MAIOS: Um *Switch* Gerenciável Orientado a IoT

Maximiano Eduardo Pereira

Universidade Federal de Uberlândia
Faculdade de Computação
Programa de Pós-Graduação em Ciência da Computação

Uberlândia
2024

Maximiano Eduardo Pereira

MAIOS: Um *Switch* Gerenciável Orientado a IoT

Dissertação de mestrado apresentada ao Programa de Pós-graduação da Faculdade de Computação da Universidade Federal de Uberlândia como parte dos requisitos para a obtenção do título de Mestre em Ciência da Computação.

Área de concentração: Ciência da Computação

Orientador: Professor Dr. Pedro Frosi Rosa

Uberlândia
2024

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

P436 Pereira, Maximiano Eduardo, 1981-
2024 MAIOS: Um Gerenciável Orientado a IoT [recurso eletrônico] / Maximiano Eduardo Pereira. - 2024.

Orientador: Pedro Frosi Rosa.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Ciência da Computação.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.di.2024.349
Inclui bibliografia.
Inclui ilustrações.

1. Computação. I. Rosa, Pedro Frosi,1959-, (Orient.). II. Universidade Federal de Uberlândia. Pós-graduação em Ciência da Computação. III. Título.

CDU: 681.3

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:

Gizele Cristine Nunes do Couto - CRB6/2091
Nelson Marcos Ferreira - CRB6/3074

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Coordenação do Programa de Pós-Graduação em Ciência da Computação
Av. João Naves de Ávila, 2121, Bloco 1A, Sala 243 - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4470 - www.ppgco.facom.ufu.br - cpgfacom@ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Ciência da Computação				
Defesa de:	Dissertação de Mestrado, 16/2024, PPGCO				
Data:	31 de maio de 2024	Hora de início:	14:00	Hora de encerramento:	16:45
Matrícula do Discente:	12112CCP023				
Nome do Discente:	Maximiano Eduardo Pereira				
Título do Trabalho:	MAIOS: A Multi Accountability IoT Oriented Switch				
Área de concentração:	Ciência da Computação				
Linha de pesquisa:	Sistemas de Computação				
Projeto de Pesquisa de vinculação:	Sistemas Seguros e Inteligentes baseados na Internet da Coisas e em Nuvem Aplicados à Indústria e ao Agronegócio				

Reuniu-se por videoconferência, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Ciência da Computação, assim composta: Professores Doutores: Flávio de Oliveira Silva- FACOM/UFU, Sérgio Takeo Kofuji - PSI/EPUSP e Pedro Frosi Rosa - FACOM/UFU, orientador do candidato.

Os examinadores participaram desde as seguintes localidades: Flávio de Oliveira Silva Braga/Portugal e Sérgio Takeo Kofuji- São Paulo/SP . Os outros membros da banca e o aluno participaram da cidade de Uberlândia.

Iniciando os trabalhos o presidente da mesa, Prof. Dr. Pedro Frosi Rosa, apresentou a Comissão Examinadora e o candidato, agradeceu a presença do público, e concedeu o Discente a palavra para a exposição do seu trabalho. A duração da apresentação do Discente e o tempo de arguição e resposta foram conforme as normas do Programa.

A seguir o senhor presidente concedeu a palavra, pela ordem sucessivamente, aos examinadores, que passaram a arguir o candidato. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando o candidato:

Aprovado

Esta defesa faz parte dos requisitos necessários à obtenção do título de Mestre.

O competente diploma será expedido após cumprimento dos demais requisitos, conforme as normas do Programa, a legislação pertinente e a regulamentação

Documento assinado eletronicamente por **Pedro Frosi Rosa**, **Professor(a) do Magistério Superior**, em 17/07/2023, às 12:06, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **João Henrique de Souza Pereira**, **Professor(a) do Magistério Superior**, em 17/07/2023, às 20:48, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **SERGIO TAKEO KOFUJI**, **Usuário Externo**, em 24/07/2023, às 14:00, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4649907** e o código CRC **A82AA638**.

Este trabalho é dedicado à minha amada família: Graziele, Heitor e Yasmin.
São vocês a razão da minha força e coragem. Tudo que faço, faço por amor a vocês.

Agradecimentos

Em primeiro lugar, quero expressar minha profunda gratidão a Deus, Supremo Arquiteto do Universo, cuja graça sustentadora foi meu alicerce durante toda esta jornada. Lembro-me das palavras de Filipenses 4:13, que dizem: "Posso todas as coisas naquele que me fortalece". Deus para mim não é apenas minha base, mas também minha paz inabalável e minha esperança infindável.

À minha querida esposa Graziele, meu eterno apoio e fonte de inspiração, e aos meus filhos, Heitor e Yasmin, que trouxeram luz e alegria à minha vida. Agradeço por compreenderem as longas horas que passei dedicando-me a esta pesquisa e por serem a razão pela qual me esforcei tanto. Aos meus pais, por seu apoio incondicional, e aos meus irmãos, sobrinhos e amigos, por sempre estorcerem por mim momentos de desafio. Cada um de vocês foi fundamental para minha jornada e por isso, minha eterna gratidão.

Aos meus colegas de trabalho, amigos, cuja colaboração e incentivo foram inestimáveis, em especial agradeço ao Elias Teixeira, ao Belkior Alves e ao Ricardo Faval que compartilharam das minhas ideias e forneceram opiniões e apoio, sem vocês teria sido muito mais difícil. Aos meus irmão maçons, que ensinam a cada dia a importância de desbastar a pedra bruta. Cada conversa, cada palavra de encorajamento, moldou este trabalho de maneiras que eu não poderia ter imaginado.

Agradeço também aos meus professores e mentores, que guiaram meus passos e expandiram meu conhecimento. Suas orientações foram cruciais para o desenvolvimento desta tese. Ao meu orientador, Dr. Pedro Frosi, não tenho palavras para agradecer, acredito que cada pessoa é colocada em nossas vidas por alguma razão, acho que esse encontro, serviu para mostrar o quanto eu tenho a aprender e o quanto um apoio pode impulsionar.

Por fim, dedico este trabalho a todos aqueles que se abdicaram da minha presença para que eu pudesse me dedicar a esta jornada. A todos, minha eterna gratidão. Que este trabalho possa ser não apenas um reflexo do meu esforço, mas também uma contribuição valiosa para o nosso campo de conhecimento.

"Eu acredito que às vezes são as pessoas que ninguém espera nada que fazem as coisas que ninguém consegue imaginar."

(Alan Turing)

Resumo

A presente dissertação propõe uma solução para a crescente preocupação com a segurança de dispositivos da Internet das Coisas (IoT - *Internet of Things*) em ambientes domésticos ou empresariais. Intitulado MAIOS (Monitoramento e Aplicação de Inteligência para Redes Orientadas a IoT), o sistema oferece uma arquitetura de um *switch* SDN (*Software Defined Networking*), que proporciona uma segmentação eficaz para dispositivos IoT, aumentando sua proteção contra ameaças cibernéticas.

A pesquisa começa contextualizando o aumento exponencial de dispositivos IoT e os desafios de segurança associados a eles. O MAIOS trata essa questão por meio de uma camada de controle centralizada, que permite o gerenciamento eficiente de dispositivos IoT e a implementação de políticas de segurança dinâmicas, que podem ser aplicadas a partir de uma camada de aplicação do plano de controle SDN.

O sistema foi projetado considerando requisitos funcionais, não funcionais e cenários de implementação, tanto em ambientes domésticos quanto empresariais. Para aumentar a usabilidade, foi desenvolvida uma interface intuitiva para os usuários, facilitando a configuração e monitoramento dos dispositivos IoT. A solução é baseada em tecnologias de código aberto, como pfSense e *Home Assistant*, para fornecer funcionalidades de *firewall*, controle IoT e monitoramento de tráfego em tempo real.

A eficácia do MAIOS é avaliada por meio de testes de segurança e desempenho em ambientes simulados, que demonstraram sua capacidade de identificar e mitigar ameaças cibernéticas, proporcionando uma segurança robusta para os dispositivos IoT.

