A Segurança da Informação e a Garantia da Integridade Social Cibernética Contemporânea

GEOVANNA RODRIGUES
LUCAS STOCCO SOLDERA
RICARDO PRADO
JOÃO EMMANUEL D'ALKMIN NEVES

Resumo

Este artigo aborda a relevância da Segurança da Informação no contexto social e tecnológico contemporâneo, com o objetivo de aprofundar o debate sobre sua importância e promover a conscientização sobre o tema. A metodologia deste estudo combina revisão bibliográfica e pesquisa de campo. Primeiramente, explora o desenvolvimento histórico e as tendências futuras da Segurança da Informação, analisando também os impactos das tecnologias em processos sociais e empresariais. A pesquisa inclui uma comparação de investimentos em segurança entre empresas de diferentes portes e avalia o conhecimento dos usuários sobre o tema. A abordagem visa identificar lacunas na aplicação de práticas de segurança e correlacionar o conhecimento com a percepção sobre sua importância. Os resultados indicam que, apesar da crescente conscientização sobre os riscos cibernéticos, ainda existem lacunas significativas na aplicação da Segurança da Informação, evidenciando a necessidade de maiores investimentos e capacitação para garantir a proteção da ordem social e empresarial. Conclui-se que a área exige maior atenção para a mitigação de riscos e a promoção de práticas mais eficazes de proteção da informação.

Palavras-chave*:* Segurança da Informação; Sociedade Digital; Ataques Cibernéticos; Investimento em Segurança.

Information Security and Ensuring Contemporary Cyber Social Integrity

Abstract

This article addresses the relevance of Information Security in the contemporary social and technological context, aiming to deepen the discussion on its importance and raise awareness on the topic. The methodology combines a literature review with field research. It first explores the historical development and future trends of Information Security, also analyzing the impact of technologies on social and business processes. The study includes a comparison of investments in security among companies of different sizes and assesses users' knowledge on the subject. The approach aims to identify gaps in the implementation of security practices and correlate knowledge with perceptions of its importance. The results indicate that, despite increasing awareness of cybersecurity risks, significant gaps remain in the application of Information Security, highlighting the need for greater investments and training to ensure the protection of social and business order. It is concluded that the field requires more attention to risk mitigation and the promotion of more effective information protection practices.

Keywords: *Information Security; Digital Society; Cyber Attacks; Security Investment.*

---

1 INTRODUÇÃO

Entende-se por "integridade social" o ato de compreender que uma ação individual tem influência, positiva ou negativa, sobre as demais pessoas. Ou seja, é um senso de coletividade que, se bem utilizado, gera o bom convívio (Nodirbek, 2023). No mundo cibernético, essa premissa se mantém igualmente válida. Atividades maliciosas realizadas através da internet e outros meios digitais prejudicam milhares de pessoas e empresas todos os dias. Essas ações, na maioria das vezes, são motivadas por interesses financeiros ou pela busca de alguma vantagem

sobre as vítimas, e é exatamente contra esse cenário que os estudos de Segurança da Informação vêm intensificando seus esforços.

Desta forma, o quanto a Segurança da Informação, enquanto área do conhecimento, é intrínseca a garantir a integridade da sociedade em que vivemos? A Segurança da Informação é fundamental para garantir a integridade da sociedade contemporânea, mediante crescimento exponencial da Tecnologia da Informação, pois sua aplicação efetiva reduz significativamente os riscos associados a vazamentos de dados, ataques cibernéticos e interrupções nos serviços essenciais, assegurando a estabilidade de processos sociais, econômicos e governamentais.

Neste contexto, a integridade social no mundo digital não se limita apenas à coexistência pacífica, mas também à preservação da confiança e da estabilidade (Oliveira, 2022). O propósito subentendido é que promover uma cultura de integridade social no ciberespaço pode ser uma estratégia eficaz para mitigar ameaças e fortalecer a confiança nas interações online.

O objetivo geral deste trabalho é de contribuir na compreensão da relação entre Segurança da Informação, integridade social cibernética e o impacto desses fatores no ambiente digital que segue em constante evolução. Ao contextualizar o problema, explorar hipóteses e traçar um escopo, este trabalho busca apontar uma nova perspectiva para pesquisadores, educadores, formuladores de políticas e demais profissionais de segurança cibernética.

Assim, o estudo justifica-se pela necessidade de reforçar o debate acadêmico e prático, proporcionando conscientização sobre a importância da Segurança da Informação em um cenário de constante evolução tecnológica e crescente vulnerabilidade social.

