***CAMPUS* PORTO VELHO ZONA NORTE**
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

THALLES DE LIMA BRUNO
THAYNARA CRISTINA ALMEIDA BARROS

SEGURANÇA DA INFORMAÇÃO: UMA REVISÃO DE LITERATURA COM FOCO NAS VULNERABILIDADES DAS REDE WIRELESS PÚBLICAS

PORTO VELHO
2024

THALLES DE LIMA BRUNO
THAYNARA CRISTINA ALMEIDA BARROS

SEGURANÇA DA INFORMAÇÃO: UMA REVISÃO DE LITERATURA COM FOCO NAS VULNERABILIDADES DAS REDE WIRELESS PÚBLICAS

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Tecnólogo em Redes de Computadores pelo Instituto Federal de Educação, Ciência e Tecnologia de Rondônia– Campus Porto Velho Zona Norte.

Orientador: Prof. Me. Silmar Antonio Buchner de Oliveira
Coorientador: Prof. Me. Douglas Moro Piffer

PORTO VELHO
2024

Ficha catalográfica elaborada pelo Sistema Gerador de Ficha Catalográfica do IFRO, com dados informados pelo(a) próprio(a) autor(a).

Bruno, Thalles de Lima.
Segurança da Informação: Uma revisão de literatura com foco nas vulnerabilidades das redes wireless públicas / Thalles de Lima Bruno, Thaynara Cristina Almeida Barros, Porto Velho-RO, 2024.
18 f.

Orientador(a): Prof. Me. Silmar Antonio Buchner de Oliveira.
Coorientador(a): Prof. Me. Douglas Moro Piffer.

Trabalho de Conclusão de Curso (Superior de Tecnologia em Redes de Computadores) – Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO, Porto Velho-RO, 2024.

1. Segurança da Informação. 2. Redes Wifi. 3. Redes Públicas. 4. Vulnerabilidades. I. Barros, Thaynara Cristina Almeida. II. Oliveira, Silmar Antonio Buchner de (orient.). III. Piffer, Douglas Moro (coorient.). IV. Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO. V. Título.

Bibliotecário(a) Responsável: Roseni Santos Rodrigues, CRB-11/916 (Reitoria)

International Contemporary Management Review

ICMR –Volume 05, Número 02, p. 01-18, 2024
ISSN: 2595-0428 - ARTIGO CIENTÍFICO-

SEGURANÇA DA INFORMAÇÃO: UMA REVISÃO DE LITERATURA COM FOCO NAS VULNERABILIDADES DAS REDE WIRELESS PÚBLICAS

Date of receipt: 05/01/2024
Date of acceptance for publication: 05/24/2024

DOI: 10.54033/icmrv5n2-007

Thalles de Lima Bruno[1], Thaynara Cristina Almeida Barros[2], Silmar Antonio Buchner de Oliveira[3] e Douglas Moro Piffer[4]

RESUMO

A segurança da informação é um campo essencial que envolve a análise e proteção contra diversos tipos de riscos associados à informação digital. Neste contexto, a segurança de dados em redes wireless assume um papel crucial, uma vez que está relacionada a diversas condições, desde a escolha dos equipamentos de uma rede até o dispositivo que o usuário está utilizando ao se conectar à internet. Objetivo: Este estudo tem como objetivo aprofundar a compreensão sobre a segurança da informação em redes públicas, identificando as vulnerabilidades específicas das redes wireless e os riscos associados à integridade dos dados nessas redes. Metodologia: A metodologia adotada para este estudo foi uma pesquisa bibliográfica sistemática, que permitiu a análise dos desafios e êxitos documentados na literatura recente. Esta abordagem foi essencial para identificar os pontos críticos e as melhores práticas já estabelecidas no campo da segurança de dados em redes wireless. Resultados: Os resultados desta pesquisa destacaram várias vulnerabilidades significativas nas redes wifi. Entre as mais importantes, foram identificadas questões relacionadas ao "documento digital", "armazenamento de dados", "rede interna" e "ambiente organizacional". Estas vulnerabilidades representam ameaças consideráveis à integridade e à segurança dos dados transmitidos e armazenados em redes wireless, especialmente em ambientes públicos. Considerações Finais: Nas considerações finais, enfatiza-se a importância de implementar medidas imediatas destinadas a aprimorar a abordagem da segurança da informação em redes wireless. Essas medidas incluem a atualização e fortalecimento dos protocolos de segurança, a educação contínua dos usuários sobre práticas seguras ao utilizar redes públicas, e a adoção de tecnologias avançadas de proteção de dados. Somente com uma abordagem proativa e abrangente será possível mitigar os riscos e assegurar a integridade dos dados em redes

[1]Tecnólogo em Redes de Computadores, Campus Porto Velho Zona Norte do Instituto Federal de Rondônia (IFRO), Porto Velho - Rondônia, Brasil. E-mail: thalleslimab@gmail.com
[2]Tecnólogo em Redes de Computadores, Campus Porto Velho Zona Norte do Instituto Federal de Rondônia (IFRO), Porto Velho - Rondônia, Brasil. E-mail: ct.thaynara@gmail.com
[3]Mestre em Ensino Tecnológico pelo Instituto Federal de Educação, Ciência e Tecnologia do Amazonas (IFAM), Campus Porto Velho Zona Norte do Instituto Federal de Rondônia (IFRO), Porto Velho - Rondônia, Brasil. E-mail: silmar.oliveira@ifro.edu.br
[4]Mestre em Administração pela Universidade Federal de Rondônia (UNIR), Campus Porto Velho Zona Norte do Instituto Federal de Rondônia (IFRO), Porto Velho - Rondônia, Brasil. E-mail: douglas.piffer@ifro.edu.br

wireless, garantindo assim a proteção adequada da informação digital em um mundo cada vez mais conectado.

Palavras-chave: Segurança da Informação. Redes Wifi. Redes Públicas. Vulnerabilidades.