Esta dissertação oferece uma contribuição para o campo da segurança IoT, apresentando uma solução prática, acessível e eficaz para proteger dispositivos em redes residenciais e empresariais. O MAIOS representa um avanço importante na garantia da segurança digital em um mundo cada vez mais conectado.

Palavras-chave: Cibersegurança. *Internet of Things* (IoT). MAIOS. Redes. *Software Defined Networking* (SDN). Inteligência Artificial (IA).

Abstract

This dissertation proposes a solution to the growing concern about the security of Internet of Things (IoT) devices in home or business environments. Entitled MAIOS (Multi Accountability IoT Oriented Switch), the system offers an SDN (Software Defined Networking) switch architecture, which provides effective segmentation for IoT devices, increasing their protection against cyber threats.

The research begins by contextualizing the exponential increase in IoT devices and the security challenges associated with them. MAIOS addresses this issue through a centralized control layer, which allows efficient management of IoT devices and the implementation of dynamic security policies, which can be applied from an SDN control plane application layer.

The system was designed considering functional, non-functional requirements and deployment scenarios, either in home or business environments. To increase usability, an intuitive interface was developed for users, facilitating the configuration and monitoring of IoT devices. The solution is based on open source technologies such as pfSense proxy/firewall and Home Assistant to provide functionalities such as firewall, IoT control and real-time traffic monitoring.

The effectiveness of MAIOS is evaluated through security and performance tests in simulated environments, which demonstrated its ability to identify and mitigate cyber threats, providing robust security for IoT devices.

This dissertation offers a contribution to the field of IoT security, presenting a practical, affordable and effective solution to protect devices in residential and business networks. MAIOS represents an important advance in ensuring digital security in an increasingly connected world.

Keywords: Cybersecurity. IoT. MAIOS. Network Segregation. SDN. IA.

Lista de ilustrações

Figura 1 – Pontes de Konigsberg (DALLAQUA, 2016) 45
Figura 2 – Representação por Grafo (DALLAQUA, 2016) 46
Figura 3 – Representação de Rede (DALLAQUA, 2016) 46
Figura 4 – Elementos da Comunicação (LIMA, 2019) 46
Figura 5 – Acesso à internet em domicílios brasileiros (IBGE, 2021) 48
Figura 6 – Equipamento usado para o acesso à internet, em 2021 (IBGE, 2021) . 48
Figura 7 – *OpenFlow* na arquitetura SDN 56
Figura 8 – Topologia simples 57
Figura 9 – Funcionamento do MQTT 64
Figura 10 – Exemplo de comunicação MQTT 65
Figura 11 – Método de Pesquisa e Desenvolvimento 68
Figura 12 – Conexão IoT Casa 69
Figura 13 – Conexão IoT Casa <-> Empresa 70
Figura 14 – Conexão IoT Casa <-> Empresa <-> Segura 71
Figura 15 – Arquitetura Geral - *Multi Accountability IoT Oriented Switch* (MAIOS) 75
Figura 16 – Organização em Camadas - MAIOS 75
Figura 17 – MAIOS: Arquitetura proposta 76
Figura 18 – Topologia da simulação no *Global Network Simulator* (GNS3) 82
Figura 19 – Interfaces MAIOS/*pfSense* 82
Figura 20 – Regras de *Firewall* 85
Figura 21 – Monitoramento de logs MAIOS/*pfSense* 85
Figura 22 – Monitoramento de Tráfego MAIOS/*pfSense* 86
Figura 23 – Configuração inicial de rede MAIOS/*pfSense* 88
Figura 24 – Dispositivos Tuya e Sonoff 89
Figura 25 – Integração de dispositivos *Home Assistant* 90
Figura 26 – Exemplo de *dashboard Home Assistant* 91
Figura 27 – Tela com informação de bloqueio de execução de *script Power Shell* . . 93
Figura 28 – Utilização do comando *Get-ExecutionPolicy Power Shell* 93

Figura 29 – Utilização do comando *Set-ExecutionPolicy Power Shell* 93
Figura 30 – Utilização do comando *Get-ExecutionPolicy Power Shell* 94
Figura 31 – Execução do *script - ESXi-Customizer-PS-V2.4.3.ps1* 94
Figura 32 – Parâmetros opcionais do script - ESXi-Customizer-PS-V2.4.3.ps1 . . . 95
Figura 33 – Tela inicial da instalação VMware EXSi 95
Figura 34 – Adaptadores RJ45-USB 96

Lista de tabelas

Tabela 1 – Requisitos Funcionais 72

Lista de siglas

AVA Ambiente Virtual de Aprendizagem

BIOS *Basic Input Output System*

COVID-19 Corona Virus Disease

CPD Centro de Processamento de Dados

CPU *Central Processing Unit*

DHCP *Dynamic Host Configuration Protocol*

DNS *Domain Name System*

DUDH Declaração Universal dos Direitos Humanos

EUA Estados Unidos da América

EAD Educação a Distância

GNS3 *Global Network Simulator*

HTTP *Hypertext Transfer Protocol*

IA Inteligência Artificial

IBGE Instituto Brasileiro de Geografia e Estatística

IBM *International* Business Machines

ICMP *Internet Control Message Protocol*

IDS *Intrusion Detection System*

IEEE *Industrial Electronics Society*

ISIE *33rd IEEE International Symposium on Industrial Electronic*s

IOS *Internetwork Operating System*

IoT *Internet of Things*

IP *Internet Protocol*

IPS *Intrusion Prevention System*

LAN *Local Area Network*

LoRaWAN *Long Range Wide Area Network*

LPWAN *Low Power Wide Area Network*

MAIOS *Multi Accountability IoT Oriented Switch*

MQTT *Message Queuing Telemetry Transport*

MTC *Machine Type Communication*

NAT *Network Address Translation*

NE *Network Element*

NFC *Near Field Communication*

NIDS *Network Intrusion Detection System*

Nmap *Network Mapper*

OMS Organização Mundial de Saúde

OSI *Open System Interconnection*

QoS *Quality of Service*

RAM *Random Acess Memory*

RF Requisito Funcional

RNF Requisito não Funcional

SDN *Software Defined Networking*

SNORT *System for Network and Host-based Event Recognition and Analysis Technologies*

SO Sistema Operacional

TCP *Transmission Control Protocol*

TI Tecnologia da Informação

USB *Universal Serial Bus*

WAN *Wide Area Network*

WI-FI *Wireless Fidelity*

WSN *Wireless Sensor Networks*

VLANs *Virtual Local Area Network*

VPN *Virtual Private Network*

Sumário

1 INTRODUÇÃO . . . 27
1.1 Motivação . . . 28
1.2 Objetivos e Desafios da Pesquisa . . . 29
1.3 Hipótese . . . 29
1.4 Organização da Dissertação . . . 30

2 TRABALHOS CORRELATOS . . . 33
2.1 FamilyGuard: Uma Arquitetura de Segurança para Detecção de Anomalias em Redes Domésticas . . . 34
2.1.1 Pontos de Concordância . . . 34
2.1.2 Pontos de Discordância . . . 35
2.1.3 Como Esses Pontos São Tratados no MAIOS . . . 35
2.2 NEA: Arquitetura de elemento de rede SDN com suporte a MAC definido pela aplicação . . . 35
2.2.1 Pontos de Concordância . . . 36
2.2.2 Pontos de Discordância . . . 37
2.2.3 Como Esses Pontos São Tratados no MAIOS . . . 37
2.3 Privacy-Preserving Defense: Intrusion Detection in IoT using Federated Learning . . . 37
2.3.1 Pontos de Concordância . . . 38
2.3.2 Pontos de Discordância . . . 38
2.3.3 Como Esses Pontos São Tratados no MAIOS . . . 39
2.4 Outros trabalhos . . . 39

