentes de *software*, utilizando a plataforma *DialogFlow*. O estudo apresenta etapas detalhadas para a implementação e o treinamento contínuo do *chatbot*, com o objetivo de otimizar a identificação e a resolução de incidentes em sistemas computacionais. O trabalho explora a aplicação de técnicas de Processamento de Linguagem Natural (NLP) para compreender as intenções dos usuários e fornecer respostas relevantes. As etapas incluem a coleta de exemplos de incidentes, a definição de fluxos de decisão, e o monitoramento contínuo do desempenho do *chatbot*, favorecendo a adaptação e o aprimoramento constante da solução. Além disso, destaca-se

o alinhamento com o *framework* ITIL, garantindo a padronização e a eficiência no suporte técnico.

3.2 Ferramentas similares

O *ScamAdviser* é uma ferramenta *online* que permite verificar a confiabilidade de um *site*. Baseado em algoritmos avançados, ele analisa diversos fatores, como a idade do domínio, localização do servidor e opiniões de usuários, para atribuir uma pontuação de confiabilidade ao *site*. Isso ajuda os consumidores a identificarem possíveis fraudes antes de realizarem transações *online*. A figura 4 apresenta uma imagem da ferramenta.

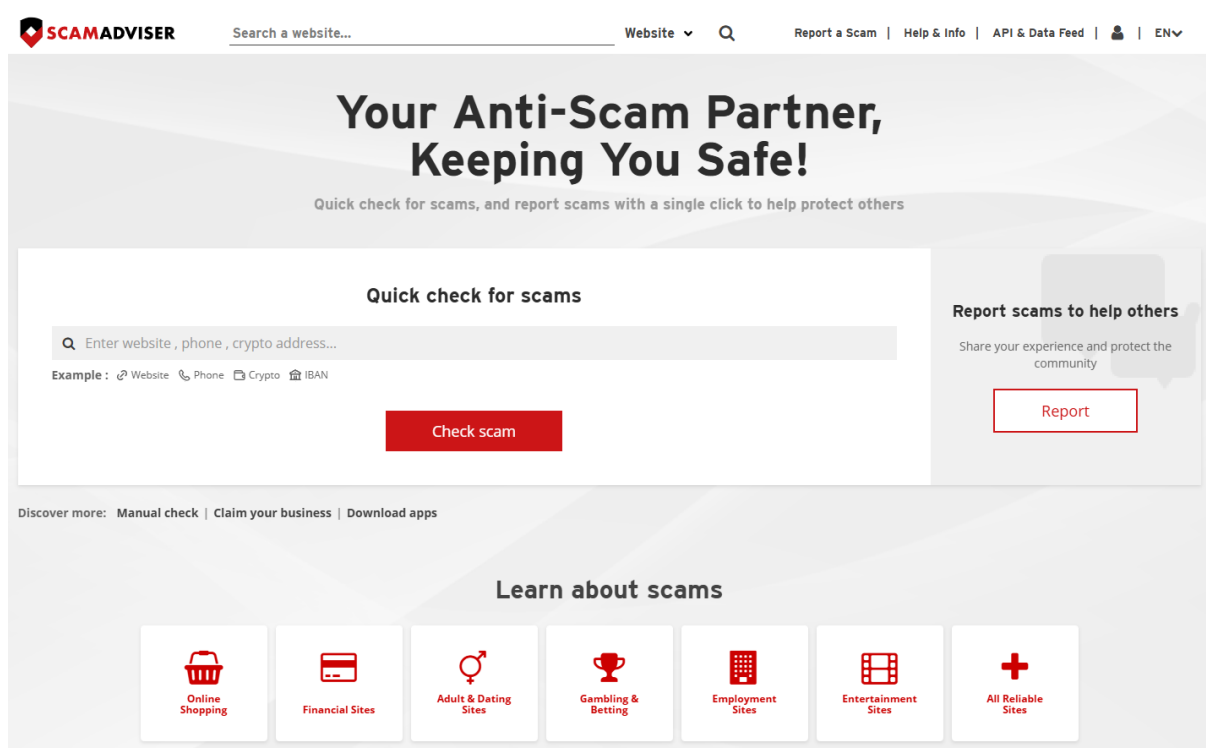


Figura 4 – Imagem da ferramenta *ScamAdviser* (dia 07/01/2025)

O Detector de *Site* Confiável do Reclame Aqui, disponibilizada pelo Reclame Aqui, permite que os usuários verifiquem rapidamente a reputação de um *site* de *e-commerce*. Ao inserir o endereço do *site*, o sistema consulta dados como reclamações registradas, taxa de resolução de problemas e índices de satisfação dos consumidores. Com isso, os usuários podem tomar decisões mais informadas e seguras ao realizar compras *online*. A imagem da ferramenta pode ser encontrada na figura 5.



Figura 5 – Detector de Site Confiável do Reclame Aqui (dia 07/01/2025)

3.3 Comparativo

A presente proposta visa implementar um *bot* em plataformas de mensagens instantâneas para consultar domínios com TLD *.br*, extrair os dados administrativos e integrá-los com informações da Receita Federal. A ferramenta deve funcionar da seguinte maneira, basta enviar um *link* e ela realizará uma análise detalhada do *site*. Em seguida, fornecerá informações úteis que podem ajudar o usuário a avaliar se o *site* é confiável ou não. Com isso, pretende-se contribuir para a proteção dos usuários em plataformas de *e-commerce*.

O primeiro trabalho analisado, que serviu como base para o presente trabalho, desenvolveu uma extensão para navegadores voltada à auditoria de dados administrativos de *sites* de *e-commerce*, utilizando informações do protocolo *WhoIs* e da Receita Federal. Apesar de cumprir o objetivo de aumentar a segurança do consumidor, sua implementação é limitada, já que extensões dependem da compatibilidade com navegadores e não estão disponíveis em dispositivos móveis. O presente trabalho inova ao propor um *chatbot* integrado a aplicativos de mensagens instantâneas, ampliando o acesso a essas informações de forma mais democrática e prática.