2 DESENVOLVIMENTO

O desenvolvimento reúne, de maneira clara e sistemática, os principais elementos da pesquisa. Estruturado em seções e subseções, inicia-se com uma fundamentação teórica do tema.

2.1 Quadro teórico

Para o desenvolvimento do referencial teórico deste artigo, optou-se pela estrutura organizada em três seções: inicialmente, discute-se a importância da segurança da informação como um pilar estratégico nas organizações e na sociedade (2.1.1); em seguida, aborda-se a dimensão humana, destacando aspectos como comportamento, privacidade e conscientização (2.1.2); por fim, são exploradas as consequências da negligência na segurança da informação, bem como os desafios que tendem a se intensificar no futuro (2.1.3). Essa divisão visa oferecer uma base sólida para a compreensão crítica do tema e fundamentar as discussões desenvolvidas ao longo do artigo.

2.1.1 A Importância da Segurança da Informação nos setores empresarial e social

O acelerado progresso tecnológico trouxe consigo uma mudança de paradigma em diversos aspectos de vivência nas grandes metrópoles, de maneira geral, as cidades inteligentes envolvem uma variedade de tecnologias essenciais, como inteligência artificial, *big data*, *machine learning*, internet das coisas, 5G e computação em nuvem (Faustino, 2023). Seus avanços influenciaram na forma de produzir, organizar e trabalhar com a diversidade de dados disponíveis em diferentes meios de comunicação. Essa alta flexibilidade resulta em um cenário diversificado para sua atuação, sendo formulada por diversos benefícios atrelados ao seu uso igualmente a diversas preocupações, como por exemplo, a demanda de segurança dos ativos informacionais.

Um exemplo da presença interdisciplinar entre áreas que antes eram distantes pode ser observado no estudo de Souza et al. (2024), que destaca como a implementação de tecnologias digitais no campo trouxe uma ampla gama de possibilidades e oportunidades, mas também resultou em vulnerabilidades relacionadas à cibersegurança, especialmente no que diz respeito à big data, envolvendo grandes volumes de dados sensíveis.

Segundo Durkheim (1895), a sociedade é uma realidade autônoma e distinta dos indivíduos que a compõem, caracterizada por normas e valores que exercem influência sobre os comportamentos coletivos.

Barbosa, Ferreira e Neves (2023), destacam que a segurança é o principal fator para prevenir ataques, garantindo proteção contra a modificação de dados, a indisponibilidade de sites, o vazamento de informações e outros problemas relacionados.

Serviços hospitalares também expõem seus beneficiados à Segurança da Informação, incluindo ameaças de software e hardware capazes de colocar em risco o estado clínico de pacientes. Em função disso, no Brasil foi criado o Departamento de Saúde Digital, e logo após, a Comissão Intergestores Tripartite (CIT) instituiu o Comitê Gestor de Saúde Digital (CGSD), que substituiu o antigo Comitê Gestor da Estratégia de e-Saúde (Rachid et al., 2023).

De acordo com a pesquisa conduzida por Godson, Ngarukon e Oreku (2023), é possível inferir que o monitoramento contínuo de segurança está associado de forma positiva e estatisticamente significativa aos controles de segurança dos registros de saúde eletrônicos em hospitais públicos da Tanzânia.

Em termos de educação, que é o principal esteio da sociedade, também se vê a presença do fenômeno da digitalização nas instituições de ensino, as quais também estão sujeitas ao cumprimento de leis de proteção de dados e disponibilidade de serviços. Todavia o processo de transformação ainda está embrionário, como exemplificado na pesquisa de Bezerra a qual o índice de satisfação com a proteção de dados obtido no campus da universidade a partir da média das respostas, foi de 2,85, o que o posiciona na categoria "Insuficiente". A maioria dos respondentes optou por uma postura neutra em suas respostas, refletindo uma percepção de insatisfação geral (Bezerra, 2024).

Segundo Tømte, Edelhard e Smedsrud (2023), embora os municípios tenham relatado contar com cobertura 1:1 e infraestrutura digital, apenas um deles dispõe de sistemas avançados para garantir a Segurança da Informação e a privacidade.