3 POSICIONAMENTO DE CONTEXTO . . . 41
3.1 Tecnologia no Mundo . . . 41
3.1.1 Revolução Tecnológica e suas Implicações . . . 43
3.1.2 Sociedade em Rede . . . 43

3.1.3 Conectividade 44
3.1.4 Democratização Tecnológica 47
3.2 A Tecnologia em Tempo de Pandemia 49
3.2.1 Transformações na Comunicação e Conectividade durante a Pandemia . 51
3.2.2 Educação e Trabalho Remoto 52
3.3 Redes de Computadores 53
3.3.1 Redes Definidas por Software - SDN 55
3.3.2 Aplicações de Proteção de Rede 56
3.3.3 Cibersegurança 59
3.4 Automação 60
3.4.1 Automação Industrial 60
3.4.2 Automação Residencial 61
3.4.3 Aplicações na Automação: Desafios na Era da IoT 61
3.5 Internet das Coisas (IoT) 62
3.5.1 Conexão de IoT 64
3.5.2 Segurança em IoT 65

4 MAIOS: PROPOSTA DE UM SWITCH COM PORTA ORIENTADA A IOT 67
4.1 Caracterização do Problema 67
4.1.1 Percepção 67
4.1.2 Análise 69
4.1.3 Necessidades e Desafios 70
4.2 Metodologia de Desenvolvimento 72
4.2.1 Requisitos Funcionais - RF 72
4.2.2 Requisitos Não Funcionais 73
4.2.3 Arquitetura Proposta 74
4.2.3.1 Cenário Residencial 76
4.2.3.2 Cenário Empresarial 76
4.2.3.3 Aplicativos do MAIOS 77

5 EXPERIMENTOS E ANÁLISE DOS RESULTADOS 79
5.1 Ambiente de Simulação e Prototipagem 79
5.1.1 Instalação do GNS3 80
5.1.2 Configuração Inicial 81
5.1.3 Adição de Dispositivos Virtuais 83
5.1.4 Configuração Específica para a Simulação 84
5.1.5 Verificação da Integridade da Simulação 84
5.1.5.1 Verificação de Conectividade 84
5.1.5.2 Monitoramento em Tempo Real 85

5.1.5.3 Verificação de *Logs* e Mensagens do Sistema 86
5.1.5.4 Validação dos Resultados Esperados 86
5.2 Simulação no GNS3 87
5.2.1 Integração do *pfSense* 87
5.2.2 Integração com *Home Assistant* 87
5.2.3 Testes Iniciais 87
5.2.3.1 Segmentação de rede 87
5.2.3.2 Interoperabilidade 89
5.2.3.3 Detecção e Prevenção de intrusão 90
5.3 Protótipo Real 91
5.3.1 Hardware Proposto para os testes (*Switch* MAIOS) 91
5.3.2 Configuração Física 92
5.3.3 Preparação do ambiente 92
5.3.4 Testes de Funcionalidade 95
5.4 Resiliência a Ataques 96
5.5 Resultados Parciais 97

6 CONCLUSÃO 99
6.1 Principais Contribuições 99
6.2 Trabalhos Futuros 101
6.3 Contribuições em Produção Bibliográfica 101

REFERÊNCIAS 103

Capítulo 1

Introdução

A revolução tecnológica ocorrida nas últimas décadas tem propiciado um avanço nas mais diversas áreas da ciência. Como obtemos dados, lidamos com informações e geramos conhecimento, sofreu grande impulsionamento com as novas tecnologias advindas da evolução tecnológica. Na esteira dessa evolução temos um mundo altamente conectado com redes cada vez mais rápidas e dispositivos ainda mais integrados. Desta forma, o mundo, acaba sendo impactado de maneira substancial, seja em sua forma organizacional, econômica ou social.

Para (MACEDO, 2005), a confluência de fatores sociais, políticos e econômicos, conjugados com novas tecnologias de comunicação, permitiu a ascensão da sociedade pós-industrial para a atual sociedade em rede. Não obstante a essa evolução, temos uma significativa popularização de recursos computacionais, motivada pela constante redução dos custos. Ao emergir uma nova versão de hardware ou software, a anterior se torna mais acessível e não menos utilizável.

Aliado a isso temos uma maior rede de conexão e a existência de um marketing imersivo, com estratégias agressivas, que faz uso das novas tecnologias e se insere nos novos meios de comunicação, despertando desejos até pelo que não conhecemos.

Todo cenário explanado até o momento foi a base necessária para o surgimento de um novo recurso altamente dependente e oriundo das evoluções tecnológicas geradas pela revolução retromencionada. Pode se dizer que estamos a presenciar uma nova fase dessa revolução com o surgimento da IoT, Internet das Coisas em português, que tem transformado a maneira como interagimos com o mundo ao nosso redor. A frase "Internet das Coisas" surgiu em 1999 e foi cunhada pelo pesquisador britânico Kevin Ashton e o termo IoT começou a ser utilizado em 2008, com a popularização do Twitter, hoje rebatizado para "X".

Diversas empresas, principalmente aquelas de matriz industrial, fazem uso de sensores e atuadores desde a década de 1950, que foram criados para substituir antigas chaves de acionamento e propiciar a automação. Apesar desses sensores não serem as primeiras "coisas" pensadas pelo pesquisador britânico, acabaram por fornecer um caminho para o

que poderia ser conectado.

A ideia de conectar objetos já era discutida desde 1991, com o advento da utilização dos protocolos *Transmission Control Protocol* (TCP)/*Internet Protocol* (IP) da arquitetura Internet, que conhecemos hoje. Logo, com a melhora da estrutura de comunicação pensar em objetos conectados se tornou factível.

A melhora nas redes e nas formas de conexão permitiram não só que pessoas se conectassem, mas também que novos dispositivos pudessem ser integrados, isto é, "coisas" passaram a ser constantes na vida das pessoas. Esses dispositivos são capazes de suprir o usuário com diversos tipos de dados, sejam voltados para área da saúde, do clima, do conforto ou para automação, com a comunicação M_2M**!** (M_2M**!**) ou *Machine Type Communication* (MTC), em tempos de 5G. Com tudo isso, tivemos o surgimento de diversos dispositivos, pavimentados pelo desenvolvimento em redes de sensores sem fio (*Wireless Sensor Networks* (WSN)), telecomunicações e informática (SHAFIQUE et al., 2020. https://doi.org/10.1109/ACCESS.2020.2970118; SANTOS et al., 2018).

No contexto da evolução, vemos os dispositivos ficarem cada vez menores, com maior poder computacional e acessíveis ao grande público. Estimativas da *IoT Analytics*, consultoria que atua na área de IoT, apontam para 16,7 bilhões até o final do ano de 2023 e existirão mais de 29 bilhões até o ano de 2027 (SINHA, 2023). Ainda que os números pareçam altos, no mesmo estudo da IoT Analytics 2023, essa perspectiva ainda leva em conta a oferta de *chipsets* que segue restrita e incertezas ma China em constante atrito com os Estados Unidos da América (EUA).

O objeto de estudo deste trabalho é propor a arquitetura de uma solução para a conexão segura desses dispositivos à rede, principalmente para usuários domésticos, que buscam bem-estar e conforto em suas residências, que se tornaram extensões dos escritórios com o serviço remoto, por meio dessas novas tecnologias.

1.1 Motivação

Dispositivos inteligentes estão fomentando a relação humano-máquina, ampliando o conceito da computação ubíqua, tornando seu uso natural e até mesmo imperceptível (SACCOL; SCHLEMMER; BARBOSA, 2021). A sociedade passou a ter acesso a uma infinidade de possibilidades, inclusive a de trabalhar ou desenvolver atividades de maneira remota. Houve um aumento significativo de postos de trabalho à distância e até mesmo a educação passou a ser ressignificada com as novas possibilidades existentes em plataformas de educação a online.