O segundo trabalho, focado no uso do *chatbot SafeBot* para apoiar decisões clínicas em situações de emergência, demonstra como a clareza e rapidez na apresentação de

informações podem facilitar tomadas de decisão críticas. Essa perspectiva influenciou a construção de um sistema intuitivo e acessível no contexto de segurança em *e-commerce*.

Já o terceiro trabalho explorou um *chatbot* para gerenciamento de incidentes de *software*, destacando a importância de técnicas como o Processamento de Linguagem Natural (PLN) e a adaptação contínua às necessidades dos usuários. Essas características reforçaram a abordagem proposta neste trabalho, visando um *chatbot* dinâmico e eficiente.

A primeira ferramenta analisada é o *ScamAdviser*, uma ferramenta *online* que permite verificar a confiabilidade de um *site* por meio de algoritmos avançados. Essa ferramenta avalia diversos fatores, como a idade do domínio, localização do servidor e opiniões de usuários, atribuindo uma pontuação de confiabilidade ao *site*. Embora seja eficaz em identificar possíveis riscos em *sites* internacionais, sua abordagem genérica pode não atender adequadamente às especificidades do mercado brasileiro. O presente trabalho inova ao integrar dados administrativos diretamente da Receita Federal, oferecendo uma análise mais contextualizada para os usuários brasileiros.

A segunda ferramenta considerada foi o Detector de *Site* Confiável do Reclame Aqui, que verifica a reputação de *sites* de *e-commerce* com base em reclamações registradas, taxas de resolução de problemas e índices de satisfação dos consumidores. Apesar de sua relevância para empresas com histórico no Reclame Aqui, a ferramenta possui limitações ao lidar com *sites* novos ou sem registro na plataforma. A solução proposta neste trabalho complementa essa abordagem ao incorporar dados administrativos de domínios, possibilitando a avaliação de *sites* ainda não mapeados por plataformas de reputação.

Em síntese, o presente trabalho se diferencia ao integrar elementos dessas abordagens, propondo uma solução mais acessível e adaptada às demandas de segurança no comércio eletrônico. Para melhor visualizar essa comparação, a Tabela 1 apresenta uma análise baseada em critérios relevantes, como:

- **Uso de aplicativos de mensagens:** se a solução utiliza plataformas de comunicação instantânea para interação;
- **Experiência do usuário:** se há foco na usabilidade e facilidade de navegação para o consumidor;
- **Proteção contra golpes virtuais:** se a solução é capaz de detectar e alertar sobre possíveis fraudes;
- **Tomada de decisões:** se a ferramenta auxilia os usuários na escolha consciente de realizar ou não uma ação;
- **Uso de mensagens automatizadas:** se o sistema faz uso de *bots* ou automações para comunicação;
- **Foco em auxiliar usuários:** se o objetivo principal é apoiar ou proteger o usuário.

Esses critérios permitem avaliar de forma objetiva as principais características dos

trabalhos e ferramentas analisados em relação à proposta desenvolvida neste estudo.

Tabela 1 – Comparativo de Trabalhos e Ferramentas Relacionados

Crítérios	T1	T2	T3	F1	F2	PT
Uso de aplicativos de mensagens	X	X	V	X	X	V
Experiência do usuário	X	V	V	V	V	V
Proteção contra golpes virtuais	V	X	X	V	V	V
Tomada de decisões	V	V	V	V	V	V
Uso de mensagens automatizadas	X	V	V	X	X	V
Focado em auxiliar usuários	V	V	V	V	V	V

T1, T2, T3 Representam trabalhos relacionados:

- **T1:** Uma extensão facilitadora para consulta de dados administrativos sobre *sites* de e-commerce (CARVALHO; LAZARIN, 2023).
- **T2:** *Experiences and perceptions of final-year nursing students of using a chatbot in a simulated emergency situation: A qualitative study* (RODRIGUEZ-ARRASTIA *et al.*, 2022).
- **T3** *Chatbot Based Solution for Supporting Software Incident Management Process* (FILHO; ROSSI, 2020).

F1, F2 Representam ferramentas analisadas:

- **F1:** *ScamAdviser*.
- **F2:** Detector de *Site* Confiável do Reclame Aqui.

PT Representa o presente trabalho.

V Indica a presença do atributo no item avaliado.

X Indica a ausência do atributo no item avaliado.