2.1.2 A dimensão humana: comportamento, privacidade e conscientização em Segurança da Informação

A crescente relevância da Internet como um meio de comunicação essencial tem alterado profundamente diversas áreas de nossas vidas, influenciando desde o trabalho até a maneira como compramos, nos comunicamos, aprendemos e nos entretemos (Vieira; Dian, 2023). Decorre que ao ser participante de uma rede digital, usuários alocam na internet muito além do que está publicamente exposto. Disso, ergue-se o questionamento sobre o nível de preocupação de tais usuários em relação à segurança de seus dados mais restritos.

A preocupação com a privacidade dos usuários é evidente, conforme destacado por Araújo, Soares e Sousa (2020). Os usuários se encontram em um dilema ao utilizar diversos aplicativos e redes sociais para aumentar sua produtividade e interação social digital, visto que muitas vezes são obrigados a aceitar termos de política de privacidade que não oferecem informações claras e abrangentes sobre o tratamento de seus dados pessoais. Araújo, Soares e Sousa (2020), afirmam ainda, que existe um desequilíbrio entre a escolha pela conveniência dos serviços digitais e a proteção da privacidade dos dados pessoais.

Fatidicamente, o esforço primordial de proteção deveria provir dos próprios titulares de dados, entretanto, a maioria dos usuários negligência hábitos de segurança, o fator humano é

frequentemente apontado como o elo mais fraco na gestão de segurança da informação, devido à sua complexidade, que envolve emoções, comportamentos e outras questões relacionadas (Akayama Kanagusku; Gaseta, 2023). Nesse cenário, a conscientização e a educação dos usuários desempenham um papel fundamental em relação à eficácia da Segurança da Informação.

2.1.3 Consequências da falta de segurança e desafios futuramente enfrentados

Nos primórdios da computação, os sistemas eram isolados em ambientes controlados devido ao tamanho e dificuldade de acesso, limitando a interação a um grupo restrito. A segurança estava ligada à localização física (IT.S, 2023). Com a crescente acessibilidade, surgiram senhas e permissões de usuários. A falta de conscientização sobre riscos cibernéticos era comum devido à menor prevalência de ameaças.

A história da segurança de dados teve início por volta de 1950, quando se reconheceu o valor intrínseco dos dados durante a era da informação digital no século XX. No entanto, com a progressiva quantidade de dados armazenados, a percepção sobre o valor dos dados mudou, especialmente em relação a informações pessoais identificáveis (Avast, 2023). A introdução do acesso online e da internet aumentou ainda mais esse risco, já que as empresas compartilhavam, vendiam e reempacotavam dados, gerando preocupações adicionais (Avast, 2023).

A negligência na Segurança da Informação pode acarretar consequências graves em diversas situações. No âmbito empresarial, a ausência de medidas apropriadas de segurança pode resultar na exposição de dados sensíveis, comprometendo a privacidade e confidencialidade das informações, o que leva à perda de confiança por parte dos clientes, danos à reputação da empresa e possíveis implicações legais, ressaltando sanções, diretrizes pautadas pela Autoridade Nacional de Proteção de Dados (ANPD) na Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023.

Em setores sensíveis, como saúde e finanças, a negligência da segurança pode ter implicações mais sérias, violando regulamentações e prejudicando diretamente a vida e o bem-estar das pessoas afetadas pelo vazamento de suas informações. Um forte exemplo é o ataque cibernético ao Hospital Ciudad Neily, foi implementado um plano de contingência que utilizava métodos físicos, como documentos e formulários em papel, para garantir o atendimento aos pacientes em serviços de emergência e internação (Ulloa, 2023).

Ainda, em ambientes governamentais, a indiferença à proteção dos dados pode comprometer a segurança nacional ao permitir o acesso não autorizado a informações estratégicas e confidenciais, visível no conflito entre a Rússia e a Ucrânia frequentemente caracterizado como uma guerra híbrida, pois, além da mobilização das forças militares, inclui o uso de outros recursos, como ataques cibernéticos, que começaram antes da invasão terrestre (Fonseca, 2023).

Nos últimos anos, casos notórios de falhas na Segurança da Informação tornaram-se amplamente conhecidos, recebendo destaque nos noticiários. Em 2016, o Banco Central do Brasil enfrentou um ataque cibernético, ressaltando as ameaças à segurança de instituições financeiras (Bertolucci, 2022). No ano de 2018, veio à tona o escândalo envolvendo a Cambridge Analytica, que acessou indevidamente dados de cerca de 87 milhões de usuários do Facebook (G1, 2022).