Todo o cenário de trabalho remoto foi impulsionado pelo que vivemos desde meados do ano de 2020 até o ano corrente, quando a Organização Mundial de Saúde (OMS) declarou, em maio de 2023, o fim da emergência de saúde pública. A pandemia global de Corona Virus Disease (COVID-19) forçou a adoção de uma abordagem nunca vista na história,

levando ao desenvolvimento de ações que mobilizaram toda a comunidade cientifica para busca de soluções, sendo que o isolamento e medidas de controle foram as adotadas em grande escala.

Em um curto espaço de tempo, sem nenhum tipo de preparação, as pessoas não puderam se locomover de um local para outro, trabalhar ou desenvolver normalmente suas atividades. A circulação de pessoas nas ruas foi restringida e somente serviços essenciais foram mantidos.

Todo o avanço tecnológico, que antes era eventualmente um desejo, virou mandatório, ajudou na busca de soluções e propiciou um certo grau de conforto. As pessoas isoladas puderam manter o contato com seus entes queridos e ser informadas de medidas a serem adotadas. O cenário pandêmico propiciou um aumento significativo no trabalho remoto e revisitou desafios cruciais relacionados à segurança de rede e à integração de dispositivos IoT. Sendo isso a principal motivação para a proposta deste estudo.

Enquanto a adoção do trabalho remoto se acelerava durante o período pandêmico, muitas empresas optaram por permitir que seus funcionários desenvolvessem suas atividades em ambientes domésticos, com seus próprios equipamentos, para manter a continuidade dos negócios. Em muitos casos, necessitou-se apenas de um computador conectado à internet para a execução das atividades. Todavia, pergunta-se: os milhões gastos em cibersegurança pelas empresas em suas sedes podem garantir a segurança em postos avançados na residência de seus colaboradores?

1.2 Objetivos e Desafios da Pesquisa

Esta dissertação visa abordar uma lacuna crítica na segurança de rede. Temos o **objetivo geral** de **desenvolver uma solução de hardware** que permita a **criação de conexões segregadas para dispositivos IoT** em uma rede local, preservando a integridade e a confidencialidade dos dados, **sem prejudicar a conectividade** desses dispositivos. De maneira específica pretendemos:

- ❏ Realizar pesquisa bibliográfica para conhecer o estado da arte acerca do tema;
- ❏ Desenvolver um modelo conceitual referente à proposta;
- ❏ Desenvolver em bancada um modelo funcional do projeto;
- ❏ Analisar a viabilidade do projeto;
- ❏ Traçar um paralelo da proposta em funcionamento e o modelo atual; e
- ❏ Avaliar os resultados de maneira pormenorizada.

1.3 Hipótese

A integração de dispositivos pessoais à infraestrutura de rede corporativa gerou preocupações crescentes em relação à segurança da informação. As empresas têm tradicional-

mente investido recursos consideráveis em medidas de segurança, como *firewalls*, sistemas de detecção de intrusões (*Intrusion Detection System* (IDS)) e autenticação multifatorial, para proteger seus dados confidenciais e propriedade intelectual.

Ocorre que o usuário final não precisa se preocupar com elementos de configuração sofisticados para instalação dos IoT. Em questão de poucos cliques é possível colocar o dispositivo em operação. Entretanto, essa facilidade pode gerar problemas justamente no que diz respeito à privacidade, pois tudo é transparente ao usuário e informações pessoais passam ou podem ser compartilhadas com fabricantes desses dispositivos.

À medida que a IoT se expande em residências e empresas, uma questão crítica surge: como podemos permitir que dispositivos IoT se conectem à rede sem comprometer a segurança da informação? Até o momento, roteadores e *switches* convencionais não oferecem uma solução dedicada para isolamento e gerenciamento seguro de dispositivos IoT em uma rede local. Isso cria uma vulnerabilidade potencial que pode ser explorada por cibercriminosos para acessar informações sensíveis ou controlar dispositivos IoT, comprometendo a privacidade e a segurança dos usuários.

Ferramentas de anti-vírus e IDS atuam para notificar usuários em seus equipamentos e *firewalls* atuam no perímetro das redes. Note-se que Elementos de Rede (*Network Element* (NE)), tais como *switches*, ficam desprovidos de capacidade de ser controlados para responder a incidentes de segurança.

A hipótese deste trabalho é que um elemento de rede, como o *switch* MAIOS, com uma porta dedicada a IoT, capaz de interagir com aplicações da camada de Aplicação[1] do Plano de Controle SDN, pode incrementar a segurança na rede em seu contexto, tornando-as mais seguras em termos de ameaças de segurança em dispositivos IoT.

1.4 Organização da Dissertação

Esta dissertação está organizada do seguinte modo. O capítulo corrente buscou introduzir o assunto, externar a motivação para seu desenvolvimento, bem como definiu os objetivos gerais e específicos do trabalho, terminando com a hipótese.

O capítulo 3 inicia a exploração teórica, delineando o cenário tecnológico global. Nele são abordadas questões fundamentais, como a Revolução Tecnológica e suas implicações, a Sociedade em Rede, Conectividade e Democratização Tecnológica. Este capítulo também investiga o impacto da tecnologia durante a pandemia, especialmente nas áreas de comunicação, conectividade, educação e trabalho remoto. Além disso, são discutidos tópicos correlatos, tais como Redes de Computadores, Automação e IoT

O capítulo 4 mergulha na proposta de pesquisa, começando com uma caracterização do problema. É apresentada a metodologia de desenvolvimento, delineando requisitos

[1] Essas aplicações podem ser dotadas de técnicas de IA tais como *Machine Learning*, que podem coletar evidências e comunicá-las ao MAIOS por meio do plano de Controle SDN

funcionais e não funcionais, culminando com o modelo conceitual. A arquitetura proposta é descrita em dois cenários distintos: residencial e empresarial. Aplicações específicas do MAIOS são detalhadas, oferecendo uma visão clara de sua funcionalidade e potencial.

O capítulo 5 foi destinado para explanação dos testes realizados e nele é detalhada a metodologia usada para avaliação. São apresentados os experimentos e analisados os resultados obtidos. Cada passo dos experimentos é realizado de maneira a garantir a transparência e replicabilidade.

A conclusão do trabalho é apresentada no capítulo 6, onde são apontadas percepções, as principais contribuições, possíveis trabalhos futuros e contribuições em produção bibliográfica.

Capítulo 2

Trabalhos Correlatos

Este capítulo tem o objetivo de analisar as principais pesquisas e trabalhos que possuam correlação direta ou indireta com a presente dissertação. A importância de explorar trabalhos correlatos vai além de situar nosso estudo no contexto acadêmico; trata-se de entender o estado da arte no campo de investigação, identificar lacunas no conhecimento existente e estabelecer as bases teóricas e práticas que possam embasar e direcionar a evolução da nossa proposta.

Busca-se compreender como os pesquisadores têm abordado os desafios que emergem com a crescente adoção de dispositivos conectados, como os dispositivos IoT (Internet das Coisas), e a complexidade associada à segurança de redes heterogêneas. Esses trabalhos fornecem percepções valiosas sobre metodologias, tecnologias e limitações enfrentadas, permitindo que novas soluções sejam projetadas para atender às demandas atuais e futuras.

O universo da computação é amplo e quando falamos em IoT temos a real proporção de seus efeitos, visto a gama de dispositivos que se conectam na rede a todo momento. Deste modo, podemos falar que tal assunto, embora não seja novo, corresponde um desafio enorme.

Portanto, este capítulo busca conectar o presente trabalho a pesquisas que fundamentam e inspiram suas soluções, destacando abordagens inovadoras, pontos de convergência e diferenciais que agregam valor ao nosso estudo. Acredita-se que será possível fortalecer os alicerces da proposta apresentada, contribuindo com conhecimentos e experiências para uma sociedade mais segura e conectada.

2.1 FamilyGuard: Uma Arquitetura de Segurança para Detecção de Anomalias em Redes Domésticas

FamilyGuard (MELO, 2023) propõe uma solução inovadora para os desafios de segurança em redes domésticas. Esta pesquisa aborda a crescente presença de dispositivos IoT em ambientes residenciais, os problemas associados à heterogeneidade desses dispositivos e às limitações de hardware e software. Este trabalho foi escolhido em função da similaridade na abordagem e preocupação com a segurança de rede em ambientes domésticos.