INFORMATION SECURITY: A LITERATURE REVIEW FOCUSING ON THE VULNERABILITIES OF PUBLIC WIRELESS NETWORKS

ABSTRACT

Information security is an essential field that involves analyzing and protecting against various types of risks associated with digital information. In this context, data security in wireless networks assumes a crucial role, since it is related to several conditions, from the choice of the equipment of a network to the device that the user is using when connecting to the internet. Objective: This study aims to deepen understanding about information security in public networks by identifying the specific vulnerabilities of wireless networks and the risks associated with data integrity in those networks. Methodology: The methodology adopted for this study was a systematic bibliographic research, which allowed the analysis of the challenges and successes documented in recent literature. This approach was essential to identify the critical points and established best practices in the field of data security in wireless networks. Results: The results of this research highlighted several significant vulnerabilities in wifi networks. Among the most important, issues related to the "digital document", "data storage", "internal network" and "organizational environment" were identified. These vulnerabilities pose significant threats to the integrity and security of data transmitted and stored on wireless networks, especially in public environments. Final Considerations: In the final considerations, the importance of implementing immediate measures aimed at improving the approach to information security in wireless networks is emphasized. These include updating and strengthening security protocols, continuing education of users about safe practices when using public networks, and adopting advanced data protection technologies. Only with a proactive and comprehensive approach will it be possible to mitigate the risks and ensure data integrity in wireless networks, thus ensuring adequate protection of digital information in an increasingly connected world.

Keywords: Information Security. Wifi networks. Public Networks. Vulnerabilities.

SEGURIDAD DE LA INFORMACIÓN: REVISIÓN BIBLIOGRÁFICA CENTRADA EN LAS VULNERABILIDADES DE LAS REDES INALÁMBRICAS PÚBLICAS

RESUMEN

La seguridad de la información es un campo esencial que implica el análisis y la protección contra diversos tipos de riesgos asociados con la información digital. En este contexto, la seguridad de los datos en las redes inalámbricas asume un papel crucial, ya que está relacionada con varias condiciones, desde la elección del equipo de una red hasta el dispositivo que el usuario está utilizando al conectarse a Internet. Objetivo: Este estudio pretende profundizar en la comprensión

de la seguridad de la información en las redes públicas identificando las vulnerabilidades específicas de las redes inalámbricas y los riesgos asociados a la integridad de los datos en dichas redes. Metodología: La metodología adoptada para este estudio fue una investigación bibliográfica sistemática, que permitió el análisis de los retos y éxitos documentados en la literatura reciente. Este enfoque fue esencial para identificar los puntos críticos y las mejores prácticas establecidas en el campo de la seguridad de los datos en las redes inalámbricas. Resultados: Los resultados de esta investigación pusieron de manifiesto varias vulnerabilidades significativas en las redes wifi. Entre las más importantes, se identificaron cuestiones relacionadas con el "documento digital", el "almacenamiento de datos", la "red interna" y el "entorno organizacional". Estas vulnerabilidades plantean amenazas significativas a la integridad y seguridad de los datos transmitidos y almacenados en redes inalámbricas, especialmente en entornos públicos. Consideraciones finales: En las consideraciones finales, se enfatiza la importancia de implementar medidas inmediatas dirigidas a mejorar el enfoque de la seguridad de la información en redes inalámbricas. Estos incluyen la actualización y el fortalecimiento de los protocolos de seguridad, la educación continua de los usuarios sobre prácticas seguras al utilizar redes públicas y la adopción de tecnologías avanzadas de protección de datos. Sólo con un enfoque proactivo y global será posible mitigar los riesgos y garantizar la integridad de los datos en las redes inalámbricas, garantizando así una protección adecuada de la información digital en un mundo cada vez más conectado.

Palabras clave: Seguridad de la información. Redes Wifi. Redes públicas. Vulnerabilidades.

1 INTRODUÇÃO

A segurança da informação é um campo essencial que envolve a análise e proteção contra diversos tipos de riscos associados à informação digital. Fundamentada nos conceitos de sistemas de informação, a segurança da informação visa proteger dados contra uma ampla gama de ameaças, como destacado por Hintzbergen (2018). Os sistemas de informação representam a interação complexa entre pessoas, processos, dados e tecnologia, formando a espinha dorsal das operações contemporâneas em organizações de todos os tipos. À medida que grandes inovações tecnológicas emergem, a sociedade adentra uma era digital onde o acesso à informação e notícias se torna mais fácil e rápido graças à internet. No entanto, essa conectividade crescente traz consigo um aumento exponencial nas ameaças cibernéticas. Dados do Gabinete de Segurança Institucional da Presidência da República indicam que, em 2019, ocorreram mais de 10 mil ataques cibernéticos no Brasil, colocando em risco a segurança dos dados pessoais dos cidadãos (ITO, 2022).

Neste contexto, a segurança de dados em redes wireless se destaca como um aspecto crítico. Esse campo abrange desde a seleção de equipamentos de rede até os dispositivos que os usuários

utilizam para se conectar à internet. As redes sem fio são particularmente vulneráveis a uma série de ameaças potenciais, incluindo hackers e malware sofisticado. A falta de medidas de segurança robustas pode resultar na exposição de dados sensíveis, violação de privacidade e interrupções nos serviços. Portanto, é imperativo produzir e disseminar artigos que abordem a segurança de dados em redes wireless. Esses estudos devem focar na prevenção de violações, na proteção da integridade dos dados e na conscientização dos usuários sobre os riscos e as melhores práticas de segurança cibernética. A conscientização desempenha um papel fundamental na mitigação de riscos, pois capacita os indivíduos a adotarem práticas seguras ao utilizar tecnologias digitais.

