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

AGNAR RIVERO RIBEIRO COLARES
GEOVANA SILVA NASCIMENTO

REDES WIFI: UM ESTUDO PRÁTICO SOBRE OS ASPECTOS DA SEGURANÇA DA INFORMAÇÃO NO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RONDÔNIA – IFRO CAMPUS PORTO VELHO ZONA NORTE

PORTO VELHO
2024

AGNAR RIVERO RIBEIRO COLARES
GEOVANA SILVA NASCIMENTO

REDES WIFI: UM ESTUDO PRÁTICO SOBRE OS ASPECTOS DA SEGURANÇA DA INFORMAÇÃO NO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RONDÔNIA – IFRO CAMPUS PORTO VELHO ZONA NORTE

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. Esp. Tiago Lopes de Aguiar.
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).

Colares, Agnar Rivero Ribeiro.
REDES WIFI: um estudo prático sobre os aspectos da segurança da informação no Instituto Federal de Educação, Ciência e Tecnologia de Rondônia – IFRO Campus Porto Velho Zona Norte / Agnar Rivero Ribeiro Colares, Geovana Silva Nascimento, Porto Velho-RO, 2024.
16 f.

Orientador(a): Prof Tiago Lopes Aguiar.
Coorientador(a): Prof 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. Vulnerabilidades em redes wireless. I. Nascimento, Geovana Silva. II. Aguiar, Tiago Lopes (orient.). III. Piffer, Douglas Moro (coorient.). IV. Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO. V. Título.

Bibliotecário(a) Responsável: Gizele de Melo Viana, CRB-CRB11/914 (Campus Porto Velho Zona Norte)

REDES WIFI: um estudo prático sobre os aspectos da segurança da informação no Instituto Federal de Educação, Ciência e Tecnologia de Rondônia – IFRO *Campus* Porto Velho Zona Norte

Agnar Rivero Ribeiro Colares[1], Geovana Silva Nascimento[2], Tiago Lopes de Aguiar[3], Douglas Moro Piffer[4]

RESUMO: O ambiente de segurança da informação inclui a análise e proteção de diversos tipos de risco à informação digital. A segurança de dados em rede *wifi* está relacionada a diversas condições, desde a escolha dos equipamentos de uma rede, suas configurações adequadas, até os dispositivos que o usuário está utilizando ao se conectar. Este estudo tem por finalidade descrever a importância da segurança da informação no cotidiano das pessoas que utilizam a rede de acesso *wifi* e para isso conduziu-se uma pesquisa bibliográfica sistemática e descrição dos achados com foco nos desafios e êxitos relatados na literatura recente, em conjunto com a realização de pesquisa aplicada combinada com testes práticos na rede *wifi* do Instituto Federal de Educação, Ciência e Tecnologia – IFRO *Campus* Porto Velho Zona Norte.
Palavras-chave: Segurança da informação. Redes *wifi*. Vulnerabilidades em redes *wireless*.

WIFI NETWORKS: a practical study on the aspects of information security at the Federal Institute of Education, Science and Technology of Rondônia - IFRO Campus Porto Velho Zona Norte

ABSTRACT: *The information security environment includes the analysis and protection of various types of risk to digital information. Data security on a Wi-Fi network is related to various conditions, from the choice of equipment on a network, its appropriate configurations, to the devices the user is using when connecting. The purpose of this study is to describe the importance of information security in the daily lives of people who use the wifi access network. To this end, a systematic literature search was conducted and the findings described, focusing on the challenges and successes reported in recent literature, together with applied research combined with practical tests on the wifi network of the Federal Institute of Education, Science and Technology IFRO Campus Porto Velho Zona Norte.*
Keywords: *Information security. Wi-Fi networks. Vulnerabilities in wireless networks.*

[1] Discente do Curso Superior de Tecnologia em Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia, Campus Porto Velho Zona Norte. Lattes: http://lattes.cnpq.br/4338138322327555. E-mail: agnarrivero@hotmail.com.