FamilyGuard projeta uma arquitetura baseada no paradigma de Redes Definidas por Software (SDN), que oferecem flexibilidade e capacidade de monitoração e controle em redes residenciais.

Nossa proposta, MAIOS (**??**), também se baseia em SDN para oferecer uma arquitetura de rede doméstica que possa se adaptar a cenários de uso de IoT em residências. *FamilyGuard* combina algoritmos de aprendizado de máquina, tanto supervisionados quanto não supervisionados, para a detecção e classificação de tráfego anômalo, destacando-se por avaliar três aspectos: (i) a implementação da arquitetura em hardware de baixo custo; (ii) a eficiência dos modelos de aprendizado de máquina na detecção de ameaças; e (iii) o tempo de resposta do sistema.

Os experimentos realizados demonstraram a viabilidade do uso de modelos não supervisionados para identificar anomalias e algoritmos supervisionados para classificar ameaças. Os resultados indicaram Área Sob a Curva (AUC) superior a 94% nos cenários analisados, evidenciando a eficácia da proposta. Ademais, *FamilyGuard* contribui com o campo de Cibersegurança ao propor uma camada adicional de proteção a redes residenciais, com foco em mitigar ameaças cibernéticas e aprimorar a privacidade.

É uma importante referência para nosso trabalho, pois demonstra que a preocupação com a segurança de redes domésticas não é irrelevante e em proporção maior, à preocupação com novos dispositivos que ingressam em uma rede já complexa, notadamente os IoT, que trazem não só soluções, mas grandes desafios.

2.1.1 Pontos de Concordância

Primeiramente, o trabalho reconhece o crescimento de dispositivos inteligentes nos ambientes residenciais, evidenciando que a adoção de novas tecnologias ocorre em escala global. A oferta de novos dispositivos, de diversos fabricantes e mercados, aumenta a complexidade da integração e gerenciamento, sendo um dos pontos de contribuição do MAIOS no que tange à interoperabilidade.

Adicionalmente, *FamilyGuard* propõe uma arquitetura de segurança que inclui o monitoramento de anomalias como abordagem central. Essa solução é pensada para atender

a necessidades práticas, utilizando hardware de baixo custo para viabilizar sua aplicação. Outro ponto de concordância é que ambos os trabalhos enfatizam a utilização de aprendizado de máquina como ferramenta para gerar conhecimento sobre anomalias e aprimorar os mecanismos de segurança, o que está alinhado com as estratégias adotadas no MAIOS.

2.1.2 Pontos de Discordância

FamilyGuard propõe uma nova arquitetura de segurança para redes domésticas, com ênfase na detecção de anomalias e na proteção contra ameaças, enquanto que MAIOS propõe uma solução mais abrangente, adicionando a capacidade de prover um sistema capaz de se retroalimentar por meio de sua camada *Controller*. Essa camada permite o aprendizado continuo com novas anomalias identificadas, ajustando suas políticas e melhorando sua eficiência ao longo do tempo. Além disso, diferentemente do *FamilyGuard*, MAIOS propõe a segregação de rede especializada para IoT, garantindo que cada elemento de tráfego dentro da residência tenha uma parte dedicada e segura dentro da infraestrutura.

Outra diferença é o escopo de aplicação. Enquanto *FamilyGuard* é projetado especificamente para ambientes residenciais, nossa abordagem expande seu alcance para atender tanto ambientes domésticos quanto corporativos. Essa adição é fundamental, dado que dispositivos IoT teve origem ligada ao contexto industrial, onde sensores e atuadores desempenham funções críticas. Essa adaptabilidade permite que se atenda a uma gama maior de necessidades.

2.1.3 Como Esses Pontos São Tratados no MAIOS

No MAIOS, a segregação de redes para dispositivos IoT é tratada por meio de uma arquitetura baseada em SDN que permite a criação de conexões segmentadas e seguras. Além disso, foi priorizada a utilização de ferramentas de código aberto, como o *firewall* pfSense e o *HomeAssistant*, durante a fase de testes.

O pfSense possibilitou a análise de segurança por meio de sistemas de prevenção e detecção de intrusão (IPS e IDS), enquanto que o *HomeAssistant* foi essencial para garantir a interoperabilidade com uma ampla gama de dispositivos, mesmo aqueles de fabricantes distintos e que não compartilham protocolos comuns.

2.2 NEA: Arquitetura de elemento de rede SDN com suporte a MAC definido pela aplicação

NEA (MOLINOS, 2024) apresenta uma arquitetura de um switch SDN com suporte a MAC Definido pela Aplicação. NEA propõe instanciar métodos de acesso ao meio (MAC - *Medium Access Control*) para melhorar a Qualidade de Serviço (QoS) e a Qualidade da

Experiência do Usuário (QoE) em redes SDN. Esta pesquisa se destaca por propor um protótipo de *switch* que manipula políticas de encaminhamento a partir de requisitos da camada de aplicação do plano de dados, implementando MAC orientado por requisitos de aplicações.

O trabalho aborda os desafios da arquitetura de Internet existente, destacando as limitações da abordagem tradicional para separação entre os planos de controle e de dados das redes SDN. NEA permite a reprogramação sistemática do comportamento do switch, atribuindo parâmetros como priorização de tráfego, controle de banda e burst de forma granulada, além de possibilitar a segmentação de diferentes fluxos na mesma porta física com base nas necessidades das aplicações.

O trabalho foi escolhido como referência pela utilização de software e APIs para desenvolver soluções flexíveis e programáveis, integrando conceitos como controle por Ontologias, suporte ao protocolo ETSCP e uso de módulos como NEA-Scheduler e NEA-Control. Os resultados experimentais evidenciam avanços significativos em termos de QoS, com destaque para melhorias no desempenho do plano de dados e maior confiabilidade em comunicações sensíveis ao tempo.

NEA apresenta diversas similaridades com MAIOS, refletindo preocupações comuns relacionadas a otimização e segurança em ambientes de rede. Alguns pontos de convergência incluem: a utilização do paradigma SDN para melhorar a gestão e segurança de redes; o controle granular e a programabilidade do plano de dados, permitindo a configuração de políticas específicas para diferentes fluxos; a escolha por soluções baseadas em software e código aberto, reforçando a flexibilidade e escalabilidade das soluções propostas; e a melhoria da QoS como objetivo central, integrando mecanismos que favorecem comunicações mais eficientes e confiáveis.

2.2.1 Pontos de Concordância

Ambos os trabalhos possuem propostas de criação de um hardware dedicado baseado em SDN. Tanto NEA quanto MAIOS enfatizam a utilização de sistemas embarcados para implementar as funcionalidades dos switches, demonstrando o potencial desses dispositivos para lidar com desafios técnicos específicos no contexto de redes SDN.

Ambas as propostas destacam que soluções convencionais não atendem plenamente às demandas atuais de Qualidade de Serviço (QoS) e Qualidade da Experiência do Usuário (QoE). Assim, NEA e nosso projeto buscam explorar novas arquiteturas que superem essas restrições, utilizando tecnologias modernas e integrando software e hardware de forma mais eficiente.

Os dois trabalhos compartilham uma visão sobre a importância de oferecer suporte a múltiplos fluxos de dados em uma única porta física, configurando parâmetros como priorização de tráfego e controle de banda de maneira adaptável. Essa capacidade é fundamental para atender às necessidades de aplicações variadas, incluindo aquelas sensíveis

a tempo, como *streaming* de áudio ou vídeo. No caso do MAIOS, essa capacidade de segregação de dados poderia atender à necessidade de separação de tráfego IoT.

2.2.2 Pontos de Discordância

Apesar das similaridades, MAIOS tem como foco o oferecimento de maior segurança por meio da segregação de redes IoT e interoperabilidade. Além disso, nossa proposta explora a retroalimentação do sistema através da camada *Controller*, permitindo aprendizado contínuo e aprimoramento das políticas de segurança, enquanto NEA tem foco em QoS/QoE no plano de dados.