Este estudo tem como objetivo aprofundar a compreensão sobre a segurança da informação em redes públicas, identificando as vulnerabilidades específicas das redes wireless e os riscos associados à integridade dos dados nessas redes. Para atingir esse objetivo, foi realizada uma pesquisa bibliográfica sistemática, analisando os desafios e êxitos documentados na literatura recente. A análise detalhada dos achados proporciona uma visão abrangente das melhores práticas e estratégias para reforçar a segurança em redes wireless. Esse estudo contribuirá para o desenvolvimento de um ambiente digital mais seguro e resiliente, oferecendo recomendações práticas para a implementação de medidas de segurança eficazes. Além disso, destacará a importância da criação de políticas de segurança da informação e a necessidade de uma abordagem proativa para enfrentar as ameaças cibernéticas emergentes. Com uma compreensão aprofundada e a aplicação das melhores práticas de segurança, será possível minimizar os riscos e garantir a proteção dos dados em um mundo cada vez mais conectado.

2 REFERENCIAL TEÓRICO

A segurança da informação está relacionada com a proteção de informações que apresentam um valor para pessoas ou instituições, de acordo com De Souza Júnior e seus colaboradores (2019), ela obtém aspectos que envolvem integridade, disponibilidade e confidencialidade: a integridade está relacionada à informação que se mantém íntegra, sem modificações; a disponibilidade visa que os dados estejam disponíveis para quem possua acesso; e a confidencialidade, certifica garantir de quem realmente deve acessar a informação.

Segundo Santos e Gulo (2018), a segurança da informação visa a proteção de vários tipos

de ameaças para garantir a continuidade do negócio, retorno de investimentos, oportunidades, entre outros fatores. Buscando zelar pela integridade e resguardo das informações, protegendo - as contra acessos não autorizados.

Conforme Hintzbergen (2018), para aplicar a segurança da informação é necessário realizar uma análise de risco, pois a segurança é alcançada através de um conjunto, que envolve políticas, processos, estruturas organizacionais, funções de software e hardware. Desse modo, para o desenvolvimento dessa análise é necessário haver um gerenciamento de risco, visto que é um gerenciamento de minimizar as vulnerabilidades de uma organização.

Segundo Machado (2014), a importância da segurança da informação se baseia na identificação dos dados e gerenciá lo de acordo com as diretrizes e normas existentes de uma organização, obtendo manter os seus aspectos, que envolvem, disponibilidade, confidencialidade e integridade do elemento.

2.1 HISTÓRIA DA SEGURANÇA DE DADOS

Segundo Gugik (2009), os primeiros computadores foram desenvolvidos com uma arquitetura muito grande e eram utilizados por organizações e militares. As primeiras máquinas surgiram no período da segunda guerra mundial com o objetivo de desencriptação de mensagens e criação de novos objetos inteligentes.

De acordo com Macedo (2018), ao passar dos anos com os avanços tecnológicos, as máquinas começaram a ser desenvolvidas com equipamentos melhores, dessa forma diminuindo o tamanho do hardware, utilizando dispositivos de entrada e saída, entre outros fatores. De modo que surge a conectividade em rede, no qual começa aparecer a necessidade de proteger as informações transmitidas entre os computadores.

Conforme Moreira (2009), com o crescimento da internet e a dependência das pessoas, surgem os primeiros vírus de computador, logo, a precisão da criação de antivírus, desenvolvimento de padrões de segurança e criptografia, visto que as formas de ataques estão se tornando cada vez mais sofisticadas, desse modo, fazendo com que as instituições busquem melhorias para se proteger contra as ameaças.

Com o aumento da dependência tecnológica, devido às pessoas utilizarem a tecnologia para

a realização de tarefas diárias, operações comerciais, comunicação, entre outros, as organizações começaram a investir na segurança cibernética, visto que os ataques de crackers, roubos de dados estão cada vez mais presentes. Desta forma, as instituições começaram a utilizar métodos de proteção, como, firewalls, sistema de detecção, políticas de seguranças, entre outros métodos (Assunção, 2002).

2.2 LEGISLAÇÃO E REGULAMENTAÇÃO DA SEGURANÇA DE DADOS NO BRASIL

A lei nº 13.709/2018, aborda sobre a proteção de dados pessoais (LGPD), foi criada com objetivo de proteger a privacidade de cada indivíduo, além de ter um foco na proteção jurídica (Brasil, 2018). Conforme Frazão (2019) a lei é aplicada em várias situações em que há tratamento de dados pessoais, inclusive no setor público, dessa maneira, não restringindo há hipótese em que se configura em apenas relação de consumo.

De acordo com Pinheiro (2020), é uma legislação que visa a proteção do titular dos dados, inviabilidade íntima, a liberdade de expressão, entre outros fatores, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade. Contudo, apesar de ter uma lei criada pelo governo em pró de amparar os cidadãos, os mesmos ainda sofrem com essa violação de dados.

Segundo Alves e Neves (2021), a Lei Geral de Proteção de Dados entrou em vigor no ano de 2020, deste modo empresas de diferentes setores e órgãos públicos, buscam se adequar de acordo com a legislação vigente, visto que as infrações à essa lei podem decorrer a advertências, até a imposição de sanções que podem chegar a 2% de um faturamento de uma empresa, limitada a R$50 milhões por infração. Portanto, é necessário que as organizações se adequem aos requisitos da LGPD buscando garantir a proteção e segurança de dados pessoais.

2.3 SEGURANÇA DE DADOS EM REDES WIRELESS

De acordo com Bof (2012) uma rede de computadores consiste na conectividade de dois ou mais computadores com diversos dispositivos, outrossim, uma rede wireless se refere a uma conexão sem a necessidade do uso de cabos.

Conforme Sereno (2015), uma rede no qual pode trazer vantagens no momento de

instalação, visto que não há necessidade de passar cabos, há uma flexibilidade, no qual permite o uso em ambiente interno e externo de modo que os usuários possuem acesso em qualquer local, além da facilidade do uso, escalabilidade e baixo custo.