A partir de 2020, houve um aumento substancial nos casos de ataques cibernéticos e vazamentos de dados, impulsionado pela pandemia de COVID-19 (Barbosa, 2021). O trabalho remoto e a exploração de vulnerabilidades levou ao aumento de ataques de *phishing* e *ransomware*, além da expansão do cibercrime como serviço. Exemplos notáveis incluem ataques direcionados a hospitais e organizações de pesquisa médica. Durante as eleições municipais de 2020, o Tribunal Superior Eleitoral (TSE) foi alvo de tentativas de ataques

cibernéticos, aumentando preocupações sobre a integridade dos processos eleitorais e a segurança das informações eleitorais (Arbex, 2020). Ainda em tempo de pandemia, no Brasil, o Ministério da Saúde enfrentou ataques cibernéticos que impactaram a divulgação de dados relacionados à COVID-19 (Aragão, 2022).

De acordo com dados da *Check Point Research* (CPR) citados pelo *Cointelegraph* (2023), houve um aumento de 7% na média global de ataques cibernéticos contra organizações no primeiro trimestre de 2023 em comparação com o mesmo período do ano anterior. O número de ataques semanais por organização atingiu 1.248 neste ano, enquanto no período de janeiro a março de 2022, os dados indicavam aproximadamente 1.160 investidas digitais.

2.2 Materiais e Métodos

A metodologia adotada será exploratória e comparativa, analisando o histórico da Segurança da Informação desde sua concepção até os dias atuais. O estudo visa compreender os cenários e impactos decorrentes da ampla adoção ou negligência dessa área nas empresas e na sociedade em geral. O público-alvo inclui toda a sociedade interessada na proteção de dados, empresas de todos os portes e entusiastas em tecnologia.

Tendo em vista isso, foram realizadas as seguintes etapas: revisão bibliográfica, explorando a literatura, artigos e revistas técnicas existentes sobre a Segurança da Informação; estudo de casos, analisando casos específicos de ataques cibernéticos, selecionando incidentes significativos visando ressaltar a importância da conscientização sobre a proteção digital; análise comparativa, do investimento em segurança da informação entre empresas de diferentes portes; uma pesquisa de campo realizada na comunidade, através de um formulário produzido através do Microsoft Forms com questões a fim de testar o conhecimento popular sobre alguns princípios elementares de Segurança da Informação, aplicada a públicos de diferentes idades e áreas de trabalho, os quais cederam suas respostas de maneira voluntária cientes da finalidade, não se limitando apenas a atuantes e/ou estudantes de sistemas de informação e segurança. A amostra totalizou sessenta (60) respostas, estas foram consideradas de forma anônima, cujo compartilhamento para responder foi feito sem distinções de meio, capacitando qualquer indivíduo de contribuir com o estudo, por fim os dados foram analisados utilizando recursos da própria plataforma como correlação de respostas somados aos insights globais.

2.3 Resultados e discussões

Através do referencial teórico, verifica-se a utilização inconsciente da população a respeito dos recursos de Segurança da Informação, afinal, estão implementados no *background* da maioria das aplicações tecnológicas.

Para ser possível visualizar a valência de algumas práticas primárias de segurança, dependentes exclusivamente dos próprios usuários, foi desenvolvida uma pesquisa através de um formulário digital, as questões abordadas são as apresentadas abaixo:

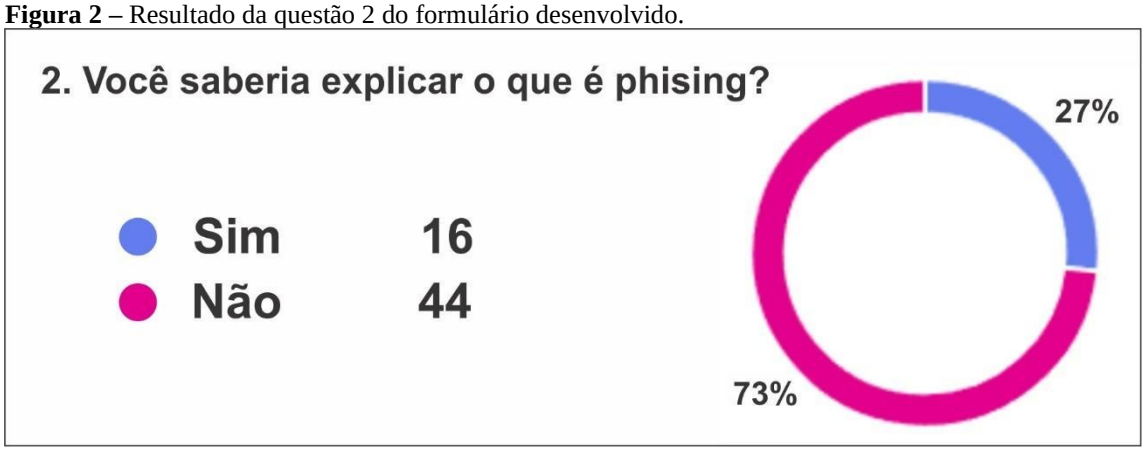
A primeira pergunta questiona sobre a definição de senhas por parte dos usuários e se estes seguem as orientações de utilizarem senhas reforçadas e distintas para cada sistema/*site*/aplicativo. O resultado predominante, conforme ilustrado na Figura 1, foi contrário ao esperado, evidenciando uma falha significativa por parte dos usuários em adotar uma estratégia básica, mas frequentemente recomendada, de segurança.

