CRIPTOGRAFIA E PRIVACIDADE DOS DADOS

Igor Florentino Amaro
Faculdade Tecnologica de Assis
igor.amaro01@fatec.sp.gov.br

Cleber Henrique de Oliveira
Faculdade Tecnologica de Assis
cleber.oliveira16@fatec.sp.gov.br

RESUMO

Este Trabalho de Graduação aborda a Segurança da Informação, concentrando-se na criptografia e na preservação da privacidade frente às ameaças cibernéticas. Destaca-se o papel crucial da criptografia na proteção dos dados digitais, abarcando desde comunicações online até transações financeiras, e explora-se regulamentações de privacidade, ameaças emergentes como ransomware e desafios éticos. No referencial teórico, são abordados os conceitos essenciais da segurança da informação, incluindo os pilares de disponibilidade, integridade e confidencialidade, enfatizando a importância da gestão na segurança dos dados e medidas complementares à criptografia. A metodologia adotada é qualitativa e indutiva, fundamentada na revisão da literatura. Na apresentação dos resultados, destaca-se a preocupação dos usuários de internet com a privacidade dos dados, sublinhando a necessidade de governança e proteção de informações sensíveis.

Palavra-chave: Segurança da Informação, Criptografia, Privacidade de Dados, Proteção de Dados.

ABSTRACT

This Undergraduate Thesis addresses Information Security, focusing on cryptography and privacy preservation against cyber threats. The crucial role of cryptography in protecting digital data is emphasized, encompassing everything from online communications to financial transactions, while also exploring privacy regulations, emerging threats like ransomware, and ethical challenges. The theoretical framework covers essential concepts of information security, including the pillars of availability, integrity, and confidentiality, emphasizing the importance of data management in security and complementary measures to cryptography. The methodology adopted is qualitative and inductive, grounded in literature review. In presenting the results, the concern of internet users regarding data privacy is highlighted, emphasizing the need for governance and protection of sensitive information.

Keywords: Information Security, Cryptography, Data Privacy, Data Protection.

1. INTRODUÇÃO

Este Trabalho de Graduação se dedica a explorar a temática crucial da Segurança da Informação, com especial enfoque na criptografia e na preservação da privacidade e dos dados. Nosso objetivo primordial é compreender o papel essencial desempenhado pela criptografia na manutenção da confidencialidade e integridade dos dados digitais, além de sua significativa contribuição para salvaguardar a privacidade de indivíduos e organizações num cenário digital em constante evolução (FONTES, 2006).

Destaca-se a crescente urgência de proteger dados pessoais e corporativos diante da contínua ameaça cibernética, onde a privacidade é considerada um direito fundamental. Nesse sentido, investiga-se como a criptografia, ao converter informações em formato ilegível e permitir sua decodificação apenas por meio de chaves apropriadas, atua como uma barreira eficaz contra acesso não autorizado. Adicionalmente, exploram-se diversas aplicações da criptografia, desde a segurança de comunicações online até a proteção de dados em servidores e dispositivos móveis, incluindo seu papel na autenticação de usuários e em transações financeiras (OLIVEIRA e FIGUEIRAS, 2022).

Analisa-se, também, o panorama das regulamentações de privacidade de dados, como o GDPR, para evidenciar a crescente conscientização sobre a privacidade como um direito fundamental e a necessidade de conformidade. Paralelamente, discutem-se ameaças emergentes, como ataques de ransomware, enfatizando a importância de estratégias avançadas de criptografia. Abordam-se, ainda, desafios éticos e sociais, incluindo o equilíbrio entre segurança cibernética e liberdade individual, assim como implicações para a vigilância governamental e a ética empresarial. Em síntese, oferece-se uma visão abrangente da importância crítica da criptografia e da privacidade de dados na era digital, sublinhando a necessidade contínua de inovação e vigilância na proteção de informações sensíveis e na preservação dos direitos individuais (OLIVEIRA e FIGUEIRAS, 2022).

Neste estudo, busca-se compreender e avaliar a importância da criptografia na segurança da informação, investigando seu papel na proteção da privacidade dos dados e na mitigação de ameaças cibernéticas. O objetivo é contribuir para o desenvolvimento de estratégias eficazes de segurança da informação e conscientização sobre a importância da privacidade dos dados em ambientes digitais. Num contexto em que a segurança da informação e a privacidade de dados representam preocupações críticas em todo o mundo, torna-se vital compreender e implementar estratégias de proteção de dados, alinhadas às regulamentações de privacidade, visando assim proporcionar uma compreensão mais aprofundada da criptografia e seu papel na segurança da informação e na proteção da privacidade (VIANA *et al.,* 2022).