4 Proposta

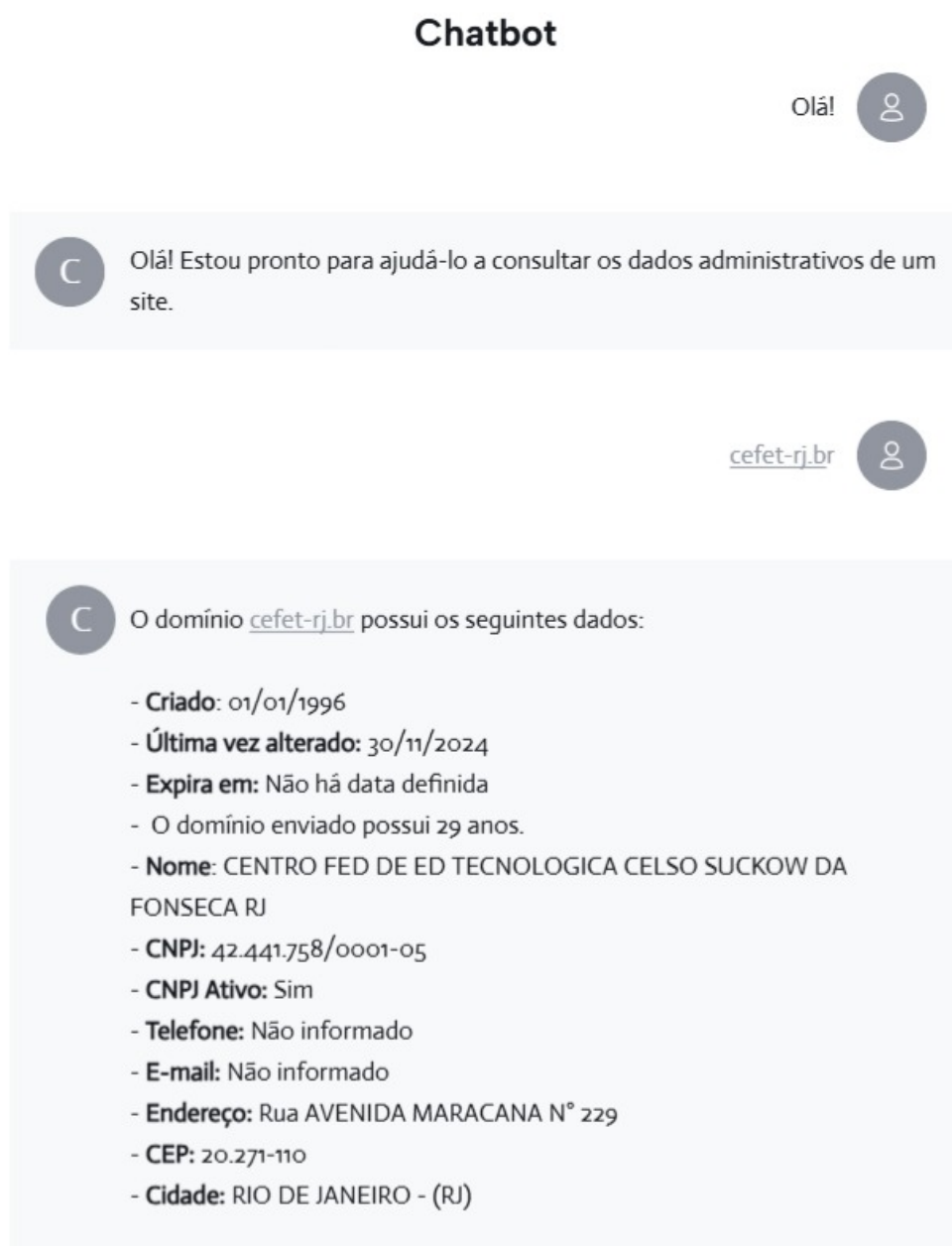
Apesar dos diversos trabalhos e ferramentas existentes para verificação de confiabilidade de *sites* de *e-commerce*, como extensões de navegador (CARVALHO; LAZARIN, 2023), plataformas de avaliação de reputação (*ScamAdviser*) e consultas de reclamações (Detector de *Site* Confiável do Reclame Aqui), ainda persistem lacunas importantes que justificam a necessidade de uma nova abordagem.

As soluções baseadas em extensões de navegador, por exemplo, restringem seu uso a dispositivos compatíveis e exigem conhecimentos técnicos para instalação, o que dificulta o acesso de usuários com menor familiaridade digital. Já ferramentas como *ScamAdviser* têm foco em análises genéricas, muitas vezes desconsiderando particularidades do mercado brasileiro, como a obrigatoriedade do registro de domínios .br no NIC.br. Além disso, o Detector de *Site* Confiável do Reclame Aqui depende da existência prévia de reclamações registradas, sendo ineficaz para identificar riscos em novos *sites* ou empresas que ainda não possuem histórico na plataforma.

Diante dessas limitações, este trabalho propõe a implementação de uma ferramenta para a realização de consultas a domínios com TLD .br, extraindo informações administrativas diretamente do registro de domínios e validando-as com dados oficiais da Receita Federal. A escolha por utilizar um comunicador instantâneo, amplamente difundido no Brasil, visa democratizar o acesso à verificação de segurança de *sites*, superando barreiras técnicas e ampliando a proteção dos consumidores de forma prática, rápida e acessível.

4.1 Abordagem

A abordagem adotada neste trabalho fundamenta-se na democratização do acesso à informação e na simplificação de processos de verificação de segurança no ambiente digital. Para alcançar esses objetivos, optou-se pela utilização de um comunicador instantâneo como plataforma de implementação. Essa decisão baseia-se em fatores como a ampla acessibilidade dessas plataformas, sua compatibilidade com diferentes dispositivos e sistemas operacionais, e a familiaridade que a maioria dos usuários já possui com elas. Isso garante que mesmo usuários com pouca experiência técnica possam acessar as funcionalidades da ferramenta. O objetivo é proporcionar uma experiência prática, inclusiva e eficiente, permitindo que qualquer usuário possa verificar informações administrativas e cadastrais de domínios de forma rápida e simplificada. A Figura 6 ilustra a interação entre o *chatbot* e o usuário, utilizando um protótipo como demonstração.

Figura 6 – Protótipo de interação entre o *chatbot* e o usuário

4.2 Implementação

O desenvolvimento do *bot*, denominado Ricky (*inteRnet domain Check sYstem*), foi realizado com o objetivo de integrar eficiência e acessibilidade na verificação de informações de segurança de domínios da internet.

A arquitetura geral do Ricky foi desenvolvida com as linguagens *TypeScript* e *JavaScript*. Os dados necessários para as consultas e a integração com as APIs externas foram armazenados no banco de dados *MongoDB*, uma solução *NoSQL* escolhida por sua flexibilidade e escalabilidade no gerenciamento de grandes volumes de dados.

Para assegurar a acessibilidade e a inclusão de usuários com diferentes níveis de familiaridade técnica foi escolhido o *WhatsApp* como plataforma de interação com os usuários. Essa escolha foi motivada por sua ampla popularidade, alta taxa de adoção em diferentes dispositivos e sistemas operacionais, além de sua interface amigável e amplamente conhecida.

A implementação do *bot* no *WhatsApp* exigiu um chip de celular ativo necessário para autenticação e funcionamento contínuo na plataforma. Também foi utilizada uma biblioteca especializada para automação de mensagens, responsável por gerenciar o envio e recebimento de mensagens e processar comandos dos usuários.

O *bot* realiza a consulta de dados administrativos de domínios por meio do protocolo *WHOIS*, que permite acessar informações cruciais sobre o registro de um domínio, como a titularidade, a data de criação e o status de validade. Essas informações são então combinadas com dados cadastrais obtidos a partir da integração com a base da Receita Federal.