Figura 1 – Resultado da questão 1 do formulário desenvolvido.

Fonte: Elaborado pelos autores (2024)

O ataque de *phishing* é um dos métodos de engenharia social mais fáceis de ser aplicado, principalmente em usuários leigos. Essa questão foi selecionada a fim de obter um número aproximado de quantos colaboradores da pesquisa estudam ou atuam profissionalmente com sistemas de dados e consequentemente, estão mais familiarizados aos tipos de ataques existentes. Neste caso, como apresentado na Figura 2, foram minoria.

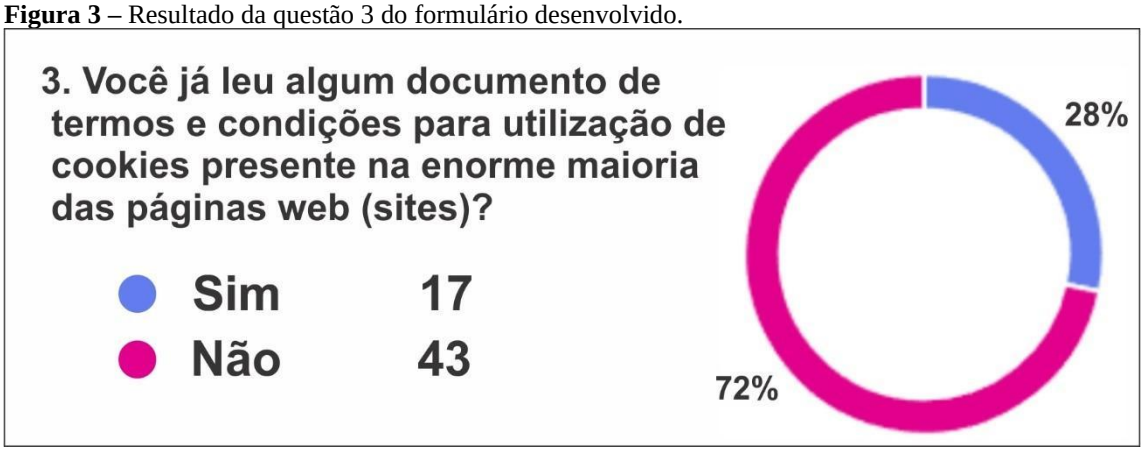
Figura 2 – Resultado da questão 2 do formulário desenvolvido.



Fonte: Elaborado pelos autores (2024)

Com o resultado da questão 3, percebe-se uma grande despreocupação dos titulares com o tratamento e utilização de seus dados. Termos de Condições e Políticas de Privacidade muitas vezes podem não estar em conformidade com a Lei Geral de Proteção de Dados (LGPD), e ainda assim, é possível visualizar através da Figura 3 que a grande maioria de usuários aprovam estes documentos sem lê-los adequadamente.