[2] Discente do Curso Superior de Tecnologia em Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia, Campus Porto Velho Zona Norte. Lattes: http://lattes.cnpq.br/5434166816379933. E-mail: geovananascimento786@gmail.com.

[3] Docente do Curso Superior de Tecnologia em Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia, Campus Porto Velho Zona Norte. Especialista em Gestão e Governança de Tecnologia da Informação. Lattes: http://lattes.cnpq.br/8744775169659538. E-mail: tiago.aguiar@ifro.edu.br.

[4] Docente do Curso Superior de Tecnologia em Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia, Campus Porto Velho Zona Norte. Mestre em Administração (PPGMAD/UNIR). Lattes: http://lattes.cnpq.br/8754245231535185. E-mail: douglas.piffer@ifro.edu.br.

1. INTRODUÇÃO

O ambiente de segurança da informação inclui a análise e proteção de diversos tipos de risco à informação digital e, inicialmente, baseia-se nos conceitos de sistemas de informação. De acordo com Hintzbergen (2018), segurança da informação é a proteção de dados contra uma ampla gama de ameaças. Segundo o mesmo, sistema de informação é um termo que se refere à interação entre pessoas, processos, dados e tecnologia.

Com o passar dos anos grandes inovações tecnológicas foram surgindo causando uma influência na vida das pessoas, devido a esses avanços atualmente o mundo vive em uma era tecnológica. O acesso à informação e às notícias ficou mais fácil devido a acessibilidade à internet, porém esse desenvolvimento tecnológico não é totalmente seguro. De acordo com Gabinete de Segurança Institucional da Presidência da República no ano de 2019 foram registrados mais de 10 mil incidentes cibernéticos sofridos pelo governo, com isso colocando em risco os dados pessoais dos cidadãos (ITO, 2022).

Desse modo, a segurança de dados em rede *wifi* está relacionada a diversas condições, desde a escolha dos equipamentos de uma rede, ao dispositivo que o usuário utiliza para se conectar à internet. Sendo assim, é necessário que existam estudos no quais descrevam sobre a segurança de dados, que visem promover discussões sobre a segurança das informações, prevenção contra a violação de dados e principalmente para conscientizar os usuários sobre ataques e políticas de segurança.

Este estudo tem por finalidade descrever como a segurança da informação é importante no cotidiano das pessoas que utilizam a rede *wifi* do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia – IFRO, Campus Porto Velho Zona Norte. A pesquisa se justifica pelo fato de tal rede ter apresentado vulnerabilidades e características próprias relativas à segurança da informação, que serão tratadas neste artigo. Para isso, foi conduzida pesquisa bibliográfica sistemática e descrição dos possíveis achados a partir da análise dos desafios e êxitos para compreensão relatados na literatura recente, a fim de compreender a importância da segurança da informação em redes públicas, além de relembrar os tipos de vulnerabilidades existentes em uma rede *wireless* e como elas podem colocar em risco os dados trafegados.

2. REFERENCIAL TEÓRICO

De acordo com Nobre (2019), a segurança da informação está relacionada com a

proteção de informações, sendo que estas apresentam um valor para pessoas ou instituições, obtendo aspectos que envolvem integridade, disponibilidade e confidencialidade. Integridade está relacionada à informação que se mantém íntegra, sem modificações. A disponibilidade visa que os dados estejam disponíveis para quem possua acesso. Já a confidencialidade, procura garantir de quem realmente deve acessar a informação.

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 tal gerenciamento procura minimizar as vulnerabilidades de uma organização.

Segundo Machado (2014), a importância da segurança da informação se baseia na identificação dos dados, gerenciando-os de acordo com as diretrizes e normas existentes de uma organização, procurando manter os seus atributos: disponibilidade, confidencialidade e integridade.