O fluxo de funcionamento do *bot* é dividido em etapas. Primeiramente, ele captura as mensagens enviadas pelos usuários no *WhatsApp*. Em seguida, processa essas mensagens para identificar os *links* de domínios presentes. Após a extração, o *bot* consulta os dados relevantes dos domínios através do protocolo *WHOIS* e realiza a integração com a Receita Federal para validar as informações. Finalmente, os resultados são apresentados diretamente na conversa com o usuário, proporcionando uma resposta rápida e eficiente. A figura 7 demonstra, por meio de um diagrama, o funcionamento do *bot*, enquanto a Figura 8 apresenta um exemplo de interação com a ferramenta.

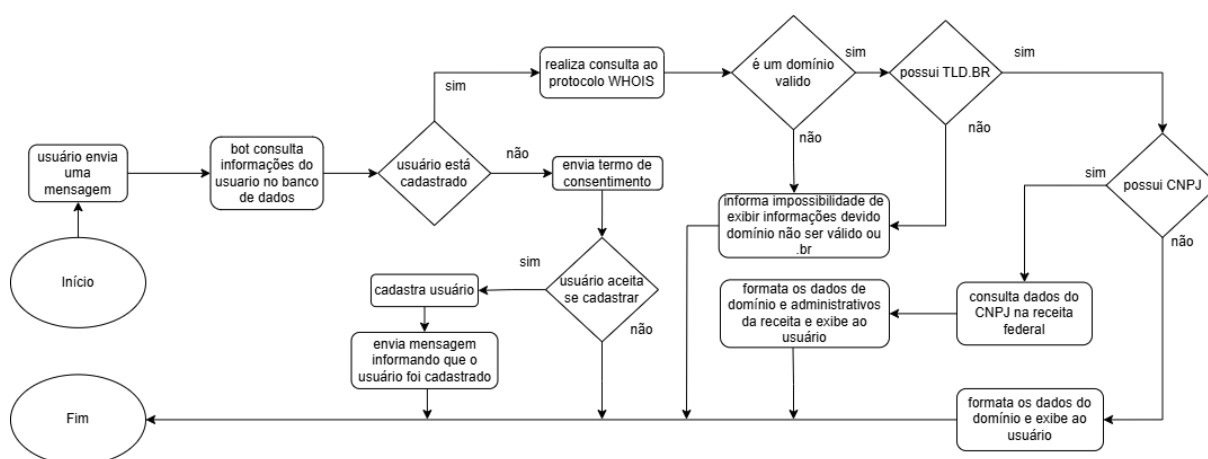


Figura 7 – Diagrama do funcionamento do chatbot

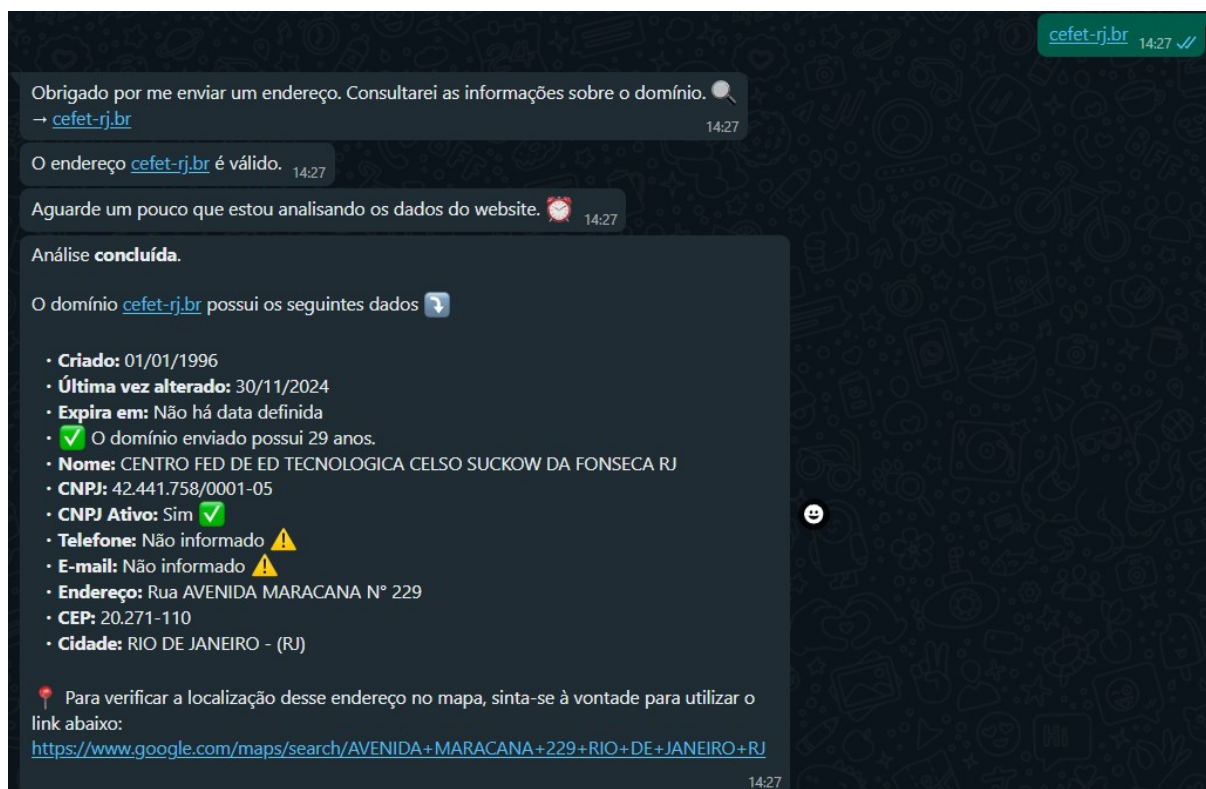


Figura 8 – Interação do chatbot com o usuário

O código-fonte do Ricky está disponível no *GitHub*¹. Além disso, há um vídeo no *YouTube* explicando como iniciar o projeto² e um *website* dedicado ao projeto³.