Segundo Regonha (2010), em contrapartida, é uma rede muito vulnerável a acessos não autorizados, visto que um invasor pode acessar a rede nem mesmo estando fisicamente no local dos dispositivos, além de poder interceptar o tráfego de dados dependendo do sistema de segurança que a rede possui, ademais, existem os sniffer, que se refere quando os dados são transmitidos em uma rede e podem ser capturados, entre outras situações, que podem ocorrer dependendo da forma de configuração da rede sem fio.

De acordo com Santos e Gulo (2018), a configuração da rede wireless é primordial para manter a segurança dos dados, e um dos principais princípios dessa configuração está relacionado com a criptografia, visto que ela é utilizada tanto por usuários como por empresas, tem a função de codificar a informação, a mesma utilizada de forma incorreta apresentará falhas dos quais podem colocar os dados em riscos.

2.4 VULNERABILIDADES DA SEGURANÇA DE DADOS PARA USUÁRIOS DE REDES WIRELESS PÚBLICAS

É perceptível a existência da vulnerabilidade de dados existente em uma rede sem fio, segundo Recco (2020) uma forma de vulnerabilidade que pode ocorrer está relacionada às falhas e brechas encontradas em protocolos. Além disso, é necessário ter um certo cuidado em relação a segurança física, por mais que seja uma rede sem fio, a área de abrangência de um sinal, dependendo do equipamento utilizado, deve ser monitorada, visto que dependendo da propagação do sinal, um ataque pode ser realizado de uma distância não esperada.

Conforme Rufino (2019), uma rede wireless, basta o usuário receber um sinal que o mesmo pode estar sujeito a uma captura passiva, visto que existem cibercriminosos, que utilizam ferramentas para coletar dados que trafegam na rede, ou até mesmo chegam a enviar link para os usuários, contendo programas que coletam informações das pessoas.

Além de tudo, a vulnerabilidade também pode ser causada devido ao dispositivo do usuário, caso o usuário tenha um dispositivo que contenha configurações incorretas, aplicativos

desatualizados, falhas no sistema operacional, entre outras condições, o dispositivo pode estar exposto, desprotegido, a acessos não autorizados (Nakamura; De Geus, 2007).

Conforme Magacho e Trento (2021), a necessidade de compreender sobre a segurança dos dados na internet é de suma importância, visto que o usuário tem que conhecer se a proteção que um site oferece é suficiente para não ter sua privacidade violada por terceiros.

3 METODOLOGIA

Considerando a classificação metodológica de Creswell e Clark (2015), o presente estudo classifica-se como: qualitativa, quanto à natureza da abordagem metodológica, pois busca obter dados que contribuam para a segurança da informação em rede wifi pública e medidas que aprimorem a segurança; transversal, quanto à temporalidade, pois observa os achados relativos à temática e objetivos de estudo nas publicações científicas nos últimos 13 anos; descritivo, quanto aos objetivos de pesquisa, posto que propõe a descrição destes achados a partir da análise das vulnerabilidades existentes que podem colocar em risco os dados dos usuários; e quanto ao método, como pesquisa bibliográfica sistemática, pois adota estratégia sistematizada de coleta, avaliação, sintetização, análise e discussão dos achados junto aos artigos científicos, com o propósito de criar um embasamento teórico-científico (estado da arte) sobre a temática segurança da informação.

A estratégia para coleta de dados consistiu da operacionalização do motor de buscas por publicações do Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), através dos descritores e operadores booleanos: “segurança da informação” AND “redes públicas” AND “dados”.

Tabela 1: Instrumento de coleta e tabulação de resultados por base de dados

Base de Dados utilizada para Coleta: Busca realizada na base de dados da plataforma Capes no período dos últimos 13 anos.	
Publicações Obtidas na Língua Portuguesa	Nº de Publicações: **24**
Publicações Obtidas na Língua Inglesa	Nº de Publicações: **28**
Publicações Obtidas na Língua Espanhola	Nº de Publicações: **03**
Publicações realizadas entre os períodos de 2010 a 2023	Nº de Publicações: **39**
Publicações restringidas apenas a artigos científicos	Nº de Publicações: **39**
Publicações restringidas a apenas artigos científicos revisados por pares	Nº de Publicações: **39**
Publicações cujo título relaciona-se com os objetivos do estudo	Nº de Publicações: **04**
Restringidas publicações em duplicidade	Nº de Publicações: **04**

Publicações cujo resumo relaciona-se com os objetivos do estudo	Nº de Publicações: **04**
Publicações restringidas a apenas artigos originais excluindo revisões bibliográficas	Nº de Publicações: **04**