2.1. História da Segurança de Dados

Segundo Gugik (2009), os primeiros computadores foram desenvolvidos com uma arquitetura muito grande e eram utilizados apenas por organizações e militares. As primeiras máquinas surgiram no período da Segunda Guerra Mundial, com o objetivo de decriptação de mensagens inimigas 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 melhores recursos, dessa forma reduzindo o tamanho do *hardware*, utilizando dispositivos de entrada e saída, entre outros fatores. De modo que surge a conectividade em rede, a partir da qual começam a surgir 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, houve a necessidade da criação de antivírus, desenvolvimento de padrões de segurança e criptografia, visto que as formas de ataques estavam se tornando cada vez mais sofisticadas, desse modo, fazendo com que as instituições buscassem melhorias para se proteger contra as tais 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 dentre outros, estão cada vez mais presentes. Desta forma, as instituições começaram a utilizar métodos de proteção, como, *firewalls*, sistema de detecção, políticas de segurança entre outros métodos (ASSUNÇÃO, 2002).

2.2. Redes *Wifi*

Wifi é abreviação da palavra Wireless Fidelity é o termo utilizado para uma rede sem fio, geralmente de alta velocidade a curtas distâncias. Uma conexão *wifi* funciona por meio de ondas de rádio, sinais transmitidos por meio de um adaptador, "roteador", que decodifica e transmite os sinais por meio de antenas. Desse modo, para obter acesso a esses sinais os dispositivos, como celular, *notebook, smart* TV entre outros, devem estar dentro de um determinado raio de alcance (BARROS, 2021).

Conforme Simões (2015), a tecnologia *wifi* é mais habitual entre os usuários por não precisar de investimentos em estruturas físicas, além de estar disponível em dispositivos de últimas gerações da comunicação móvel. Além disso, é uma rede que está disponível na maioria dos espaços frequentados pelas pessoas no dia a dia, seja em casa, no trabalho, shopping entre outros ambientes.

Segundo Nunes (2006), as empresas e organizações implantaram rapidamente em suas estruturas o padrão 802.11 do *Institute of Electrical and Electronic Engineers* (IEEE). Uma vez que este padrão sugere a possibilidade de trocar uma rede cabeada para uma rede *wifi*, considerando que a mudança gera um custo financeiro menor em relação aos equipamentos, além da impossibilidade da instalação de redes com fio em certos lugares, desta forma obtendo a facilidade de mobilidade.

De acordo com Ramos (2020), devido aos avanços tecnológicos as redes *wifi* começaram a apresentar algumas vulnerabilidades. Devido ser uma rede que trafega vários tipos de informações do cotidiano das pessoas, os riscos de ataques são bem maiores, fazendo com que o usuário tenha mais atenção ao utilizar tais redes e que estas sejam devidamente configuradas.

2.3. Vulnerabilidades em Redes *Wifi*

Em virtude da rede *wifi* ser uma das tecnologias mais usadas pelos usuários para se conectar à internet, devido a sua praticidade, a mesma depende de vários fatores para não se tornar vulnerável a ataques. Uma das principais vulnerabilidades nas redes *wifi* é a ausência de conhecimento do administrador e usuário na implementação e uso dos recursos disponível para

segurança (FIGUEIREDO, 2020).

Além disso, uma vulnerabilidade bastante comum é em relação a segurança física, os locais onde os componentes da rede estão instalados, visto que é importante analisar a área de abrangência do sinal e a potência dos equipamentos, pois isso pode colocar em risco o bom funcionamento da rede e facilitar o acesso não autorizado e outros tipos de ataques (RUFINO, 2019).

Conforme Duarte (2003), as redes *wifi* podem apresentar vulnerabilidades interna e externa. A vulnerabilidade interna está relacionada às configurações, associação acidental, gerenciamento entre outras causas. A vulnerabilidade externa está associada a ataques à rede, captura de informações pelo tráfego de dados, sequestro de senhas, possíveis danos às configurações de rede entre outros fatores.