2. DESENVOLVIMENTO

2.1. Segurança da Informação

A informação é um recurso de valor inestimável, fornecendo insights que possibilitam uma compreensão mais ampla do mundo ao nosso redor, permitindo-nos discernir as causas e consequências dos fenômenos naturais e artificiais que influenciam a vida humana. O uso inteligente da informação impulsiona o avanço e o desenvolvimento, tanto em esferas profissionais quanto pessoais. Para as organizações, em particular, a informação é uma ferramenta vital, utilizada para descobertas, análises, tomadas de decisão estratégica e outros propósitos de grande relevância (FONTES, 2006).

A Política de Segurança da Informação (PSI) representa um conjunto vital de normas e princípios que demandam implementação e atualização em concordância com a LGPD. Conforme destacado pelo Tribunal de Contas da União (TCU) (2012, p. 14), é importante ressaltar que a PSI pode abranger diversas políticas interligadas, incluindo aquelas relacionadas a senhas, backup, contratação e instalação de equipamentos e softwares. É crucial que essas políticas sejam examinadas de maneira clara e objetiva, visando facilitar o entendimento, e que estejam sempre alinhadas às diretrizes e regulamentos para aprimoramento da segurança da informação no âmbito da administração pública (LIMA *et al.,* 2022).

Por essa razão, a segurança dos dados emerge como uma prioridade primordial para todas as organizações. A segurança da informação, portanto, refere-se à proteção e confiabilidade dos dados, garantindo que informações confidenciais sejam acessadas exclusivamente por indivíduos autorizados, preservando assim seu valor. Conforme definido por Fontes (2006, p. 14), a segurança da informação consiste em "um conjunto de orientações, normas, procedimentos, políticas e demais ações que visam proteger o recurso informação, possibilitando a realização dos negócios da organização e o alcance de sua missão". Essa área envolve uma variedade de técnicas, estratégias e normas destinadas a proteger qualquer tipo de dado ou informação, prevenindo que indivíduos mal-intencionados os roubem ou os divulguem de maneira inadequada (FONTES, 2006).

A compreensão da segurança da informação nos leva a distinguir entre dados e informações. Os dados são elementos quantificáveis de informação que, por si só, podem não possuir um significado relevante, como números, letras e imagens. Por outro lado, as informações são a organização e interpretação desses dados, transmitindo um significado e uma compreensão específica sobre um determinado tema (MACHADO, 2014). Conforme Machado (2014, p. 10), um dado é "uma representação, um registro de uma informação" que pode ser quantificado. Além disso, ele afirma que "informação acrescenta algo ao conhecimento de uma

realidade analisada", citando como exemplo a dosagem de um medicamento, o que constitui uma informação de significado relevante.

2.2. Pilares da Segurança da Informação

Atualmente, há conhecimento sobre os pilares ou princípios da segurança da informação, conforme indicado pela TECHNET (2006), órgão vinculado à Microsoft Corporation responsável pela manutenção da Academia Latino-Americana de Segurança da Informação. Os princípios fundamentais da Segurança da Informação delineados pela norma ISO 17799:2000, um padrão internacional direcionado à segurança da informação, conforme indicado pela Technet (2006), são os seguintes:

Disponibilidade: Refere-se à capacidade de acessar informações relevantes para o funcionamento de uma organização sempre que necessário. A disponibilidade ganha significado quando as informações podem ser recebidas e interpretadas por indivíduos.

Integridade: Tem como objetivo assegurar que as informações disponíveis não sejam modificadas, a menos que seja por indivíduos autorizados. Para que a informação mantenha sua integridade e seja útil, é essencial a contribuição do elemento humano.

Confidencialidade: Visa garantir que somente pessoas autorizadas tenham acesso às informações. No entanto, a mera existência dessa regra não assegura a segurança, a menos que o aspecto comportamental seja adequadamente considerado e gerenciado.