Tabulação dos Resultados

Título do Artigo	Ano	Considerações do Artigo	Autor(es)
Certificação Digital e Arquivologia: benefícios e aplicações	2015	Objetivo do artigo é analisar o mercado certificado digital na cidade de Manaus, sobre a ótica de arquivologia; Metodologia pesquisa exploratória-descritiva, realizada por meio de um estudo de caso; Resultado - uso do certificado digital os processos se tornaram mais ágeis, confiáveis, sigilosos e seguros, além de atribuir autenticidade.	Tatiane Rodrigues Nascimento Kátia Viana Cavalcante Felipe Vlaxio Id.: NASCIMENTO et al., 2015.
Segurança da Informação na rede educacional do IFF	2017	O objetivo é utilizar técnicas de mineração de dados sobre as informações do tráfego de redes do campus Instituto Federal Fluminense,tanto o tráfego interno,quanto a rede mundial de computadores, para extrair regras que apresentem as principais vulnerabilidades e tráfegos considerados maliciosos ainda não identificados pela equipe de tecnologia da informação do instituto. Metodologia para identificar ameaças em potencial no tráfego de rede do instituto, perceber as vulnerabilidades nos serviços hospedados internamente, foi instalado um sistema de detecção de intrusão (IDS) para logar todo o tráfego de rede de dentro do instituto para a internet e vice-e-versa, e também o tráfego de rede entre os câmpus. Resultados - necessita aplicar um horário de alerta, pois esse tipo de informação auxilia o administrador de rede a traçar o perfil das ameaças e proteger a rede bloqueando os tráfegos com tais características no firewall da instituição. Outro fator importante foi determinar os hosts com mais alertas, e em caso de o host ser uma máquina interna do IFF;	André de Azevedo Cunha Simara Netto Martins Georgia Regina Rodrigues Gomes Id.: DE AZEVEDO CUNHA et al., 2017.
Grau de maturidade da segurança da informação na visão dos gestores da rede pública de hospitais federais do Brasil	2021	Objetivo - é retratar sobre o conhecimento dos colaboradores das instituições de saúde sobre segurança da informação; Metodologia - qualitativa foi a escolhida para o desenvolvimento da pesquisa, pois investiga detalhadamente os fenômenos do ambiente estudado – o pesquisador vive e conhece a realidade desse grupo ou ambiente. A pesquisa terá caráter descritivo, para, dessa forma, apresentar as características dos hospitais federais do município do Rio de Janeiro Resultados - fundamental que as instituições de saúde pública tenham conhecimento sobre segurança da informação e sobre a legislação diz a respeito;	José Bredariol Junior Antônio Augusto Gonçalves Antônio Carlos Magalhães José Geraldo Pereira Barbosa Guilherme Neves Lopes Frederico Sauer Guimarães Oliveira Id.: BREDARIOL et al., 2021.

Controle Social e Necessidade de Proteção de dados pessoais	2013	Objetivo: compreender controle social e os desdobramentos do poder na denominada Sociedade da Informação, tanto na esfera pública quanto na esfera privada Metodologia - analisar marcos teóricos em relação evolução das sociedades, internet e segurança da informação; Conclusão - nos dias atuais existem princípios em relação a proteção de dados, esses princípios, mesmo que fracionados, condensados ou adaptados, podem ser identificados em diversas leis, tratados e convenções.	José Renato Gaziero Cella Luana Aparecida dos Santos Rosa Id.: CELLA et al., 2013

Fonte: Adaptado de PIFFER et al., 2023.

3.1 ESTRATÉGIA PARA ANÁLISE DOS DADOS

Para analisar os dados obtidos, levando em consideração fatores como recursos disponíveis, necessidades da população, capacidade de monitoramento e controle, e oferta de serviços de saúde à população nas publicações coletadas, adotou-se a estratégia de análise das publicações por saturação de dados, como define Fontanella et. al (2008), é uma ferramenta conceitual frequentemente empregada nos relatórios de investigações qualitativas em diferentes áreas no campo da saúde, entre outras. Assim, a avaliação da saturação teórica a partir de uma amostra é feita por um processo contínuo de análise dos dados, ao passo em que a definição de variáveis de agrupamento ocorrem contiguamente à tabulação dos dados a partir da análise do conteúdo.

Operacionalmente, realiza-se a tabulação utilizando-se uma ficha com as seguintes informações: identificação ordinária (Id), variável emergente, conteúdo manifesto na publicação, identificação da publicação, agrupando através da mesclagem das linhas da variável emergente todas as publicações que a compartilham. Assim, a análise encerrou-se quando todas pelo menos cinco publicações, ordenadas ao acaso, deixaram de manifestar novos conteúdos relevantes para a análise, pois como observa Fontanella et. al (2008), neste momento faz-se improvável que novas ideias apareçam, mesmo que chegássemos ao dobro de amostras analisadas.

Tabela 2: Instrumento de Saturação Teórica de Dados

Seq.	Variável Emergente	Conteúdo Manifesto	Id. dos artigos
V1	Vulnerabilidade de documento digital	*"O documento digital tem suas especificidades e complexidades. Tem, pois, a necessidade de manutenção da autenticidade em toda a cadeia de custódia, acesso em longo prazo e consequente preservação. O documento apresenta especificidades que podem comprometer sua autenticidade, devido à rápida obsolescência das tecnologias e de intervenções não autorizadas que podem ocasionar adulteração e destruição.*"	NASCIMENTO et al., 2015.
V2	Vulnerabilidade armazenamento de dados	*"Diante disso, a preocupação que se tem é com o Marco Civil regulatório da internet no Brasil, sobretudo no que tange ao armazenamento de dados que se pretende que os provedores da internet façam relativamente a seus clientes."*	CELLA et al., 2013
V3	Vulnerabilidade em rede interna	*"Para que seja possível identificar ameaças em potencial no tráfego de rede do instituto, bem como perceber as vulnerabilidades nos serviços hospedados internamente, foi instalado um sistema de detecção de intrusão (IDS) para logar todo o tráfego de rede de dentro do instituto para a internet e vice-e-versa, e também o tráfego de rede entre os câmpus."*	CUNHA et al., 2017.
V4	Vulnerabilidade organizacional	*"Neste ambiente, as ameaças a segurança da informação podem ser categorizadas em duas grandes áreas: Organizacional onde as ameaças surgem do acesso inadequado de dados de pacientes por agentes internos que abusam de seus privilégios ou agentes externos que exploram a vulnerabilidade dos sistemas de informação, e ameaças sistêmicas que surgem de uma cadeia de fluxo de informações explorando os dados divulgados além do uso pretendido"*	BREDARIOL et al., 2021.

Fonte: Adaptado de PIFFER, et al., 2023.

4 ANÁLISE E DISCUSSÕES DOS DADOS

No artigo de Nascimento e sua equipe (2015) às vulnerabilidades da rede Wifi são discutidas sob a perspectiva da segurança de documentos digitais. Os autores afirmam que há especificidades e complexidades, especialmente relacionadas às a necessidade de manutenção da autenticidade em toda a cadeia de custódia, acesso em longo prazo e consequente preservação dos documentos digitais. Comprometendo sua autenticidade, devido à rápida obsolescência das tecnologias e de intervenções não autorizadas que podem ocasionar adulteração e destruição. Contribuindo com essa afirmativa, Santos e Flores (2017), informa que os documentos digitais são informações registradas e codificadas em dígitos binários, os quais são acessíveis por meio de um computador, em razão das vulnerabilidades existentes muitas pessoas buscam estratégias de

preservação digital e sistemas seguros para a preservação de acesso.