Vale destacar que, para reproduzir o funcionamento do Ricky, será necessário um chip de celular ativo para a autenticação e operação contínua na plataforma.

¹ Disponível em: <<https://github.com/LabRedesCefetRJ/RickyBot>>

² Disponível em: <<https://bsi.cefet-rj.br/ricky/video/demo.mp4>>

³ Disponível em: <<https://bsi.cefet-rj.br/ricky/>>

5 Estudo de Caso

Este capítulo apresenta o planejamento e execução de um estudo de caso visando avaliar a ferramenta Ricky, conforme os princípios metodológicos descritos por Robert K. Yin (YIN, 2015). Yin (2015) afirma que o estudo de caso pode ser utilizado como método de avaliação, permitindo, assim, uma investigação em seu contexto real. O estudo foi planejado e executado seguindo um protocolo sistemático visando identificar evidências iniciais de validade. Serão descritos o objetivo, o público-alvo, a unidade de análise, os procedimentos metodológicos adotados, os resultados e a discussão com base nas evidências empíricas coletadas.

5.1 Objetivo do Estudo

O objetivo principal deste estudo de caso é avaliar a eficácia da ferramenta Ricky na melhoria da segurança em transações de *e-commerce*. A pesquisa investiga como a ferramenta contribui para a tomada de decisões mais informadas pelos consumidores, promovendo maior confiança na realização de compras online.

5.2 Tipo e Design do Estudo

Este é um estudo de caso exploratório com abordagem quantitativa. O modelo de Robert K. Yin foi adotado como referência, o que implica seguir um protocolo estruturado, contendo os seguintes elementos:

- Definição clara do problema e proposições teóricas;
- Identificação das unidades de análise;
- Lógica de ligação dos dados com as proposições;
- Critérios para interpretação dos resultados.

5.3 Questão de Pesquisa

A questão central do estudo é: A ferramenta Ricky aumenta a confiança dos usuários em compras realizadas por meio de *sites* de *e-commerce*? A seguir, são apresentadas as subquestões complementares que orientam a investigação proposta.

- A ferramenta é considerada fácil de usar?
- Os usuários percebem utilidade prática na solução?
- O Ricky é capaz de influenciar na decisão de compra do usuário?

5.4 Unidade de Análise

A unidade de análise deste estudo é o usuário individual da ferramenta Ricky. Cada usuário que participou da pesquisa representa uma unidade, sendo observadas suas percepções quanto à eficácia, confiança, facilidade de uso e intenção de uso futuro.

5.5 Público-Alvo

O estudo envolveu 102 participantes com perfis variados, incluindo:

- Consumidores frequentes e infrequentes de *e-commerce*;
- Profissionais da área de segurança digital;
- Usuários com diferentes níveis de conhecimento em informática (básico, intermediário, avançado).

5.6 Procedimentos Metodológicos

A ferramenta Ricky foi desenvolvida como um *chatbot* integrado ao *WhatsApp*, com o objetivo de oferecer uma solução acessível e intuitiva para auxiliar usuários na verificação da confiabilidade de *sites* de *e-commerce*. A aplicação foi hospedada no laboratório de redes do CEFET/RJ — Campus Nova Friburgo, utilizando o *MongoDB* como solução de banco de dados em nuvem, o que garantiu escalabilidade, alta disponibilidade e flexibilidade no armazenamento das informações.

A divulgação da ferramenta foi realizada por meio de múltiplos canais, incluindo redes sociais como *Instagram*, *WhatsApp* e *Telegram*, buscando alcançar um público diversificado e promover a experimentação do *bot*. Além disso, o Ricky foi apresentado em eventos acadêmicos e tecnológicos, como *workshops* e palestras, onde foi possível demonstrar seu funcionamento na prática. Um exemplo disso foi a apresentação da versão inicial do *chatbot* no evento *Computer on the Beach* na edição 2024 (WINTER; KLEIN; LAZARIN, 2024). Também foi criada uma página oficial do projeto contendo informações detalhadas sobre o propósito da ferramenta, instruções de acesso e orientações de uso.

5.6.1 Coleta de Dados

A coleta de dados foi realizada entre os dias 31/12/2024 e 09/02/2025. Foi aplicado um questionário estruturado via Google Forms¹, com base no Modelo de Aceitação de Tecnologia (TAM) de Davis (DAVIS; DAVIS, 1989). As métricas coletadas incluíram:

- Facilidade de uso percebida;

¹ Resultados disponíveis em: <https://docs.google.com/forms/d/1fvyDBxk7IQoHBk8YUD-Ugrg1dQfbdyozId7zIz_GI8o/viewanalytics>

- Utilidade percebida;
- Atitude em relação ao uso;
- Intenção de uso;
- Confiança nas informações fornecidas;
- Usabilidade da interface.

5.7 Lógica de Ligação dos Dados com as Proposições

O modelo TAM foi utilizado como base teórica para estabelecer a ligação entre os dados coletados e as proposições do estudo. A hipótese é que quanto maior a percepção de facilidade de uso e utilidade da ferramenta, maior será a confiança do usuário nas decisões de compra online.

5.8 Critérios de Interpretação dos Dados

A interpretação dos dados foi realizada por meio da análise estatística descritiva dos resultados do questionário. Foram avaliadas as frequências relativas e absolutas das respostas, agrupadas conforme os eixos definidos pelo modelo TAM.

5.9 Resultados

Os dados foram organizados em duas categorias principais: perfil dos participantes e percepção sobre o uso da ferramenta Ricky. Os gráficos da Figura 9 ilustram os dados relacionados à frequência de compras online, conhecimento em informática e percepção de segurança.