2.4. Legislação e Regulamentação da Segurança de Dados no Brasil

Importante também destacar que o IFRO, por ser uma entidade pública vinculada ao Poder Executivo Federal, deve se atentar a algumas legislações que tratam da segurança da informação. No Brasil o Decreto Federal nº 9.637, de 26 de dezembro de 2018, institui a Política Nacional de Segurança da Informação (PNSI), e tem por objetivo assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação no âmbito da administração pública federal. Além disso a segurança da informação abrange a defesa cibernética, a segurança física e a proteção de dados organizacionais. Ademais, a PNSI tem como princípios a proteção de dados pessoais, proteção da privacidade, orientação a gestão de risco e à gestão da segurança da informação, entre outros.

Destaca-se também a Lei Federal nº 13.709, de 14 de agosto de 2018, que trata da proteção de dados pessoais (Lei Geral de Proteção de Dados Pessoais – LGPD), que tem por objetivo 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 se restringindo há hipótese de relação de consumo. Além de tudo, por ser um país em que as pessoas utilizam a internet habitualmente, principalmente em rede *wifi*, o art. 6º desta lei determina alguns princípios para persevera a boa-fé, alguns deles estão relacionados a finalidade, livre acesso, transparência, segurança, qualidade dos dados entre outras concepções.

Além disto segundo o Decreto nº 11.856/2023, o governo brasileiro consta com uma Política Nacional de Cibersegurança (PNCiber), que visa orientar a atividade de segurança e

contribuir para os combates aos crimes cibernéticos e às demais ações maliciosas. Esta política ela tem como preceitos a garantia dos direitos fundamentais, a resiliência das organizações públicas e privadas a incidentes a taques cibernético, a educação, desenvolvimento tecnológico, entre outros princípios.

2.5. Segurança de Dados em Redes *Wireless*

De acordo com Boff (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.

De acordo com Santos e Gulo (2018), a configuração da rede *wireless* é primordial para manter a segurança dos dados, e um dos 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 e mitigar falhas que podem colocar os dados em riscos.

É perceptível a existência da vulnerabilidade de dados existente em uma rede sem fio, segundo Recco e Fernandes (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 à segurança física, por mais que seja uma rede sem fio, a área de abrangência de um sinal, dependendo do equipamento utilizado, e deve ser monitorada, visto que, dependendo da propagação do sinal, um ataque pode ser realizado de uma distância não esperada.

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 podem ocorrer (NAKAMURA; DE GEUS, 2007).

3. METODOLOGIA

Considerando a classificação metodológica de Creswell e Clark (2015), a metodologia do presente estudo classifica-se como: qualitativa, quanto à sua natureza da abordagem, pois busca obter dados das experiência coletivas e individuais sobre a segurança da informação em redes *wifi* e medidas que aprimorem a segurança; descritiva, quanto aos objetivos de pesquisa, pois propõe a descrição destes achados a partir da análise de vulnerabilidades que possam colocar em risco a redes *wifi*; e aplicada, realizada em campo, utilizando-se de procedimentos

práticos, considerando os testes realizados na rede *wifi* do Instituto Federal de Educação, Ciência e Tecnologia – IFRO *Campus* Porto Velho Zona Norte, bem como entrevista realizada com o responsável técnico pela configuração da rede *wifi*.

Os testes na rede *wifi* do IFRO foram realizados com o uso do aplicativo Fing - *Scanner* de Rede, executado na plataforma Android para celular, que, segundo Defavori (2015), possibiliza ferramentas para verificação do ambiente, permitindo a detecção de falhas e vulnerabilidades.

Além disso, foi realizada uma verificação através do teste de intrusão, utilizando a ferramenta Termux. De acordo com Serafim (2020), o teste de intrusão em uma rede permite analisar o nível de segurança, vulnerabilidades, através do mesmo que é possível verificar falhas em *hardware* e *software* utilizados.