Sob a óptica da legalidade, Cella e seus colaboradores (2013) concentram seu estudo na preocupação nas vulnerabilidades do armazenamento de dados, citando o Marco Civil regulatório da internet no Brasil, no que tange ao armazenamento de dados que se pretende que os provedores da internet façam relativamente a seus clientes. Colaborando com essa assertiva, Siqueira (2021), descreve que a era da internet modificou a forma de vida das pessoas, diante da falta de informação, os cidadãos estão vulneráveis a sofrer possíveis golpes, devido a facilidade de expor os seus dados, desta forma, diversos mecanismo de proteção foram criados, visto que a exacerbação da vulnerabilidade tornou - se notório, um dos exemplos de mecanismo é a criação da Lei Geral de Proteção de Dados que visa proteger os direitos fundamentais de liberdade e privacidade dos indivíduos.

Na pesquisa de Cunha e seus auxiliares (2017) a vulnerabilidade em rede interna pode ser evitada ao instalar um sistema de detecção de intrusos. Os escritores consentem que esse modelo de sistema auxilia em identificar ameaças no tráfego de uma rede e em serviços hospedados internamente. Cooperando com esse assunto, Sato (2012), comenta que existem vários modos de ataques no tráfego de uma rede, como por exemplo, ao instalar aplicativos suspeitos no equipamento de informática, ataques remotos de usuários não autorizados, recebimentos de links atípicos, entre outros. O autor ressalta que um incidente de segurança pode impactar diretamente e negativamente uma corporação, devido à exposição de dados e a ausência de segurança.

De acordo com a perspectiva de Bredariol e seus assistentes (2021) a vulnerabilidade organizacional é vista como um ameaça à segurança da informação. Os autores pronunciam que a segurança pode ser ameaçada por duas áreas, a organizacional no qual surge do acesso inadequado de dados e por abuso de privilégio e às ameaças sistemáticas, relacionada a exploração de dados divulgados além do uso pretendido. Contribuindo com o tema Dos Santos (2015) analisa que para a preservação da informação no ambiente organizacional é necessário constituir políticas que definam estratégias de preservação de dados, para assim aumentar o nível de segurança dos documentos. Além de destacar que uma corporação pode utilizar ferramentas para verificar a integridade da informação e seus componentes, além de realizar trilhas de auditoria, com isso é possível minimizar a fragilidade.

5 CONSIDERAÇÕES FINAIS

A presente pesquisa, que teve como foco “compreender a segurança da informação em rede pública, além de conceber os tipos de vulnerabilidades existentes em uma rede wireless e como elas podem colocar em risco os dados de uma rede”, oferece importantes contribuições tanto para o avanço científico quanto para o aprimoramento das políticas de segurança sobre preservação de dados.

Os resultados desta pesquisa apresentam importantes contribuições tanto para a sociedade quanto para o desenvolvimento científico, destacando vulnerabilidades críticas das redes Wi-Fi, como documentos digitais, armazenamento de dados, redes internas e ambiente organizacional. Para a sociedade, esses resultados ressaltam a importância de adotar práticas de segurança mais rigorosas para proteger informações sensíveis e garantir a integridade dos dados. A conscientização sobre as ameaças tecnológicas e a necessidade de manutenção contínua dos sistemas de segurança pode levar a uma maior confiança nas operações digitais. A segurança dos documentos digitais, por exemplo, é fundamental para preservar a integridade das informações pessoais e corporativas, prevenindo destruição e adulteração. Este conhecimento pode ajudar indivíduos e organizações a serem mais proativos na proteção de seus dados.

A segurança no armazenamento de dados também é destacada como uma área crítica. Com a adoção de soluções robustas de criptografia e controle de acesso, os usuários podem ter mais confiança de que suas informações estão protegidas contra acessos não autorizados e violações de privacidade. Este aspecto é especialmente relevante à medida que mais dados são armazenados em servidores de provedores de internet. No ambiente organizacional, a pesquisa enfatiza a importância de softwares de detecção de intrusos e políticas de segurança bem definidas. A implementação dessas medidas pode ajudar a prevenir ataques e acessos maliciosos, garantindo que os serviços internos permaneçam seguros. Além disso, a formação contínua dos funcionários e a existência de mecanismos de auditoria são essenciais para manter uma postura de segurança robusta e resiliente.

Para as ciências da informação, especialmente da gestão de redes, a pesquisa amplia o entendimento sobre as vulnerabilidades específicas das redes wireless e as medidas necessárias para mitigá-las. Este conhecimento pode servir como base para futuros estudos, fomentando o

desenvolvimento de tecnologias e estratégias inovadoras para a proteção de dados. A identificação das lacunas na literatura existente também sublinha a necessidade de pesquisas adicionais, incentivando a investigação contínua e o aprimoramento das práticas de segurança da informação. Em suma, os achados desta pesquisa fornecem subsídios valiosos para o desenvolvimento de políticas e práticas de segurança mais eficazes, beneficiando tanto a sociedade quanto a comunidade científica. Ao abordar as vulnerabilidades das redes Wi-Fi de forma abrangente, a pesquisa contribui para a proteção de dados e o avanço contínuo na área da segurança da informação.