Com base na pesquisa foi realizada a seguinte Análise de perfil:

- **Frequência de compras *online*:** Aproximadamente 67,7% dos respondentes relataram realizar compras *online* frequentemente ou em datas comemorativas, enquanto 30,4% compram raramente e apenas 2% nunca compram.
- **Conhecimento em Informática:** A maioria dos usuários declarou possuir conhecimento intermediário (35%) ou básico (31%) em informática, enquanto 14% se consideram avançados e 11% trabalham diretamente na área de tecnologia.
- **Segurança ao realizar compras *online*:** Cerca de 54% dos participantes se sentem inseguros ou muito inseguros ao fazer compras *online*.

Os gráficos a seguir (Figura 9) ilustram o perfil dos usuários em relação à frequência de compras, conhecimento em informática e sensação de segurança ao realizar compras *online*.



Figura 9 – Gráficos abordando o Perfil dos Usuários

Seguindo foi possível levantar os presentes dados sobre o Uso do Ricky e Percepção

dos Usuários:

- **Eficácia:** Dentre esses, 95,9% relataram que o *bot* ajudou na tomada de decisão sobre realizar ou não uma compra.
- **Confiança:** Com a ajuda do Ricky, 90,8% dos usuários se sentiram mais confiantes ao realizar transações textitonline.
- **Facilidade de uso:** 98% dos participantes concordaram que o Ricky é fácil de usar, com 68,4% concordando totalmente.
- **Instruções claras:** 96,9% consideraram as instruções simples e diretas.
- **Decisões informadas:** 93,9% afirmaram que o textitbot contribui para tomar decisões mais informadas.
- **Interpretação dos resultados:** 88,8% dos participantes concordaram que os resultados apresentados pelo Ricky são fáceis de interpretar.
- **Recomendação:** 96,9% dos usuários indicariam o Ricky para outras pessoas.
- **Continuidade de uso:** 93,9% pretendem continuar utilizando o *bot*.

Os resultados obtidos do questionário baseado no Modelo de Aceitação de Tecnologia (TAM) estão representados na Figura 10, ilustrando a avaliação geral dos usuários sobre o Ricky.

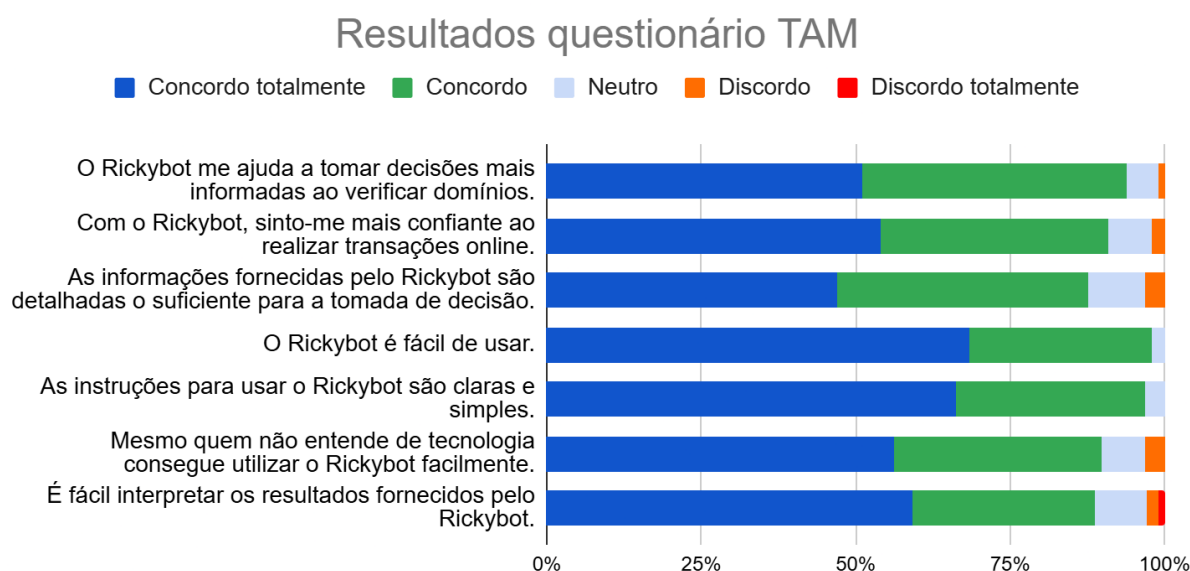


Figura 10 – Gráfico representando os resultados do questionário TAM

5.10 Análise das Questões de Pesquisa

Com base nos dados obtidos por meio da aplicação do questionário estruturado e da análise descritiva, é possível retomar as questões de pesquisa levantadas na Seção 5.3:

1. A ferramenta é considerada fácil de usar?

Os resultados indicam fortemente que a ferramenta Ricky é considerada fácil de usar. Cerca de **98% dos participantes** concordaram com essa afirmação, sendo que **68,4% concordaram totalmente**. Além disso, **96,9% afirmaram que as instruções foram simples e diretas**, o que reforça a percepção de usabilidade.

2. Os usuários percebem utilidade prática na solução?

A percepção de utilidade foi amplamente confirmada. **93,9% dos participantes** relataram que o bot contribuiu para a tomada de decisões mais precisas e detalhadas, fornecendo dados relevantes que ampliaram sua compreensão sobre a confiabilidade dos sites. A clareza das informações foi igualmente destacada, com **88,8% relatando que os resultados apresentados são fáceis de interpretar**. Esses dados indicam que o Ricky oferece benefícios concretos aos usuários no momento da decisão de compra. Um dos participantes, por exemplo, destacou que *“é uma ferramenta muito útil”*, refletindo uma percepção positiva.

3. O Ricky é capaz de influenciar na decisão de compra do usuário?

O impacto na decisão de compra foi evidente: **95,9% dos usuários** relataram que o Ricky ajudou na tomada de decisão sobre realizar ou não uma compra. Além disso, **90,8% dos participantes** afirmaram sentir-se mais confiantes ao realizar transações online após usar a ferramenta, evidenciando que o Ricky exerce influência direta no comportamento dos consumidores. Um usuário também sugeriu a integração com um serviço de reclamações amplamente utilizado no país, escrevendo: *“Ótimo bot! Poderia trazer também informações do Reclame Aqui do site (se houver).”* Essa observação reforça o potencial da ferramenta de evoluir ainda mais no suporte à decisão de compra.