Na entrevista pessoal, com o Coordenador de Gestão de Tecnologia da Informação, Gabriel Penha Bidá, foram apresentados os questionamentos que se encontram no Apêndice Único.

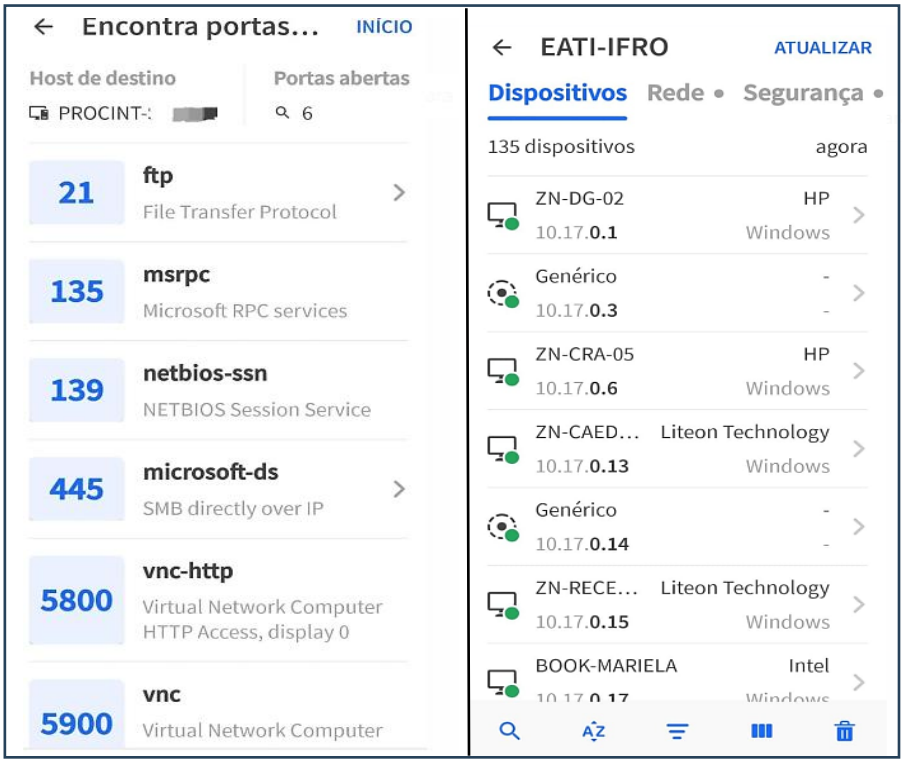
4. ANÁLISE E DISCUSSÕES DOS DADOS

Por meio da entrevista realizada com o Coordenador de Gestão de Tecnologia da Informação, foi possível identificar que o *Campus* Porto Velho Zona Norte conta com 16 (dezesseis) pontos de acesso (APs), conectando diariamente cerca de 250 (duzentos e cinquenta) alunos. Os acessos não são controlados por meio de credenciais (*login* e senha) individuais, mas sim por uma de uso universal, comum entre os alunos. Visto isso, uma forma de solucionar essa situação seria usar diferentes senhas de Wifi para diferentes grupos de usuários, implementar autenticação de usuário individual, e monitorar e gerenciar o uso da rede de forma mais regular.

Quanto aos mecanismos de controle de segurança o Coordenador de Gestão de Tecnologia da Informação informou sobre a existência de *firewall* utilizado na rede, para controlar URL, IDS e segmentações. O mesmo ressaltou que ações básicas de segurança aplicadas na rede de computadores são importantes pois evitam que ativos da informação fiquem expostos a ações maliciosas, deste modo, garantindo os pilares da segurança da informação, como a confidencialidade, integridade e disponibilidade no âmbito da Instituição.

Com o uso do Fing, foi possível exibir os *hosts* (dispositivos) que conectados à rede, além de demonstrar a velocidade geral do *wifi* e como o roteador está configurado, incluindo quais portas estão abertas no momento, conforme se verifica na Figura 1.