Por fim, este estudo destaca a importância de implementar medidas imediatas para aprimorar a segurança da informação em redes wireless, visando garantir que os dados dos usuários sejam protegidos e proporcionando maior confiança no uso dessas redes. No entanto, é crucial reconhecer as limitações intrínsecas deste trabalho, especialmente a escassez de literatura específica sobre o tema, o que pode ter restringido a abrangência das conclusões. Esta lacuna sublinha a necessidade urgente de conduzir pesquisas adicionais para aprofundar o entendimento das vulnerabilidades e desenvolver estratégias mais eficazes. Recomenda-se que futuros estudos explorem diferentes contextos e tecnologias emergentes, além de incluir abordagens empíricas que possam validar e expandir os achados presentes, contribuindo assim para um avanço contínuo e robusto na segurança das redes wireless.

REFERÊNCIAS

ALVES, Carina; NEVES, Moisés. Especificação de Requisitos de Privacidade em Conformidade com a LGPD: Resultados de um Estudo de Caso. In: **WER**. 2021. Disponível em: http://wer.inf.puc-rio.br/WERpapers/artigos/artigos_WER21/WER_2021_paper_31.pdf. Acesso em 06/09/2023.

ASSUNÇÃO, Marcos Flávio Araújo. **Guia do hacker brasileiro** . Marcos Flávio Araújo Assunção, 2002. Disponível em: https://www.academia.edu/27399524/O_Guia_do_Hacker_Brasileiro_por_Marcos_Fl%C3%A1vio_Ara%C3%BAjo_Assun%C3%A7%C3%A3o. Acesso em 06/09/2023.

BOF, Edson. **Segurança em redes wireless.** 2012. Disponível em: https://www.webartigos.com/artigos/seguranca-em-redes-wireless/70234. Acesso em 06/09/2023.

BRASIL. **Lei n. 13.709/2018, dispõe sobre a Lei Geral de Proteção de Dados Pessoais (LGPD)**.
DOU de 15.8.2018, e republicado parcialmente em 15.8.2018. Ed. Extra. Brasília/DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 06/09/2023.

CELLA, José Renato Gaziero; DOS SANTOS ROSA, Luana Aparecida. Controle social e necessidade de proteção de dados pessoais. **Revista de Direito Brasileira**, v. 6, n. 3, p. 216-231, 2013. Disponível em: http://indexlaw.org/index.php/rdb/article/view/2748. Acesso em 21/05/2024.

CRESWELL, John W.; CLARK, Vicki L. Plano. **Pesquisa de Métodos Mistos: Série Métodos de Pesquisa**. Penso Editora, 2015. Disponível em: https://books.google.com.br/books?id=HPyzCAAAQBAJ&printsec=frontcover&hl=pt-BR. Acesso em 09/09/2023.

DE AZEVEDO CUNHA, André; GOMES, Georgia Regina Rodrigues; MARTINS, Simara Netto. Segurança da informação na rede educacional do IFF. **Ciência da Informação**, v. 44, n. 3, 2015. Disponível em: http://revista.ibict.br/ciinf/article/view/1802. Acesso em 21/05/2024.

DE SOUSA JÚNIOR, Carlos Alberto; JÚNIOR, Eliseu Castelo Branco; LIMA, Alberto Sampaio. Gestão de Segurança da Informação e Utilização de Firewalls em Empresas da Indústria Têxtil. Revista Eletrônica **ACTA SAPIENTIA**, v. 6, n. 1, 2019. Disponível em: https://actasapientia.com.br/index.php/acsa/article/view/32. Acesso em 21/05/2024.

DO NASCIMENTO, Tatiane Rodrigues; CAVALCANTE, Kátia Viana; VLAXIO, Felipe. Certificação digital e Arquivologia: benefícios e aplicações. **RACIn**, João Pessoa, v. 3, n. 1, p. 19-31, jan.-jun. 2015. Disponível em: http://arquivologiauepb.com.br/racin/edicoes/v3_n1/racin_v3_n1_artigo02.pdf. Acesso em 21/05/2024.

DOS SANTOS, Henrique Machado et al. **As vulnerabilidades dos documentos digitais: Obsolescência tecnológica e ausência de políticas e práticas de preservação digital**. Biblios Journal of Librarianship and Information Science, n. 59, p. 45-54, 2015. Disponível em: https://www.researchgate.net/publication/281692626_As_Vulnerabilidades_Dos_Documentos_Digitais_Obsolescencia_Tecnologica_E_Ausencia_De_Politicas_E_Praticas_De_Preservacao_Digital. Acesso em: 22/09/2023.

DOS SANTOS, Henrique Machado; FLORES, Daniel. **Da preservação digital ao acesso à informação: uma breve revisão**. Páginas a&b: arquivos e bibliotecas, p. 16-30, 2017. Disponível em:https://ojs.letras.up.pt/index.php/paginasaeb/article/view/2836/2593. Acesso em: 17/01/2024.

FONTANELLA, Bruno José Barcellos; RICAS, Janete; TURATO, Egberto Ribeiro. Amostragem por saturação em pesquisas qualitativas em saúde: contribuições teóricas. **Cadernos de saúde pública**, v. 24, p. 17-27, 2008. Disponível em: https://www.scielo.br/j/csp/a/Zbfsr8DcW5YNWVkymVByhrN/. Acesso em 11/03/2023.

FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** Thomson Reuters Brasil, 2019. Disponível em: https://bdjur.stj.jus.br/jspui/bitstream/2011/138898/SUMARIO_lei_geral_protecao_tepedino_2020.pdf. Acesso em: 18/10/2023.

GUGIK, Gabriel. A história dos computadores e da computação. **TecMundo**, Curitiba/PR, 2009. Disponível em: https://informaticaeadministracao.wordpress.com/2014/04/18/os-computadores-e-sua- historia/. Acesso em: 20/10/2023

HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. Brasport, 2018. Disponível em: https://books.google.com.br/books/about/Fundamentos_de_Seguran%C3%A7a_da_Informa%C3%A7%C3%A3.html?hl=pt-BR&id=1CVFDwAAQBAJ&redir_esc=y. Acesso em: 22/10/2023.