Como mencionado, a incorporação de módulos para segregação de rede e interoperabilidade com dispositivos IoT de diferentes fabricantes, é um aspecto não diretamente abordado pelo NEA. Em nosso projeto, a preocupação com a QoS e a segurança é abordada de forma integrada, utilizando uma arquitetura SDN que permite segregação e gerenciamento de dispositivos IoT por meio de ferramentas de código aberto, como o pfSense e o HomeAssistant. Essa abordagem promove a interoperabilidade entre dispositivos e melhora a experiência do usuário ao simplificar o controle e a segurança do ambiente de rede.

2.2.3 Como Esses Pontos São Tratados no MAIOS

A inclusão de uma camada de aprendizado contínuo possibilita que o sistema se adapte às novas ameaças e necessidades, reforçando a eficiência e a proteção da rede. Em adição, nossa interface foi projetada para ser intuitiva, garantindo que mesmo usuários com pouco conhecimento técnico consigam gerenciar suas redes com facilidade.

2.3 Privacy-Preserving Defense: Intrusion Detection in IoT using Federated Learning

Dini et al. (2024) introduzem uma abordagem para enfrentar os desafios de segurança em redes IoT por meio do uso de aprendizado federado (FL - *Federated Learning*) (DINI et al., 2024). O trabalho foca na criação de Sistemas de Detecção de Intrusão (IDS) que preservem a privacidade dos dados, enquanto monitoram o tráfego em redes IoT.

O estudo demonstra a viabilidade de usar FL para treinar modelos de IDS, garantindo que dados sensíveis permaneçam em dispositivos locais. FL elimina a necessidade de compartilhamento centralizado de informações, o que é uma das grande preocupações da atualidade, no que tange a privacidade de dados presentes nas redes. Tal abordagem pode favorecer o aprendizado distribuído para contribuir ainda mais com o crescimento da acurácia na detecção de anomalias.

Baseado em três conjuntos de dados (*dataset*) de tráfego IoT de última geração, os experimentos exploram a eficiência do treinamento descentralizado em comparação com os métodos centralizados. O artigo destaca que os métodos baseados em FL alcançaram desempenho equivalente ao treinamento centralizado em diversas métricas de eficiência, como F1-score, MCC (*Matthew's Correlation Coefficient*) e acurácia. Além disso, os modelos com FL apresentaram tempos de convergência menores, demonstrando maior escalabilidade e eficiência.

2.3.1 Pontos de Concordância

Similar ao MAIOS, o artigo utiliza sistemas embarcados como base para execução de tarefas relacionadas à segurança. Ambos os trabalhos propõem arquiteturas que integram planos de Controle e de Dados (SDN), evidenciando a importância de uma abordagem modular para atender a requisitos específicos de redes heterogêneas.

Assim como MAIOS, o artigo reconhece que dados gerados por dispositivos IoT frequentemente contêm informações sensíveis, o que torna essencial o uso de técnicas que minimizem os riscos de vazamento de informações. A aplicação de FL para treinamento distribuído é uma escolha alinhada à necessidade de preservar a privacidade, sem comprometer a precisão dos modelos. Adicionalmente, o uso de aprendizado de máquina é central em ambas as abordagens para identificar padrões anômalos em tráfego de rede, permitindo a detecção proativa de ataques.

Além disso, a importância dada à utilização de conjuntos de dados amplos e representativos também converge com nossa proposta, destacando a relevância de bases de dados atualizadas e bem rotuladas para garantir a generalização dos modelos. Por fim, ambos os trabalhos compartilham a preocupação em otimizar os processos de treinamento, garantindo que as soluções propostas sejam escaláveis e aplicáveis a cenários reais, com dispositivos de capacidade computacional limitada.

2.3.2 Pontos de Discordância

FL apresenta diferenças importantes em relação ao MAIOS. Enquanto MAIOS enfatiza a segregação de rede especializada para IoT, como um elemento-chave para aumentar a segurança e a interoperabilidade, FL foca na detecção de intrusões por meio de aprendizado de máquina descentralizado. Em nossa arquitetura, o controle e monitoramento de dispositivos IoT são tratados de forma mais integrada, explorando não apenas a detecção de anomalias, mas também a prevenção por meio da aplicação dinâmica de regras de *firewall* e segmentação de tráfego.

Outra diferença é que nosso projeto inclui uma interface intuitiva e voltada para usuários leigos, enquanto o artigo prioriza o desempenho técnico em ambientes de pesquisa e desenvolvimento. Além disso, nossa abordagem incorpora uma camada *Controller*, para

aprendizado contínuo, permitindo que o sistema ajuste automaticamente suas políticas com base nas análises realizadas, o que não é diretamente abordado na solução baseada em FL apresentada no trabalho.

2.3.3 Como Esses Pontos São Tratados no MAIOS

MAIOS busca não apenas detectar ameaças, mas também preveni-las, utilizando uma arquitetura baseada em SDN, que permite a segregação de tráfego e controle granular de dispositivos IoT.

A utilização de aprendizado contínuo permite ao sistema adaptar-se rapidamente a novas ameaças, enquanto a segmentação de rede protege o tráfego de dispositivos IoT de acessos não autorizados. A combinação dessas estratégias nos diferencia, oferecendo uma solução abrangente que atende tanto às necessidades domésticas quanto corporativas.

FL se destaca como uma contribuição importante para a área de segurança em IoT, especialmente pela aplicação inovadora de aprendizado federado, para preservação da privacidade. As similaridades de FL com MAIOS reforçam a relevância de arquiteturas baseadas em aprendizado de máquina e sistemas embarcados para a detecção de anomalias em redes IoT. Acreditamos que MAIOS poderá complementar esses esforços, contribuindo para redes mais seguras e adaptáveis em diferentes contextos.

2.4 Outros trabalhos

Com já mencionado, privacidade é uma grande preocupação da atualidade no que diz respeito a dados e compartilhamento de informações e, nesse sentido, é fundamental MAIOS ter uma visão que propicie os mecanismos capazes de atender esses requisitos. Deste modo o trabalho "P2IDF: *A Privacy-Preserving based Intrusion Detection Framework for Software Defined Internet of Things-Fog* (SDIoT-Fog)" (KUMAR; TRIPATHI; GUPTA, 2021), apresenta contribuições importantes ao lidar com a privacidade de dados na detecção de intrusão. MAIOS possui em comum a busca de segurança para dispositivos IoT, sendo que a abordagem do trabalho de Kumar, Tripathi e Gupta (2021) amplifica essa preocupação ao adicionar o componente de privacidade no contexto.

Embora tenhamos abordagem distintas, esse trabalho fornece uma visão ampla sobre mecanismo de detecção de intrusão, oferecendo uma solução (P2IDF) que se baseia nessa detecção com a preocupação da privacidade. A proposta integra aprendizado de máquina e técnicas de preservação de privacidade, como criptografia homomórfica, para realizar a detecção de anomalias sem comprometer os dados sensíveis. Os experimentos mostram que o *framework* é eficiente em cenários distribuídos, com alta escalabilidade e compatibilidade com dispositivos de baixa capacidade computacional.

P2IDF é altamente relevante para nosso trabalho, pois aborda simultaneamente três pilares cruciais para o projeto: redes SDN, segurança em IoT e preservação de privacidade.

Ele reforça o uso de aprendizado distribuído em cenários com recursos limitados, como redes domésticas ou corporativas que incorporam dispositivos IoT. Além disso, a abordagem orientada a *Fog Computing* pode ser inspiradora para expandir nossa aplicação para arquiteturas híbridas (Edge/Fog/Cloud).