Figura 1 – Telas do Fing exibindo portas abertas e dispositivos localizados.



Fonte: Fing (2024).

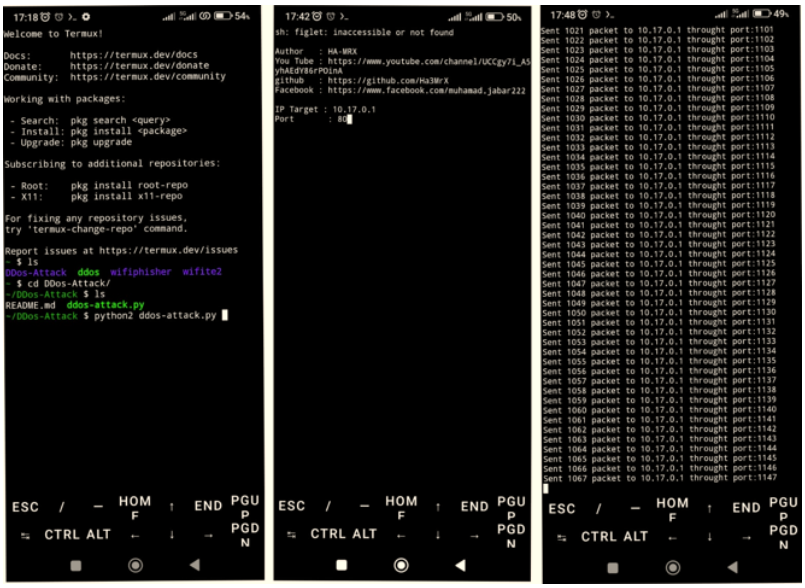
Ao realizar a análise na Rede *wifi* do *Campus* Zona Norte, foi possível identificar vários *hosts* e suas respectivas portas abertas, dentre elas destaca-se a porta 80, pertencente a um *host* em específico, permitindo acesso remoto via *web*. A referida porta pertencia a um servidor de rede modelo Power Edge R540, que permitia a conexão direta em sua porta Idrac. O Idrac é uma ferramenta adicional que permite acessar remotamente, via navegador/console, todos os recursos do servidor. Para nossa surpresa, ao realizar os testes básicos de conexão por meio das credenciais de acesso padrão (de fábrica), foi possível conectar ao servidor com perfil de administrador.

Caso alguém não autorizado acesse o Idrac de forma indevida, várias consequências negativas podem ocorrer, como, comprometimento da segurança como a exposição de informações confidenciais sobre o servidor e a rede, incluindo configurações de sistema, registros de eventos e informações de diagnóstico. Além disso, pode ocorrer a manipulação de informações de forma maliciosa, um invasor pode realizar ações no servidor por meio do Idrac, como alterar configurações críticas do sistema, desligar o servidor ou até mesmo instalar *malwares* para comprometer a integridade e a disponibilidade dos dados, além disto, pode explorar a vulnerabilidade de segurança no servidor e na rede, entre outros fatores.

Além disso, ao realizar o teste de segurança através do aplicativo Termux, com o

objetivo de desautenticação na rede, um dos roteadores recebeu uma inundação de conexões, causando sua indisponibilidade e inatividade dos dispositivos conectados na rede Wifi por meio deste.

Figura 2 – Telas do Termux fazendo o ataque DDos no IP e porta específica.



Fonte: Termux (2024).

Constatamos ainda, conforme entrevista realizada, que a senha para acesso à rede Wifi era a mesma para todos na instituição (alunos, servidores e visitantes), dessa forma, alguns prejuízos foram diagnosticados, como o comprometimento da segurança da informação da rede, já que qualquer pessoa, em posse da senha, poderia acessar a rede. Dificultando a identificação de usuários que poderiam estar envolvidos em atividades maliciosas na rede.