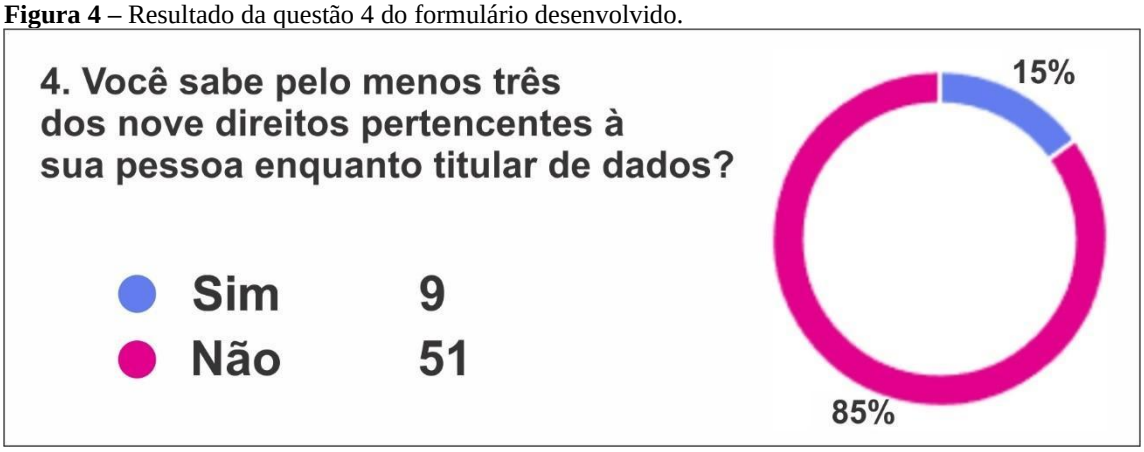
Figura 3 – Resultado da questão 3 do formulário desenvolvido.



Fonte: Elaborado pelos autores (2024)

Conhecer e entender alguns dos direitos estabelecidos aos titulares de dados pode auxiliar nas providências tomadas em caso de violação da privacidade ou integridade dos dados. Como relatado na pesquisa, exibido na Figura 4, o resultado também não é satisfatório, sendo 85% dos colaboradores alheios aos próprios direitos enquanto usuários.

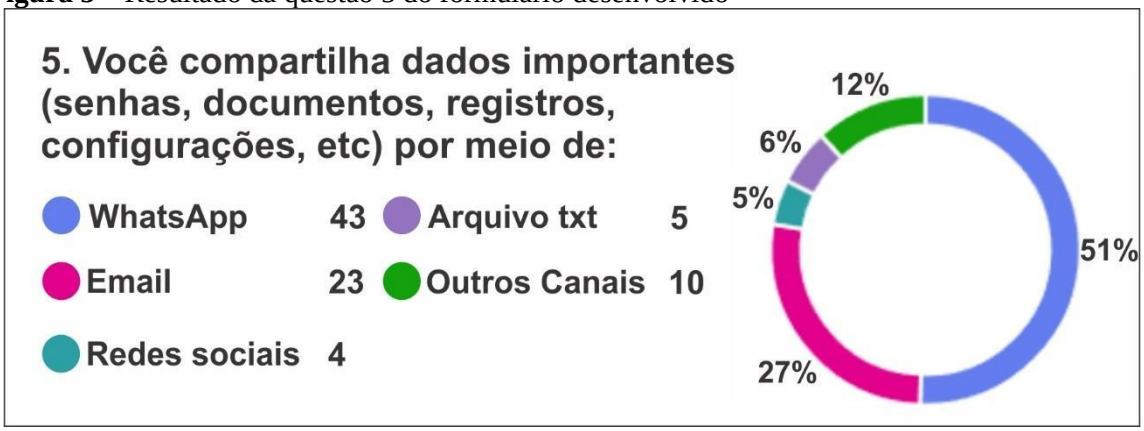
Figura 4 – Resultado da questão 4 do formulário desenvolvido.



Fonte: Elaborado pelos autores (2024)

Por fim, a pesquisa é finalizada oferecendo alternativas assinaláveis de diferentes canais utilizados para a troca de informações importantes e até sensíveis, como e-mail, redes sociais, dentre outros. Conforme exposto na Figura 5, a alternativa com maior público foi o aplicativo de mensagens *WhatsApp*, que oferece bons métodos de segurança como verificação de duas etapas e criptografia ponta a ponta, mas sem a participação do usuário nas condutas de segurança, pode ser facilmente atacado.

Figura 5 – Resultado da questão 5 do formulário desenvolvido



Fonte: Elaborado pelos autores (2024)

Ao considerar a totalidade dos resultados, estes apresentaram um índice de no mínimo 63,5% mais respostas desfavoráveis em relação as favoráveis. Através disso, é possível identificar um déficit na conscientização social em termos de segurança digital e cibernética, o que impacta demasiadamente na eficácia das vias de segurança, por mais avançadas que sejam.

Correlacionando o resultado obtido com a elementaridade da Segurança da Informação para a integridade social, existe uma discrepância entre sua necessidade e aplicação diária por parte dos usuários, o que os tornam suscetíveis a ataques.