De acordo com as considerações de Silva, Carvalho e Torres (2003), a preservação da confidencialidade, integridade e disponibilidade de informações requer a implementação de medidas de segurança. Essas medidas não apenas garantem a segurança dos dados, mas também visam estabelecer a autenticidade e a não repúdio. Independentemente de seus objetivos, todas essas medidas devem ser aplicadas antes que os riscos se materializem. Elas podem ser categorizadas em duas abordagens distintas: proteção e prevenção.

A prevenção se concentra nas ações que buscam evitar a ocorrência de ameaças. Tais medidas são eficazes até o momento em que uma ameaça se transforma em um incidente. De acordo com Silva, Carvalho e Torres (2003), a proteção, por outro lado, visa a implementação de um sistema de informação que tenha a capacidade de inspecionar e detectar ameaças, reduzindo o impacto que ocorre quando essas ameaças se materializam. Em suma, esses pilares da Segurança da Informação representam os princípios-chave para proteger os dados e garantir que eles permaneçam acessíveis, íntegros e confidenciais, contribuindo para a preservação da segurança da informação em um contexto organizacional (SILVA *et al.,* 2003).

2.3. Criptografia

A criptografia é uma presença discreta, integrada ao cotidiano de qualquer usuário, seja em sites, aplicativos ou sistemas mais sofisticados. Sua função principal é manter a confidencialidade das informações que circulam na rede, e é justamente essa sua importância: preservar o direito à privacidade e à proteção de dados (VIANA et al., 2022).

Pessoas possuem informações que desejam manter em sigilo, seja por razões de privacidade em suas redes sociais ou para se protegerem, uma vez que sempre há indivíduos mal-intencionados que poderiam usar essas informações para prejudicar. No entanto, as quantidades de informações que as pessoas lidam pessoalmente são geralmente pequenas em comparação com as vastas quantidades de dados que as empresas utilizam.Quando se trata da segurança das empresas, que envolvem segredos como dados financeiros, estratégias de negócios, resultados de pesquisas e muito mais, está-se lidando com um volume significativamente maior de informações que precisam ser protegidas. Essa proteção é necessária contra ameaças que variam de hackers a concorrentes, e até mesmo funcionários dentro da própria organização (KASPERSKY, 2022).

Atualmente, existem diversas técnicas e métodos de proteção de informações que devem ser implementados em conjunto para garantir a Confidencialidade, Integridade e Disponibilidade. Embora os sistemas operacionais de computadores forneçam algumas medidas de segurança, essas ferramentas por si só não são suficientes (FONTES, 2016). É imperativo adotar uma medida de proteção mais eficaz, que é a criptografia. Conforme Fontes (2006, pág. 8) afirma, "uma das ferramentas mais cruciais para a proteção de dados é a criptografia, que engloba diversos métodos para transformar arquivos legíveis em algo ilegível."

No mercado atual, encontramos uma variedade de criptografias em uso, todas divididas em duas modalidades: criptografia simétrica ou de chave privada e criptografia assimétrica ou de chave pública. A primeira, mais simples, utiliza uma chave única, porém é considerada vulnerável em alguns casos devido ao risco de interceptação da chave simétrica. Isso levou ao desenvolvimento da segunda modalidade. A criptografia assimétrica utiliza duas chaves diferentes: uma chave pública e uma chave privada, proporcionando um nível de segurança mais robusto nas transações online (VIANA et al., 2022).

Segundo Nogueira (2020), a proteção de ponta a ponta por meio de criptografia assimétrica é essencial para garantir a segurança de diversos tipos de informações, incluindo textos, áudios, vídeos, fotos, documentos e até mesmo chamadas telefônicas. Contudo, surge uma preocupação ao considerar o armazenamento desses dados na nuvem. Enquanto essa forma de criptografia protege as informações durante sua transmissão, ao serem armazenadas na nuvem, elas podem perder essa camada de segurança e ficar vulneráveis.

Como mencionado por Juraski e Nunes (2022), a criptografia tem como objetivo proteger dados e informações, independentemente do tipo de ataque. No entanto, é importante destacar que ela não atua isoladamente na segurança da informação. São necessárias outras medidas, como controle de acesso, sistemas de senhas, backups regulares, manutenção de equipamentos, entre outras. No entanto, a criptografia desempenha sem dúvida uma função indispensável nesse contexto.