5.11 Discussão

Os resultados obtidos demonstram que o Ricky cumpriu seu objetivo principal de fornecer uma ferramenta acessível e eficiente para auxiliar os usuários na verificação de segurança de domínios em *e-commerce*. A alta taxa de adoção (98%) e o impacto positivo relatado por 95,9% dos respondentes mostram que a solução trouxe um valor significativo para a tomada de decisão dos consumidores.

A facilidade de uso foi um dos aspectos mais elogiados, com unanimidade entre os participantes quanto à simplicidade de navegação no *bot*. Esse resultado confirma a eficácia da escolha do *WhatsApp* como plataforma de interação, além da implementação de uma interface intuitiva.

Por outro lado, os dados revelam que ainda há um cenário preocupante em relação à segurança percebida pelos usuários ao realizarem compras *online*. Com 54% dos respondentes se sentindo inseguros ou muito inseguros, destaca-se a relevância de ferramentas

como o Ricky para mitigar essa vulnerabilidade.

Outro ponto digno de nota é o impacto positivo na confiança dos usuários, com 90,8% relatando sentir-se mais confiantes em suas transações após o uso do *bot*. Essa confiança reflete a clareza das informações apresentadas, consideradas detalhadas por 87,7% dos participantes.

Em síntese, os resultados da pesquisa demonstram que o Ricky não apenas atende à demanda por segurança no *e-commerce*, mas também se destaca como uma solução de fácil acesso, alto impacto e elevado índice de satisfação entre seus usuários.

5.12 Considerações Finais

Seguindo o protocolo de Yin, o estudo demonstrou que a ferramenta Ricky atende aos critérios fundamentais de um estudo de caso aplicado: clareza no objetivo, rigor metodológico, vínculo teórico com modelos consolidados (TAM) e análise objetiva das evidências coletadas. Os dados indicam que o Ricky é uma ferramenta eficaz para aumentar a confiança do consumidor no ambiente de *e-commerce*, preenchendo uma lacuna importante na segurança digital voltada ao usuário final.

6 Conclusão

Este trabalho apresentou uma abordagem para a proteção dos usuários em plataformas de compras na internet, por meio da utilização de um *bot* implementado em um comunicador instantâneo. A proposta foca na realização de consultas de domínios com o TLD `.br`, aproveitando o cadastro obrigatório desses domínios no NIC.br, o que possibilita o acesso a informações administrativas relevantes. O *bot*, denominado Ricky, foi projetado para extrair dados administrativos dos domínios consultados e integrá-los com informações cadastrais da Receita Federal, fornecendo ao usuário uma análise mais detalhada e confiável.

A escolha pelo uso de um comunicador instantâneo, como o *WhatsApp*, visou garantir a acessibilidade e inclusão de um público diversificado, independentemente do nível de familiaridade técnica. Essa abordagem facilitou a implementação do *bot* e simplificou o processo de verificação para os usuários, que podem acessar os dados diretamente por meio de uma interface intuitiva.

6.1 Trabalhos Futuros

A proposta apresentada neste trabalho foi limitada a domínios com o TLD `.br`, o que restringe sua aplicação a domínios brasileiros. Contudo, um próximo passo para ampliar o alcance da ferramenta seria a implementação de consultas para domínios com outros TLDs. Isso exigiria a adaptação do *bot* para lidar com diferentes sistemas de registro e fontes de dados. Além disso, seria necessário desenvolver mecanismos para validar a relação entre domínios estrangeiros e empresas nacionais, considerando que muitas organizações brasileiras utilizam domínios internacionais, como `.com` ou `.net`, além do `.br`. Para esses casos, seria preciso cruzar informações de registro, como dados de titularidade e endereço, para confirmar a propriedade nacional dos domínios. Também seria interessante explorar a integração com outras bases de dados relevantes para a segurança digital e ampliar as funcionalidades do *bot*, oferecendo uma ferramenta ainda mais robusta para a verificação de domínios na internet.

Referências

- ABCOMM, A. B. d. C. E. **Crescimento do ecommerce brasileiro**. 2025. <<https://dados.abcomm.org/crescimento-do-ecommerce-brasileiro>>. Acessado em: 26 abr. 2025.
- BATISTA, C. S.; SOUZA, M. H. *et al.* Uma análise do chatbot bia (bradesco inteligência artificial) a partir de um levantamento bibliográfico. Insitituto Federal de Educação, Ciência e Tecnologia de Goiás, 2023. Disponível em: <<https://repositorio.ifg.edu.br/handle/prefix/1434>>.
- BRASIL. **LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990**. Brasília, DF: [s.n.], 1990. <https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acessado em: 7 jan. 2025.
- BRASIL. **DECRETO Nº 7.962, DE 15 DE MARÇO DE 2013**. Brasília, DF: [s.n.], 2013. <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm>. Acessado em: 7 jan. 2025.
- CARVALHO, B.; LAZARIN, N. Análise de dados administrativos de e-commerce: Uma abordagem focada no cliente. In: **Anais Estendidos do XXIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais**. Porto Alegre, RS, Brasil: SBC, 2023. p. 243–248. ISSN 0000-0000. Disponível em: <https://sol.sbc.org.br/index.php/sbseg_estendido/article/view/27296>.
- COSTA, A. R. d. S. **Certificação e-Business: Desenvolvimento de Uma Proposta de Melhoria para a Especificação QWEB**. Tese (Doutorado), 2011. AAI30228577. Disponível em: <<https://dl.acm.org/doi/abs/10.5555/AAI30228577>>.
- CRUZ, W. L. d. M. Crescimento do e-commerce no brasil: desenvolvimento, serviços logísticos e o impulso da pandemia de covid-19. **GeoTextos**, v. 17, n. 1, jul. 2021. Disponível em: <<https://periodicos.ufba.br/index.php/geotextos/article/view/44572>>.
- DAIGLE, L. **WHOIS Protocol Specification**. RFC Editor, 2004. RFC 3912. (Request for Comments, 3912). Disponível em: <<https://www.rfc-editor.org/info/rfc3912>>.
- DAVIS, F.; DAVIS, F. Perceived usefulness, perceived ease of use, and user acceptance of information technology. **MIS Quarterly**, v. 13, p. 319–, 09 1989. Disponível em: <<https://www.jstor.org/stable/249008>>.
- FEITOSA, D. d. L.; GARCIA, L. S. Sistemas de reputação: Um estudo sobre confiança e reputação no comércio eletrônico brasileiro. **Revista de Administração Contemporânea**, Associação Nacional de Pós-Graduação e Pesquisa em Administração, v. 20, n. 1, p. 84–105, Jan 2016. ISSN 1415-6555. Acessado em: 7 jan. 2025. Disponível em: <<https://doi.org/10.1590/1982-7849rac20161578>>.
- FILHO, N. S.; ROSSI, R. R. Chatbot Based Solution for Supporting Software Incident Management Process. **Journal of Software**, v. 15, n. 3, p. 68–73, maio 2020. ISSN 1796217X. Disponível em: <<https://doi.org/10.17706/jsw.15.3.68-73>>.
- GERMANI, L. A. Existência do cnpj. **AgroANALYSIS**, v. 27, n. 5, p. 28–28, 2007. Disponível em: <<https://periodicos.fgv.br/agroanalysis/article/view/35989>>.