Após a realização dos testes, ambas as vulnerabilidades encontradas foram imediatamente reportadas, por *e-mail*, aos colaboradores da área de informática do IFRO *Campus* Porto Velho Zona Norte, sendo que as mesmas foram devidamente tratadas.

A segurança da informação do Instituto Federal de Educação, Ciência e Tecnologia – IFRO *Campus* Porto Velho Zona Norte, é de suma importância visto que é um ambiente no qual cada vez mais a tecnologia se encontra presente. Neste sentindo, a pesquisa realizada foi influenciada diretamente por buscar compreender aspectos específicos sobre a segurança da rede, visando identificar possíveis vulnerabilidades. Desta forma, contribuindo para o aprimoramento da infraestrutura e da segurança da informação.

5. CONSIDERAÇÕES FINAIS

A presente pesquisa, que teve como foco a segurança da informação e sua importância

no cotidiano das pessoas que utilizam a rede *wifi* do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia – IFRO, *Campus* Porto Velho Zona Norte. Oferece importantes contribuições tanto para o avanço científico quanto para o aprimoramento das políticas de segurança da Instituição.

Por se tratar de um *campus* acadêmico, contando com um fluxo considerável de usuários da rede *wifi*, destacando alunos, servidores e visitantes, torna-se imperioso dar atenção à segurança da informação. Desta forma, a presente pesquisa buscou identificar possíveis vulnerabilidades existentes na rede *wifi* através de testes por aplicativos e entrevista com a equipe de Tecnologia do campus com o intuito de adquirir conhecimento sobre a estrutura da rede *wireless*.

Considerando os testes realizados através dos aplicativos Fing e Termux, foram identificadas vulnerabilidades na rede *wifi* e imediatamente reportadas ao setor de TI sobre as adversidades existentes, solucionando-as de pronto. Além disso, a realização da pesquisa foi muito bem recepcionada pela equipe de Tecnologia da Informação do referido Campus, que traçaram elogios quanto ao interesse sobre a temática, colaborando com o levantamento de informações quando das entrevistas.

Por fim, este estudo enfatiza a importância de implementar medidas imediatas destinadas a aprimorar a abordagem da segurança da informação em redes *wifi*. Deste modo, propõe-se, em futuras pesquisas, desenvolver ações informativas aos usuários sobre boas práticas da segurança da informação ao navegar na Internet, além de investir em ferramentas de análise que possam identificar possíveis vulnerabilidades na rede *wifi*, aprimoração na rede para desenvolver um controle de acesso individual entre outros fatores.

Uma rede *wifi* segura previne ataques cibernéticos, como interceptação de dados, roubo de informações entre outros, além de manter a integridade e confidencialidade das comunicações. Sua importância é inquestionável, uma vez que visa assegurar confiança dos usuários quanto ao uso da rede, de forma protegida.

REFERÊNCIAS

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: 6 set. 2023.

BARROS, Emanoel Guilherme. **Acesso sem controle a internet: uma abordagem com engenharia social atraves de wireless fidelity (wifi).** Monumenta-Revista Científica

Multidisciplinar, v. 2, n. 1, p. 59-63, 2021. Disponível: https://revistaunibf.emnuvens.com.br/monumenta/article/view/41/23. Acesso em: 6 mar. 2024.

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: 6 set. 2023.

Brasil. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 7 mar. 2024.

Brasil. Decreto nº 9.637, de 26 de dezembro de 2018. **Dispõe sobre a organização e o funcionamento do Sistema Nacional de Políticas sobre Drogas** - Sisnad; institui o seu Comitê Gestor; e dá outras providências. Diário Oficial da União, Brasília, DF, 27 dez. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm. Acesso em: 7 mar. 2024.

Brasil. Decreto nº 11.856, de 26 de dezembro de 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em: 7 mar. 2024.

BOF, Edson. **Segurança em redes wireless.** 2012. Disponível em: https://www.webartigos.com/artigos/seguranca-em-redes-wireless/70234. Acesso em 6 set. 2024.