2.4. Importância da Gestão na Segurança dos Dados

O papel da gestão na segurança e criptografia de dados é crucial para proteger informações sensíveis e garantir a privacidade dos dados. Santos e Silva (2021, p. 9) destacam que a Gestão da Segurança da Informação é baseada na interação entre processos, procedimentos, controles, melhores práticas e tecnologias, orientando os modelos utilizados atualmente. Marcondes (2020) identifica quatro funções distintas na administração da segurança da informação: Planejamento, Organização, Direção e Controle.

O planejamento visa executar processos administrativos com medidas preventivas e ações para reduzir vulnerabilidades e prevenir invasões. A organização abrange procedimentos internos relacionados a recursos humanos, hardware, procedimentos, políticas e outros elementos. A direção envolve a capacidade dos gestores de liderar equipes, motivá-las por meio de comunicação eficaz e coordenar esforços para atingir objetivos estabelecidos. Por último, o controle identifica falhas e as corrige (SANTOS e SILVA, 2023).

É importante destacar que a segurança da informação vai além dos sistemas de informação e computadores, incluindo qualquer ativo que contenha informações. Ter controle de acesso aos sistemas é tão essencial quanto instalar antivírus. Essa abordagem ampla é crucial para proteger dados e garantir a integridade das informações em todos os níveis da organização (SILVA, 2022).

Nessa perspectiva, Santos e Silva (2023) ressaltam que a administração da informação segue normas e princípios estabelecidos em políticas de segurança para prevenir vazamentos e proteger contra ataques cibernéticos. Ataques cibernéticos, perpetrados por "crackers", estão se tornando mais frequentes, visando organizações suscetíveis para ataques direcionados ou explorando qualquer vulnerabilidade (SANTOS e SILVA, 2023).

Silva (2022) alerta que permitir acesso livre aos funcionários pode ser um grande erro em termos de segurança, aumentando o risco de roubo de dados, vazamentos e danos no sistema. É recomendável implementar um controle rigoroso sobre esses acessos, limitando-os a pessoas selecionadas e capacitadas. Nunca utilizar senhas fracas e garantir atualizações regulares são medidas essenciais para evitar acesso não autorizado e manter a rede segura.

Além disso, é crucial que os colaboradores compreendam a importância de manter os sistemas atualizados. Atualizações regulares corrigem falhas e vulnerabilidades que poderiam expor os dados da empresa a ameaças. Contratar serviços de monitoramento e suporte de TI é uma medida valiosa para detectar e responder rapidamente a atividades suspeitas, reduzindo o risco de incidentes de segurança (SILVA, 2022).

3. METODOLOGIA

Este estudo adota uma abordagem indutiva, permitindo a ampliação de uma teoria existente, através da observação de fenômenos específicos, identificação de regularidades entre eles e generalização do objeto de investigação. Nessa perspectiva, a abordagem é classificada como qualitativa, buscando fornecer maior familiaridade com o tema e torná-lo evidente durante a pesquisa.

A revisão da literatura desempenha um papel crucial neste estudo, servindo como alicerce teórico e metodológico. Baseando-se em fontes diversificadas, como livros, artigos acadêmicos e recursos online, como SCIELO, busca-se uma compreensão abrangente e atualizada do campo de estudo. Autores renomados, como Silva (2022), Marcondes (2020) e Nogueira (2020), contribuem significativamente para o embasamento teórico desta pesquisa, fornecendo insights valiosos e perspectivas variadas sobre o assunto em questão.

Nesse contexto, a opção pela abordagem qualitativa se justifica não apenas pela busca de representatividade numérica, mas, sobretudo, pela ênfase na compreensão aprofundada e contextualizada do fenômeno em análise. Como destacado por Goldenberg (1999), essa abordagem permite uma imersão mais profunda no problema de pesquisa, possibilitando uma análise mais reflexiva e interpretativa dos dados coletados. Portanto, este estudo se propõe a não apenas reunir informações, mas também a contextualizá-las e interpretá-las de forma a proporcionar uma compreensão mais abrangente e significativa do tema.