GLOBAL, S. **Uso do WhatsApp pelos brasileiros**. 2024. Disponível em: <<https://santini.global/uso-whatsapp-brasileiros/>>.

IDTECH, U. **Metade dos consumidores brasileiros já foi vítima de fraude no e-commerce**. 2022. Acessado em: 7 jan. 2025. Disponível em: <<https://mercadoeconsumo.com.br/01/11/2022/ecommerce/metade-dos-consumidores-brasileiros-ja-foi-vitima-de-fraude-no-e-commerce/>>.

MOREIRA, D. **E-commerce durante e a pandemia e o aumento do estelionato digital**. [S.l.], 2022. Acessado em: 7 jan. 2025. Disponível em: <<https://repositorio.animaeducacao.com.br/handle/ANIMA/29867/>>.

MOREIRA, J. B. P. de A. **O CRIME DE ESTELIONATO E SUAS IMPLICAÇÕES NA ERA DIGITAL: O CONSTANTE CRESCIMENTO DOS GOLPES CIBERNÉTICOS VIA REDES SOCIAIS**. [S.l.], 2023. Disponível em: <<https://pensaracademico.unifacig.edu.br/index.php/repositoriottcc/article/view/4173>>.

MOTA, M. d. O. **Estudo de caso sobre segurança em e-commerce**. [S.l.], 2021. Pontifícia Universidade Católica de Goiás. Acessado em: 7 jan. 2025. <<https://repositorio.pucgoias.edu.br/jspui/handle/123456789/3206>>.

NAMA. **Lu, o chatbot da Magazine Luiza que é queridinho do público**. 2018. <<https://simple.nama.ai/post/lu-o-chatbot-da-magazine-luiza-que-e-queridinho-do-publico>>. Acessado em: 28 abr. 2025.

RODRIGUES, C. G. M. **A aplicação do código de defesa do consumidor na era do comércio eletrônico**. Salvador, 2020. Disponível em: <<https://ri.ucsal.br/handle/prefix/2687>>.

RODRIGUEZ-ARRASTIA, M.; MARTINEZ-ORTIGOSA, A.; RUIZ-GONZALEZ, C.; ROPERO-PADILLA, C.; ROMAN, P.; SANCHEZ-LABRACA, N. Experiences and perceptions of final-year nursing students of using a chatbot in a simulated emergency situation: A qualitative study. **Journal of Nursing Management**, v. 30, n. 8, p. 3874–3884, 2022. Disponível em: <<https://onlinelibrary.wiley.com/doi/abs/10.1111/jonm.13630>>.

SILVA, M. B. F. d. **Cibersegurança: Uma visão panorâmica sobre a segurança da informação na Internet**. Rio de Janeiro, RJ: Freitas Bastos Editora, 2023. ISBN 9786556752440.

SILVA, S. J. A. da; VILLAMAGNA, M. R.; SANTOS, E. G.; COELHO, I. B. Previsão da indústria de domínios de internet no brasil (pp. 128). **Revista da Estatística da Universidade Federal de Ouro Preto**, v. 2, 2012. Disponível em: <<https://periodicos.ufop.br/rest/article/view/3184>>.

SOBHIE, A. A.; OLIVEIRA, D. C. d. Proteção do consumidor no comércio eletrônico: Inovações relevantes para as vendas on line no brasil a partir do decreto federal nº. 7962/2013. **Revista Eletrônica de Iniciação Científica. Itajaí, Centro de Ciências Sociais e Jurídicas da UNIVALI**, v. 4, n. 4, p. 84–107, 2013. Disponível em: <<https://www.univali.br/graduacao/direito-itajai/publicacoes/revista-de-iniciacao-cientifica-ricc/edicoes/Lists/Artigos/Attachments/934/Arquivo%2006.pdf>>.

VALENTINI, M. A. C. *et al.* O uso de chatbot para identificar riscos em projetos de tecnologia da informação. Universidade Nove de Julho, 2021. Disponível em: <<http://bibliotecatede.uninove.br/handle/tede/2484>>.

WINTER, C. E. T. W. E. T.; KLEIN, D. H.; LAZARIN, N. M. Uma proposta de ferramenta de análise de dados administrativos como estratégia defensiva ao estelionato digital. In: **Anais do XV Computer on the Beach - COTB'24**. Balneário Camboriú - Santa Catarina - Brasil: Universidade do Vale do Itajaí, 2024. p. 315–317. Disponível em: <<https://periodicos.univali.br/index.php/acotb/article/view/20379>>.

YIN, R. K. **Estudo de Caso-: Planejamento e métodos**. [S.l.]: Bookman editora, 2015.