3 CONSIDERAÇÕES FINAIS

Este artigo destacou a importância da cibersegurança tanto no contexto empresarial quanto pessoal, evidenciando as disparidades na implementação de práticas de segurança entre grandes corporações e pequenas e médias empresas. Embora as grandes empresas tenham investido significativamente em segurança, os ataques cibernéticos ainda são uma ameaça constante, com potenciais brechas podendo resultar em incidentes graves. Por outro lado, empresas menores carecem de investimentos e conhecimento adequado, o que as torna mais vulneráveis.

A realidade é que a segurança digital está longe de ser uma meta alcançada, com riscos crescendo a cada dia e os esforços, muitas vezes, sendo insuficientes. Enquanto as técnicas criminosas evoluem, a dependência crescente da tecnologia exige uma adaptação contínua e eficaz das práticas de segurança. Nesse cenário, a Segurança da Informação se torna essencial para garantir a integridade da sociedade, protegendo-a de desordens e colapsos. Contudo, os índices de aplicação da segurança ainda superam os obstáculos, refletindo um esforço contínuo em manter a proteção contra as crescentes ameaças digitais.

REFERÊNCIAS

AKAYAMA KANAGUSKU, A. R.; GASETA, E. **Fator humano na segurança da informação: desmistificando o elo mais fraco**. FatecSeg - Congresso de Segurança da Informação, [S. l.], 2023. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/114. Acesso em: 16 nov. 2024.

ARAGÃO, A. **5 grandes vazamentos de dados no Brasil — e suas consequências**. JOTA. 2022. Disponível em: https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil-28012022. Acesso em: 11 nov. 2023.

ARAÚJO, N. V. S.; SOARES, H. J.; SOUZA, P. C. **Privacidade e Segurança Digital: um estudo sobre a percepção e o comportamento dos usuários sob a perspectiva do paradoxo da privacide.** Laboratório de Ambientes Interativos (LAVI). 2020. Disponível em: https://sol.sbc.org.br/index.php/wics/article/view/11040/10911. Acesso em: 20 nov. 2023.

ARBEX, T. **TSE registra 264 ataques contra candidatos em 2020**. CNN. 2020. Disponível em: https://www.cnnbrasil.com.br/politica/tse-registra-ataques-contra-candidatos-em-2020/. Acesso em: 11 nov. 2023.

AVAST. **A história e a evolução da segurança de rede**. Avast. Disponível em: https://www.avast.com/pt-br/business/resources/future-of-network-security#pc. Acesso em: 11 nov. 2023.

BARBOSA, J. S.; SILVA, D. B.; OLIVEIRA, D. C.; JESUS, D. C.; MIRANDA, W. F. A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional. **Research, Society and Development**, [S. l.], v. 10, n. 2, p. e40510212557, 2021. DOI: 10.33448/rsd-v10i2.12557. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/12557. Acesso em: 16 nov. 2024.

BARBOSA, P.; FERREIRA, M.; NEVES, J. E. D. **Abordagem de Segurança no Desenvolvimento de Aplicações Web**. III FatecSeg. 2023. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/107. Acesso em: 15 nov. 2024.

BERTOLUCCI, G. **Grupo hacker diz ter invadido "blockchain" do Banco Central.** Livecoins. 2022. Disponível em: https://livecoins.com.br/grupo-hacker-diz-ter-invadido-blockchain-do-banco-central/. Acesso em: 11 nov. 2023.

BEZERRA, **Eric dos Santos. Desafios na Proteção de Dados e Segurança da Informação em Ambientes Acadêmicos: Um Estudo de Caso na UFERSA Campus Pau dos Ferros.** Universidade Federal Rural do Semi-Árido, 2024. Disponível em: https://repositorio.ufersa.edu.br/server/api/core/bitstreams/dbfb1a36-f9d4-45de-9cb8-165d4ec245e7/content. Acesso em: 15 nov. 2024. p. 43-44.

BRASIL. Agência Nacional de Proteção de Dados (ANPD). **RESOLUÇÃO CD/ANPD Nº 4, DE 24 DE FEVEREIRO DE 2023. Estabelece diretrizes para a implementação de medidas relacionadas à proteção de dados pessoais**. Diário Oficial da União, Brasília, 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-no-4-de-24-de-fevereiro-de-2023-457216519. Acesso em: 16 nov. 2024.