4 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

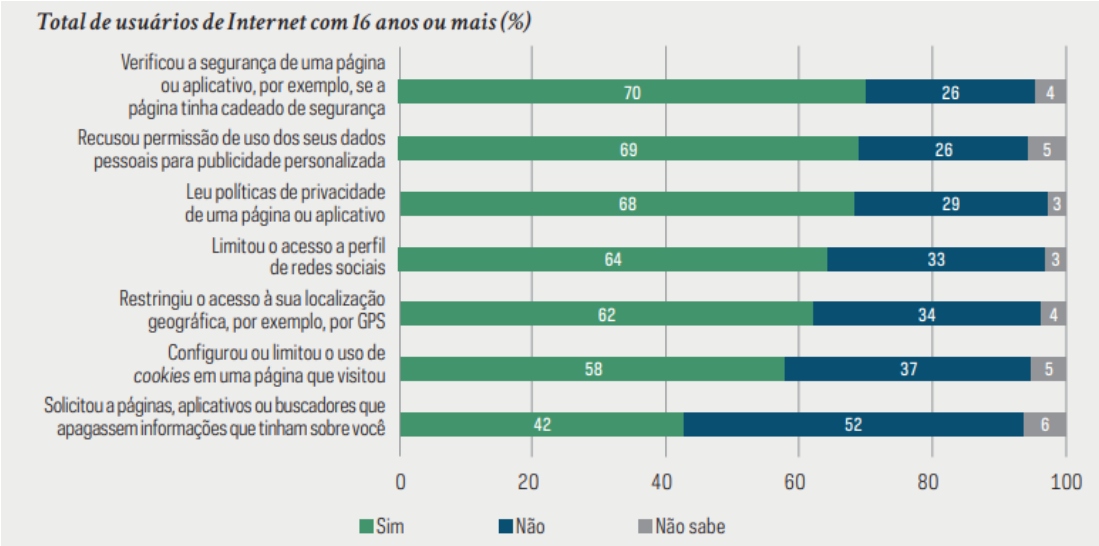
A segurança cibernética é uma prioridade em toda organização, no entanto, isso não é tão evidente na administração pública brasileira, onde muitas vezes há apenas um departamento de Tecnologia da Informação (TI) com diversas responsabilidades, incluindo a segurança da informação. De acordo com a perspectiva da Kaspersky (2022), a segurança cibernética visa proteger computadores, servidores, dispositivos móveis, redes e dados, entre outros, que são alvos de ataques.

No entanto, apesar de todas as recomendações da LAI e do MCI, é evidente que as plataformas e bancos de dados públicos ainda apresentam fragilidades em relação à segurança das informações tanto organizacionais quanto dos cidadãos. Isso ressalta a urgência de adotar práticas computacionais que fortaleçam esses ambientes (LIMA *et al.,* 2022).

Nesse sentido, é recomendável criar um departamento exclusivo para lidar com dados e análises de vulnerabilidades. Além disso, é essencial contratar serviços de Pentest - Teste de Intrusão, que simulam ataques reais e procuram por falhas em aplicações web, analisando o comportamento da empresa e dos colaboradores para identificar imediatamente tentativas de invasão, inclusive explorando técnicas de engenharia social. Também é importante garantir que os funcionários recebam treinamento adequado para identificar possíveis ameaças (LIMA *et al.,* 2022).

De acordo com a CGI.br (2022), uma pesquisa com 2.556 pessoas no Brasil, com 16 anos ou mais, revelou que os usuários de Internet estão preocupados com o uso de seus dados pelo poder público e durante compras em websites e aplicativos. 42% dos usuários se mostraram "muito preocupados" e 25% "preocupados" com a captura e tratamento de seus dados pessoais durante compras online. Além disso, o acesso a páginas e aplicativos de bancos gerou preocupação em 35% dos usuários, seguido pelo uso de apps de relacionamento, que preocupou 22% dos entrevistados, conforme ilustrado na figura abaixo.

Figura 1 – Usuários de internet gerenciam o acesso aos seus dados pessoais.