Outro trabalho relevante, no sentido de entender como avaliar a eficácia de nossa proposta, "UNSW-NB15: *A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set*" (MOUSTAFA; SLAY, 2015), introduz o conjunto de dados UNSW-NB15, amplamente utilizado para avaliar sistemas de detecção de intrusão. Ele fornece uma base diversificada e representativa de tráfego de rede, incluindo cenários normais e maliciosos. A importância desse trabalho é de realmente entender como podemos testar nossa solução, provendo um ambiente com dados atualizados. Entendemos a partir dele que conjuntos de dados devem ser sempre revisitados e são vitais para qualquer ferramenta que se pretende mitigar quaisquer ameaças.

Embora esse trabalho possua pontos de concordância apenas no diz respeito a utilidade, ainda assim, é uma importante ferramenta não só para o desenvolvimento do MAIOS, como também seu aperfeiçoamento.

Capítulo 3

Posicionamento de Contexto

Nos últimos anos, o avanço tecnológico tem impactado profundamente diversas áreas, incluindo a segurança, que enfrenta desafios cada vez mais complexos. Grande parte dos esforços na área de segurança tecnológica tem sido direcionada a ambientes corporativos e industriais, deixando o domínio doméstico em segundo plano, mesmo com o aumento exponencial do uso de dispositivos conectados, conhecidos como Internet das Coisas (IoT).

A integração de dispositivos IoT em residências trouxe benefícios significativos, como automação e monitoramento remoto, mas também abriu novas portas para vulnerabilidades e ameaças à segurança. Estudos recentes indicam que muitos dispositivos IoT domésticos possuem falhas de segurança que podem ser exploradas por atacantes, expondo os usuários a riscos como invasões de privacidade e comprometimento de redes.

Este trabalho busca explorar as interseções entre segurança e IoT, com ênfase no ambiente doméstico. Embora este seja o foco principal, muitos dos desafios e soluções analisados têm aplicabilidade em contextos corporativos e industriais. Ao compreender o panorama atual da segurança em dispositivos IoT, é possível identificar lacunas e propor soluções que fortaleçam a proteção de redes locais, ampliando a confiabilidade desses sistemas no futuro.

3.1 Tecnologia no Mundo

O entendimento do que é tecnologia para o público geral está intrinsecamente entrelaçado com dispositivos eletrônicos e, de maneira geral, com a computação. No entanto, seu alcance vai além dessas fronteiras, estendendo-se a todas as ações humanas que envolvem o estudo de técnicas, processos ou métodos destinados a fornecer meios para atender às necessidades humanas. Para Batista e Freire (2014), sem dúvida nenhuma, a relação da tecnologia e a sociedade é complexa:

> Tornar a tecnologia algo complexo não é abordar relações externamente, mas problematizar em que medida a sociedade, a ciência, a tecnologia e a educação se constroem nessas relações e não a partir delas enquanto

> dimensões que não apenas se comunicam, mas se inter determinam num processo cuja complexidade deve ser levada a sério (BATISTA; FREIRE, 2014).

Empregada pela humanidade desde a antiguidade, a tecnologia tem sido companheira constante do ser humano, influenciando sua forma de ver o mundo. Sua evolução deixou uma marca profunda no desenvolvimento da humanidade. Podemos encontrar grandes exemplos desse progresso tecnológico nos momentos cruciais da história, como a descoberta do fogo, que permitiu a humanidade dominar a escuridão da noite e se proteger dos predadores, ou a invenção da roda, que revolucionou o transporte e a logística. Segundo Andrade (2019) a tecnologia abrange uma gama imensa de invenções e descobertas que passa pela descoberta do fogo (ANDRADE, 2019).

Da mesma forma, outros marcos como o desenvolvimento da agricultura, que permitiu a sedentarização das comunidades, ou a invenção da imprensa, que democratizou o acesso ao conhecimento, também são evidências do impacto profundo da tecnologia na sociedade.

À medida que avançamos na linha do tempo, somos testemunhas do surgimento de inovações como a vacina, que transformou a medicina e salvou inúmeras vidas, e o microprocessador, que deu origem à revolução digital e à era da computação pessoal. A lista de recursos tecnológicos que moldam como percebemos e interagimos com o mundo é extensa e em constante expansão. Ainda segundo Batista e Freire (2014):

> Os aparatos tecnológicos, se não são a tecnologia em si, são o seu arauto em diferentes épocas e regiões. Se hoje temos a representação social do computador como o ícone da inovação e do desenvolvimento, o trem, por exemplo, desempenhou papel similar no período chamado de Segunda Revolução Industrial, no final do século XIX (BATISTA; FREIRE, 2014).

Embora pôr definição a tecnologia seja ligada a métodos e técnicas, vemos que ela não é só uma ferramenta; é uma resposta à necessidade fundamental do ser humano de melhorar sua qualidade de vida. Cada avanço tecnológico é motivado por um desejo de resolver problemas específicos ou abordar desafios amplos. No entanto, à medida que avançamos e exploramos novas fronteiras tecnológicas, novas possibilidades emergem, desencadeando uma sequência infinita de desafios cada vez mais complexos. Esse ciclo de inovação contínua impulsiona o mundo em direções que, em tempos passados, poderiam parecer inimagináveis. A ciência está diretamente relacionada com a sociedade de seu tempo e é com base nas prioridades definidas pela sociedade do momento que a ciência acaba se desenvolvendo, moldando-se para atender aos questionamentos dessa sociedade (RONAN, 1987).

Assim, compreender a evolução tecnológica e suas implicações é essencial para situar o presente trabalho, que busca explorar o papel da tecnologia em um contexto específico, destacando suas contribuições e desafios. À medida que avançamos, a tecnologia

segue como um catalisador para mudanças sociais, econômicas e culturais, redefinindo constantemente a maneira como vivemos e interagimos.

3.1.1 Revolução Tecnológica e suas Implicações

Ao longo da história, as transformações tecnológicas têm desempenhado um papel decisivo na maneira como percebemos e interagimos com o mundo. Essas mudanças têm sido marcantes, com impactos profundos que alteraram as estruturas sociais, econômicas e culturais, acompanhados por uma velocidade crescente de inovação. Klaus Schwab, presidente executivo do Fórum Econômico Mundial, observa que estamos no início de uma revolução que remodelará profundamente nossa maneira de viver, trabalhar e nos relacionar, destacando que a Quarta Revolução Industrial é algo sem precedentes na história humana (SCHWAB, 2016 apud SILVA et al., 2018).

A ideia de revolução tecnológica não se limita a uma linha do tempo rígida, mas sim ao impacto significativo que as inovações tecnológicas têm em cada época. A revolução desencadeada por uma tecnologia é definida pelo efeito que ela causa no contexto em que surge, moldando a sociedade em uma nova direção.

Com a invenção do microprocessador, o protocolo TCP/IP e o microcomputador, a Revolução da Tecnologia da Informação, que começou na década de 1970, inaugurou uma nova era de possibilidades e conectividade. Esse período, como destacado por Castells, marcou o início de uma nova era em que as tecnologias de comunicação passaram a ser essenciais para a organização social e econômica, criando as bases para o mundo digital e interconectado que vivemos hoje (CASTELLS, 1999).

Nesse cenário de transformações rápidas e contínuas, as tecnologias da Quarta Revolução Industrial, como a IoT, não apenas facilitam as interações humanas, mas também impõem novos desafios. A maneira como trabalhamos, nos relacionamos e enfrentamos questões éticas e de privacidade tem sido moldada por essas inovações. À medida que a tecnologia se infiltra ainda mais em nossas vidas cotidianas, é essencial estar ciente das implicações que ela traz e dos novos dilemas sociais que surgem com a conectividade cada vez maior.

A velocidade das mudanças tecnológicas exige que os indivíduos se adaptem constantemente a um universo informacional em constante evolução. Novos dispositivos e soluções, como celulares inteligentes, softwares avançados, realidade virtual e outras tecnologias emergentes, estão continuamente sendo desenvolvidos, trazendo novas formas de interagir com o mundo ao nosso redor (KENSKI, 2012 apud VILACA; ARAUJO, 2016).