DEFAVORI, Gustavo. D**etectando falhas e vulnerabilidades em redes IPV4 usando Nessus e NMAP**. 2015. Disponível em: https://ric.cps.sp.gov.br/bitstream/123456789/911/1/20151S_DEFAVORIGustavo_CD2069.pdf. Acesso em: 13 mar. 2024.

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 jan. 2024.

DUARTE, Luiz Otávio. **Análise de vulnerabilidades e ataques inerentes a redes sem fio 802.11 x. 2003.** Disponível em: http://biblioteca.unisced.edu.mz/handle/123456789/1914. Acesso em: 11 mar. 2024.

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 out. 2023.

FIGUEIREDO, Davis Anderson et al. **Vulnerabilidades em redes Wi-Fi de instituições de ensino superior: um estudo de múltiplos casos. Research, Society and Development**, v. 9, n. 2, p. e178921979-e178921979, 2020. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/1979/1821. Acesso em: 6 mar. 2024.

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

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

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 nov. 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 nov. 2023.

NUNES, Bruno Astuto Arouche. **Um sistema de localizaçao para redes wi-fi baseado em nıveis de sinal e modelo referenciado de propagaçao.** Universidade Federal do Rio de Janeiro, COPPE. Rio de Janeiro, Brasil–Maio de, 2006. Disponível em: https://www.ravel.ufrj.br/sites/ravel.ufrj.br/files/publicacoes/tese_bruno.pdf. Acesso em: 6 mar. 2024.

RECCO, Claudineia Helena. S**EGURANÇA DE REDES SEM FIO 802.11: ANÁLISE DAS VULNERABILIDADES SOBRE A ÓPTICA DA SEGURANÇA DA**

INFORMAÇÃO. Disponível em: https://www.revistaresi.com.br/index.php/resi/article/view/10/9. Acesso em: 20 nov. 2023.

SANTOS, LAF d; GULO, C. A. **Segurança da informação**. Recuperado em, v. 15, 2018. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/34613700/Termos_Tecnicos_Fundamentais_-_2014. Acesso em: 19 mar. 2024.

SERAFIM, Lurian Vieira. **Análise de segurança em redes wireless por meio do teste de penetração.** Disponível em: http://repositorio.unesc.net/bitstream/1/8839/1/Lurian%20Vieira%20Serafim.pdf. Acesso em: 19 mar. 2024.

SIMÕES, Diogo Mourão. **Navegação indoor baseada na rede WIFI como suporte a serviços baseados na localização: estudo de caso no campus da UL**. 2015. Tese de Doutorado. Disponível em: https://repositorio.ul.pt/bitstream/10451/20769/1/ulfc115884_tm_Diogo_Sim%c3%b5es.pdf. Acesso em: 6 mar. 2024.

APÊNDICE ÚNICO – QUESTIONÁRIO APRESENTADO NA ENTREVISTA COM O COORDENADOR DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO DO IFRO ZONA NORTE

a) Quantos pontos de acesso (APs) compõem a estrutura da rede wifi do IFRO? Existe um concentrador central para gerenciamento desses APs?
b) Qual é a estimativa da quantidade de alunos que acessam diariamente a rede wifi nas dependências do IFRO?
c) O acesso dos alunos à rede wifi é controlado por meio de login e senha individuais?
d) Existe um login e senha universal fornecido para acesso à rede wifi do IFRO?
e) São implementados mecanismos de controle para regular os *sites* que os alunos podem acessar? Isso inclui o uso de *proxies*, bloqueios de *sites* potencialmente perigosos ou a realização de registros de acessos?
f) Quais são os principais mecanismos de segurança adotados na rede wifi do IFRO? Isso inclui *firewalls*, *proxies* ou outras soluções de segurança?
g) Poderia salientar a importância da adoção de medias de segurança no contexto acadêmico e os resultados indesejados que podem ocorrer se essas medidas não forem tratadas adequadamente?