INEP. Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira. **Sinopse Estatística da Educação Superior 2019**. Brasília: INEP, 2020. Disponível em: http://portal.inep.gov.br/basica- censo-escolar-sinopse-sinopse. Acesso em: 10/06/2023.

ITO, Daniel. **Governo sofreu quase cinco mil incidentes cibernéticos em 2021**.Disponível em:https://agenciabrasil.ebc.com.br/radioagencia-nacional/seguranca/audio/2022-01/governo-sofreu-quase-cinco-mil-incidentes-ciberneticos-em-2021. Acesso em: 12/09/2023.

JUNIOR, José Bredariol et al. Grau de maturidade da segurança da informação na visão dos gestores da rede pública de hospitais federais do Brasil. **Revista Ibérica de Sistemas e Tecnologias de Informação**, n. E41, p. 232-243, 2021. Disponível em: https://search.proquest.com/openview/ 8c5bbc92b4525a0f858cd3a323fe2e25/1?pq-

origsite=gscholar&cbl=1006393. Acesso em 21/05/2024.

MACEDO, Ricardo Tombesi et al. **Redes de computadores.** 2018. Disponível em: https://repositorio. ufsm.br/handle/1/18351?show=full. Acesso em: 21/11/2023.

MACHADO, Felipe Nery Rodrigues. **Segurança da informação: princípios e controle de ameaças**. Saraiva Educação SA, 2014. Disponível em: https://books.google.com.br/books/about/Seguran%C3% A7a_da_Informa%C3%A7%C3%A3o.html?id=AYqwDwAAQBAJ&redir_esc=y. Acesso em: 16/11/2023.

MAGACHO, Bruna Toledo Piza; TRENTO, Melissa. LGPD e compliance na Administração Pública: O Brasil está preparado para um cenário em transformação contínua dando segurança aos dados da população? É possível mensurar os impactos das adequações necessárias no setor público. **Revista Brasileira de Pesquisas Jurídicas**, v. 2, n. 2, p. 7-26, 2021. Disponível em: https://www.sumarios.org/artigo/lgpd-e-compliance-na-administra%C3%A7%C3%A3o-p%C3%BAblica-o-brasil-est%C3%A1-preparado-para-um-cen%C3%A1rio-em. Acesso em 21/05/2024.

MOREIRA, Marcelo DD et al. Internet do futuro: Um novo horizonte. **Minicursos do Simpósio Brasileiro de Redes de Computadores-SBRC**, v. 2009, p. 1-59, 2009. Disponível em: https://www. gta.ufrj.br/ftp/gta/TechReports/20090527minicurso-parteIIvfinal.pdf. Acesso em: 16/11/2023.

NAKAMURA, Emilio Tissato; DE GEUS, Paulo Lício. **Segurança de redes em ambientes cooperativos**. Novatec Editora, 2007. Disponível em: https://www.academia.edu/9475240/ Seguran%C3%A7a_de_Redes_em_Ambientes_Cooperativos. Acesso em: 16/11/2023.

PIFFER, D. M. et al. Violência obstétrica: reflexões no itinerário de formação médica. **Brazilian Journal of Health Review**, v. 6, n. 3, p. 11815-11843, 2023d. Disponível em: https://doi.org/10.34119/bjhrv6n3-270. Acesso em: 28 ago. 2023.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais: comentários à Lei n. 13.709/2018-LGPD**. Saraiva Educação SA, 2020. Disponível em: https://bibliotecadigital.tse.jus.br/xmlui/handle/ bdtse/5974. Acesso em: 22/10/2023.

RECCO, Claudineia Helena. **Segurança de Redes sem Fio 802.11: Análise das Vulnerabilidades sobre a óptica da Segurança da Informação**. 2020. Disponível em: https://www.revistaresi.com.br/ index.php/resi/article/view/10/9. Acesso em: 20/11/2023.

REGONHA, Bruno. **Segurança em redes Wireless**. 2010. Disponível em: https://ric.cps.sp.gov.br/ bitstream/123456789/1672/1/20102S_REGONHABruno_TCCPD1023.pdf. Acesso em: 12/09/2023.

RUFINO, Nelson Murilo de O. **Segurança em redes sem fio: aprenda a proteger suas informações em ambientes wi-fi e bluetooth**. Novatec Editora, 2019. Disponível em: https://s3.novatec.com.br/ capitulos/capitulo-9788575222430.pdf. Acesso em: 06/09/2023.
SANTOS, LAF d; GULO, C. A. Segurança da informação. **Recuperado em**, v. 15, 2018. Disponível em: https://www.academia.edu/download/34613700/Termos_Tecnicos_Fundamentais_-_2014-A.pdf #page=76. Acesso em 21/05/2024.

SATO DE OLIVEIRA, RICARDO. **Estudo de Vulnerabilidade do IPSec em Redes IPV6**. 2012. Disponível em: https://aberto.univem.edu.br/bitstream/handle/11077/889/ESTUDO%20DE%20VULNERABILIDADE%20DO%20IPSEC%20EM%20REDES%20IPV6.pdf?sequence=1&isAllowed=y. Acesso em: 16/02/2024

SERENO, José Humberto Laranjeira. **Tendências de implementação e segurança nas redes wireless organizacionais**. 2015. Tese de Doutorado. Instituto Politécnico de Setúbal. Escola Superior de Ciências Empresariais. Disponível em; https://comum.rcaap.pt/bitstream/10400.26/10450/1/Disserta%C3%A7%C3%A3o%20MSIO%20JSereno%20-130313008.pdf. Acesso: 10/02/2024.

SIQUEIRA, Oniye Nashara et al. **A (hiper) vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD.** Revista Eletrônica Pesquiseduca, v. 13, n. 29, p. 236-255, 2021. Disponível em: https://periodicos.unisantos.br/pesquiseduca/article/view/1029. Acesso em: 16/02/2024.