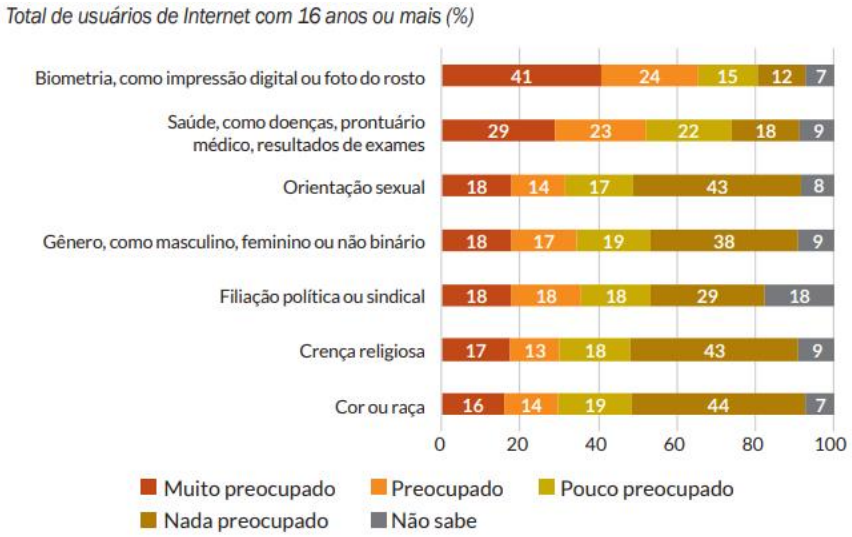


Fonte: CGI.br (2022)

O estudo da CGI.br (2022), também destacou a preocupação dos usuários em relação ao fornecimento de dados considerados sensíveis pela Lei Geral de Proteção de Dados Pessoais (LGPD). Por exemplo, em relação aos dados biométricos, 41% dos usuários de Internet relataram estar muito preocupados e 24% demonstraram preocupação. Da mesma forma, em relação aos dados de saúde, 29% se mostraram muito preocupados e 23% preocupados.

Além disso, foram observadas diferenças significativas entre grupos étnicos. Por exemplo, pretos (35%) e pardos (32%) demonstraram preocupação em proporções maiores do que brancos (26%) com o fornecimento de informações pessoais relacionadas à cor ou raça. O mesmo padrão foi observado em relação à utilização que as empresas fazem de seus dados pessoais. Cinquenta e dois por cento dos usuários autodeclarados pretos e 49% dos pardos afirmaram ficar muito preocupados, enquanto entre os usuários brancos a proporção foi de 43 (CGI.br, 2022).

Figura 2 – Preocupação com o fornecimento de informações pessoais sensíveis.



Fonte: CGI.br (2022)

Portanto, a governança de dados desempenha um papel crucial na gestão eficaz das informações, ao estabelecer políticas e práticas para garantir a qualidade, conformidade e uso apropriado dos dados. Dentro desse contexto, a proteção de dados pessoais assume uma importância central, visando preservar a confidencialidade, integridade e disponibilidade das informações. Essa proteção é essencial para mitigar riscos como acesso não autorizado, perda ou uso indevido dos dados (OYADOMARI *et al.,* 2023).

5 CONSIDERAÇÕES FINAIS

O presente trabalho dedicou-se a explorar a temática da Segurança da Informação, com um enfoque particular na criptografia e na preservação da privacidade e dos dados. Através de uma abordagem abrangente, investigou-se o papel fundamental desempenhado pela criptografia na manutenção da confidencialidade e integridade dos dados digitais, bem como sua contribuição significativa para salvaguardar a privacidade de indivíduos e organizações em um cenário digital em constante evolução.

A crescente urgência de proteger dados pessoais e corporativos diante das ameaças cibernéticas contínuas foi ressaltada, considerando a privacidade como um direito fundamental.

A criptografia foi destacada como uma barreira eficaz contra acesso não autorizado, convertendo informações em formato ilegível e permitindo sua decodificação apenas por meio de chaves apropriadas. Além disso, foram exploradas diversas aplicações da criptografia, desde a segurança de comunicações online até a proteção de dados em servidores e dispositivos móveis, incluindo seu papel na autenticação de usuários e em transações financeiras.

O panorama das regulamentações de privacidade de dados, como o GDPR, foi analisado para evidenciar a crescente conscientização sobre a privacidade como um direito fundamental e a necessidade de conformidade. Paralelamente, discutiram-se ameaças emergentes, como ataques de ransomware, enfatizando a importância de estratégias avançadas de criptografia. Abordaram-se também desafios éticos e sociais, incluindo o equilíbrio entre segurança cibernética e liberdade individual, assim como implicações para a vigilância governamental e a ética empresarial.

No âmbito do referencial teórico, foram explorados os conceitos fundamentais que permeiam a área da segurança da informação, os pilares da segurança da informação (disponibilidade, integridade e confidencialidade) e a importância da gestão na segurança dos dados. Destacou-se a necessidade de medidas de proteção além da criptografia, como controle de acesso, sistemas de senhas e backups regulares.