COINTELEGRAPH. **R$ 103 Bilhões Roubados: Brasil É O 2º País Que Mais Sofre Crimes Cibernéticos Na América Latina**. Exame, Future of Money, 2023. Disponível em: https://exame.com/future-of-money/r-103-bilhoes-roubados-brasil-e-o-2o-pais-que-mais-sofre-crimes-ciberneticos-na-america-latina/. Acesso em: 20 nov. 2023.

DURKHEIM, Émile. **Les règles de la méthode sociologique.** Paris: Félix Alcan, 1895. p. 14.

FAUSTINO, Raphael Brito. **A Metrópole digital: para a crítica da economia política das tecnologias de informação e comunicação**. In: INSTITUTO DE PESQUISA ECONÔMICA

APLICADA (IPEA). Cidades inteligentes: desafios e perspectivas. Brasília: Ipea, 2023. p. 123-145. Disponível em: https://repositorio.ipea.gov.br/handle/11058/13472. Acesso em: 15 nov. 2024.

FONSECA, Leila Oliveira da. A guerra cibernética e o conflito Rússia versus Ucrânia. **Revista Relações Exteriores**, 2023. Disponível em: https://relacoesexteriores.com.br/a-guerra-cibernetica-e-o-conflito-russia-versus-ucrania/. Acesso em: 15 nov. 2024.

G1. **Mark Zuckerberg é processado nos EUA devido ao caso Cambridge Analytica**. G1 – Tecnologia. 2022. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/05/23/mark-zuckerberg-e-processado-nos-eua-devido-ao-caso-cambridge-analytica.ghtml. Acesso em: 11 nov. 2023.

GODSON, E.; NGARUKO, D.; OREKU, G. Effects of Continuous Security Monitoring on Security Controls of Electronic Health Records in Public Hospitals, Tanzania. East African **Journal of Business and Economics**, v. 6, n. 1, p. 364-374, 2023.

IT.S. **A evolução da segurança da informação**. IT.S Tecnologia, 2023. Disponível em: https://www.itstecnologia.com.br/artigo/a-evolucao-da-seguranca-da-informacao. Acesso em: 11 nov. 2023.

NODIRBEK, K. M. Information Culture: A New Approach. **World Bulletin of Social Sciences**, v. 19, p. 129-134, 2023. Disponível em: https://scholarexpress.net/index.php/wbss/article/view/2228. Acesso em: 17 nov. 2023.

OLIVEIRA, F. S. **Uma análise do processo de Segurança da Informação: um estudo multicasos**. UniRitter, 2022. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/30445. Acesso em: 11 nov. 2023.

RACHID, R.; FORNAZIN, M.; CASTRO, L.; GONÇALVES, L. H; PENTEADO, B. E. Saúde digital e a plataformização do Estado brasileiro. **Ciência & Saúde Coletiva**, v. 28, n. 7, p. 2143-2153, 2023. Disponível em: https://doi.org/10.1590/1413-81232023287.14302022. Acesso em: 16 nov. 2024.

SOUZA, A. L. O.; BASTOS, C. V.; SANTOS, P. M. S.; SOARES, N. M.; NEVES, J. E. D. Cibersegurança na Agricultura de Precisão: Exploração à Aplicação de Medidas Preventivas. **Advances in Global Innovation & Technology**, v. 2, 61-73 p., 2024. Disponível em: https://doi.org/10.29327/2384439.2.2-5. Acesso em 15 nov. 2024.

TØMTE, C. E.; SMEDSRUD, J. Governance and Digital Transformation in Schools with 1:1 Tablet Coverage. **Frontiers in Education**, v. 08, 2023. Disponível em: https://www.frontiersin.org/articles/10.3389/feduc.2023.1164856. Acesso em: 11 nov. 2023.

ULLOA, M. L. Ataque cibernético al Hospital Ciudad Neily, Caja Costarricense Seguro Social, acciones realizadas, 31 de mayo-31 de agosto 2022. **Repertorio Científico**, [S. l.], v. 25, n. 3, p. 35–42, 2023. DOI: 10.22458/rc.v25i3.4744. Disponível em: https://revistas.uned.ac.cr/index.php/repertorio/article/view/4744. Acesso em: 15 nov. 2024.

VIEIRA, G.; DIAN, M. de O. Impacto e crescimento da internet nos últimos anos. **Revista Interface Tecnológica**, [S. l.], v. 20, n. 1, p. 122–133, 2023. DOI: 10.31510/infa.v20i1.1656.

Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/1656. Acesso em: 16 nov. 2024.