Quanto à metodologia, adotou-se uma abordagem indutiva qualitativa, com ênfase na revisão da literatura para fornecer uma compreensão aprofundada e contextualizada do tema. Por fim, na apresentação e discussão dos resultados, foram destacadas preocupações dos usuários de internet em relação à privacidade de dados, evidenciando a importância da governança de dados e da proteção de informações sensíveis.

Dessa forma, o trabalho oferece uma visão abrangente e atualizada da importância da criptografia e da privacidade de dados na era digital, sublinhando a necessidade contínua de inovação e vigilância na proteção de informações sensíveis e na preservação dos direitos individuais. Ao contribuir para o desenvolvimento de estratégias eficazes de segurança da informação e conscientização sobre a importância da privacidade dos dados, busca-se promover um ambiente digital mais seguro e confiável para indivíduos e organizações.

6. REFERÊNCIAS

ALMEIDA, M. B. Noções básicas sobre Metodologia de pesquisa científica. Universidade Federal de Minas Gerais. Disponível em: <https://mba.eci.ufmg.br/downloads/metodologia.pdf>. Acesso em 03 de março de 2024.

Comitê Gestor da Internet no Brasil. (2022). Privacidade e proteção de dados pessoais 2021: perspectivas de indivíduos, empresas e organizações públicas no Brasil. São Paulo: CGI.br. <https://cetic.br/pt/publicacao/privacidade-e-protecao-de-dados-2021/>. Acesso em: 20 de abril de 2024

FONTES, Edison Luiz Gonçalves. Segurança da Informação: O usuário faz a diferença. 1. Ed. São Paulo: Saraiva, 2006.

GOLDENBERG, M. A arte de pesquisar: como fazer pesquisa qualitativa em Ciências Sociais. Rio de Janeiro: Record, 1999.

JURASKI, Dairon R.; NUNES, Nathan P. Uma Visão Geral sobre Criptografia, 2018.

KASPERSKY. “O que é cibersegurança?”, 2022. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security#:~:text=Cibersegu-ran%C3%A7a%20%C3%A9%20a%20pr%C3%A1tica%20que,ou%20seguran%C3%A7a%20de%20in-forma%C3%A7%C3%B5es%20eletr%C3%B4nicas.> Acesso em: 20 de abril de 2024.

LIMA, Paulo Ricardo Silva; FERREIRA, Leonardo Matheus Marques; DE ALBUQUERQUE PEIXOTO, Ana Lydia Vasco. Gestão da segurança da informação: análise de políticas de defesa cibernética e estratégias para a proteção de dados e informações da administração pública brasileira. P2P E INOVAÇÃO, v. 9, n. 1, p. 206-221, 2022.

MACHADO, Felipe Nery Rodrigues. Segurança da Informação: Princípios e controle de ameaças. 1. Ed. São Paulo: Saraiva, 2014.

MARCONDES, J. S. Gestão de Segurança da Informação: O que é, o que faz, processos. Disponível em Blog Gestão de Segurança Privada. 2020.

NOGUEIRA, Simone Paes Gonçalves. Um estudo sobre a criptografia. Ensinar Com Alegria, p. 126, 2020.
OLIVEIRA, Eliane; FIGUEIRAS, Rodrigo. A importância da segurança da informação para as organizações. Revista Almoxarifa. Presidente Prudente.2022.

OYADOMARI, Winston; COSTA, Ramon Silva; RIBEIRO, Manuella Maia. Proteção de dados pessoais: privacidade e confiança no ambiente digital. 2023.

SANTOS, Rogério Batista dos; SILVA, Tiago Barros Pontes. Gestão da segurança da informação e comunicações análise ergonômica para avaliação de comportamentos inseguros. RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação, v. 19, p. e021024, 2023.

SILVA T.P; CARVALHO H; TORRES B.C. Segurança dos Sistemas de Informação - Gestão Estratégica da Segurança Empresarial. Portugal. Atlántico, 2003.

SILVA, Beatriz Taynara et al. Gestão de documentos: segurança de dados. 2022.

TECHNET, M., Curso Básico de Segurança da Informação. Microsoft Corporation, EUA, módulo 1 edition, 2006.

VIANA, C., DATTEIN, G., SILVA, J. V., & CAMPOS, P. (2022). CRIPTOGRAFIA E SEGURANÇA. *Revista Científica E-Locução*, *1*(22), 30.