3.1.2 Sociedade em Rede

A sociedade contemporânea é marcada pela ampla interconexão entre pessoas, organizações e dispositivos, possibilitada por redes de comunicação digital. Esse ambiente

transforma profundamente as dinâmicas sociais, econômicas e culturais, com a conectividade desempenhando um papel central na maneira como nos comunicamos, acessamos informações e tomamos decisões.

A interação humana sempre foi um elemento essencial para o desenvolvimento social. No contexto atual, essa interação é potencializada pela tecnologia, que facilita a comunicação em escala global, superando barreiras de tempo e espaço. Para Castells (1999), o advento da comunicação digital não apenas amplia as interações humanas, mas também redefine as estruturas sociais, promovendo uma "sociedade em rede"caracterizada pela centralidade das informações e pela descentralização do poder.

A acessibilidade à informação é um dos principais pilares dessa sociedade em rede. A Internet possibilita o acesso a vastos volumes de dados, influenciando como aprendemos, trabalhamos e nos organizamos. Essa facilidade de acesso contribui para a descentralização do conhecimento, promovendo a colaboração em plataformas digitais e a criação de redes autônomas de aprendizado e inovação. Como afirma Levy (2000), o saber não está mais centralizado em uma fonte única, mas distribuído em redes colaborativas, acessíveis a todos.

Além disso, a descentralização característica da sociedade em rede altera estruturas tradicionais de organização, substituindo hierarquias rígidas por formas mais distribuídas de interação e compartilhamento. Isso se reflete em diversos aspectos da vida contemporânea, desde movimentos sociais organizados em plataformas digitais até mudanças nas estruturas de poder e governança. Segundo Kenski (2012), a evolução tecnológica "altera comportamentos"e transforma a dinâmica cultural, afetando tanto indivíduos quanto grupos sociais.

O impacto dessa transformação vai além da esfera individual, alcançando a política, a economia e a cultura. A sociedade em rede desafia normas e instituições estabelecidas, ao mesmo tempo que cria oportunidades para inovação, colaboração e inclusão. No entanto, esses avanços trazem também desafios relacionados à privacidade, segurança e desigualdade no acesso às tecnologias.

Em síntese, a sociedade em rede representa um novo paradigma no qual a conectividade e a tecnologia moldam nossas interações e nossas vidas cotidianas. Compreender esse cenário é essencial para navegar de maneira eficaz na era da informação, aproveitando suas oportunidades enquanto enfrentamos seus desafios.

3.1.3 Conectividade

Assumindo que estamos realmente vivendo em uma sociedade em rede, sustentada principalmente por novas formas de interconexões para comunicação e interação, se torna de fundamental importância conhecer os meios utilizados para que as conexões ocorram. Em um aspecto social, as conexões ocorrem pela necessidade humana de conexão e são realizadas por diversos meios e formas o que veremos a seguir.

Voltando um pouco no tempo, por volta de 1736, o matemático e físico Leonhard Euler iniciou seus estudos em grafos discutindo um enigma, hoje conhecido como "O Problema das Pontes de *Königsberg*", como mostra a Figura 1, que ele resolveu e, então, determinou um método geral para problemas do mesmo tipo (COSTA, 2011). O entendimento do que se tornou a Teoria dos Grafos serve de base para o entendimento das redes.

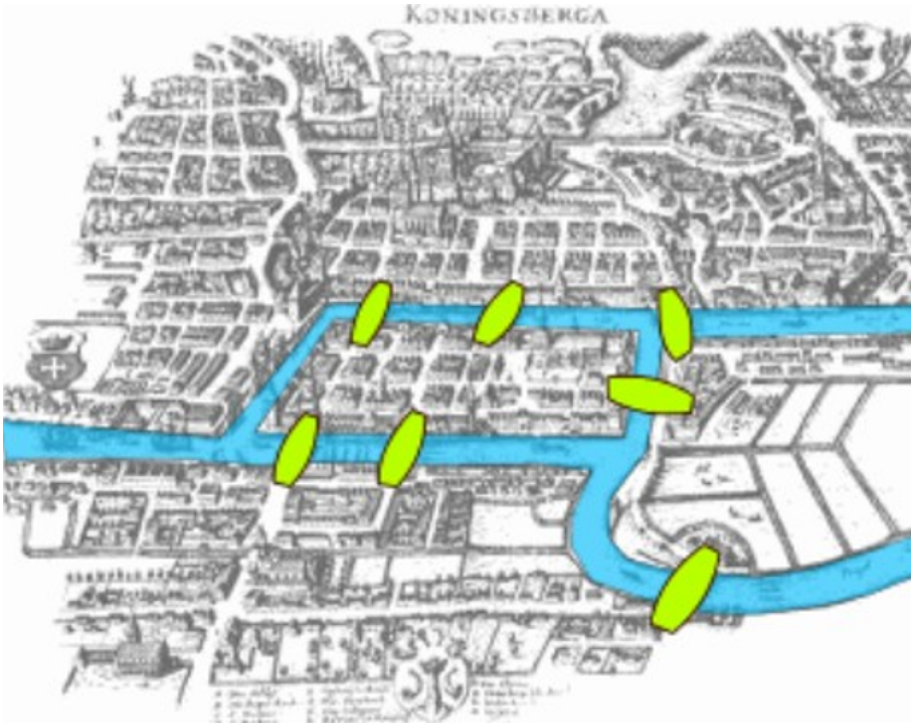


Figura 1 – Pontes de Konigsberg (DALLAQUA, 2016)

O problema resolvido por Euler era originário de uma lenda popular, que discutia a possibilidade de se atravessar todas as pontes, de um complexo de sete pontes, que uniam duas grandes ilhas na cidade de Konigsberg, atualmente Kaliningrado na Rússia, sem repetir nenhuma. Euler conseguiu provar que não era possível resolver a questão cumprindo todas as regras. Para resolver o problema, os caminhos foram transformados em linhas (arestas) e suas intersecções em pontos, conforme mostra a Figura 2.

Podemos dizer que a Teoria de Grafos (1736) está na origem da Teoria de Redes Complexas (1999), que se difere uma da outra principalmente da segunda ser dinâmica e relacionada com a modelagem de redes reais. Nesse sentido o grau de uma rede é medido pelo número de ligações entre dois pontos.

Após a explanação vemos que a capacidade de conexão/ligação vai ditar a capilaridade da rede, logo, quanto maior a conectividade, maior a possibilidade de novos pontos e consequentemente o aumento da rede, como mostra a Figura 3.

Na sociedade informacional, a comunicação ocorre de maneira ininterrupta e necessita dos mesmos elementos de outrora, quais sejam: O canal de comunicação, o remetente, o

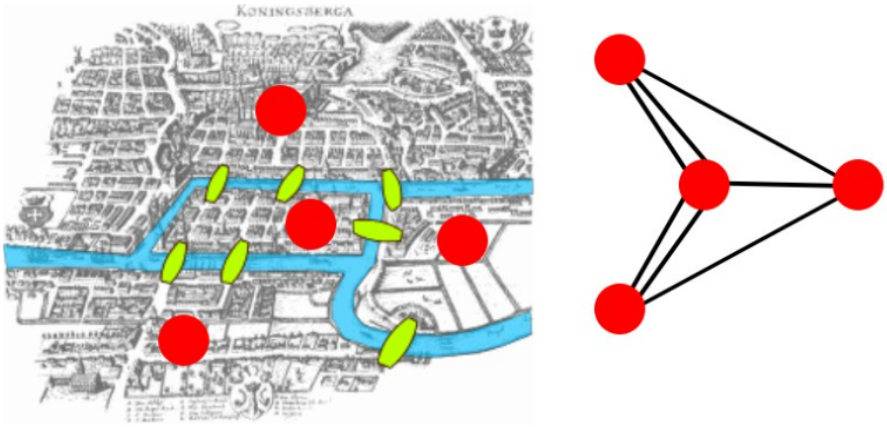


Figura 2 – Representação por Grafo (DALLAQUA, 2016)

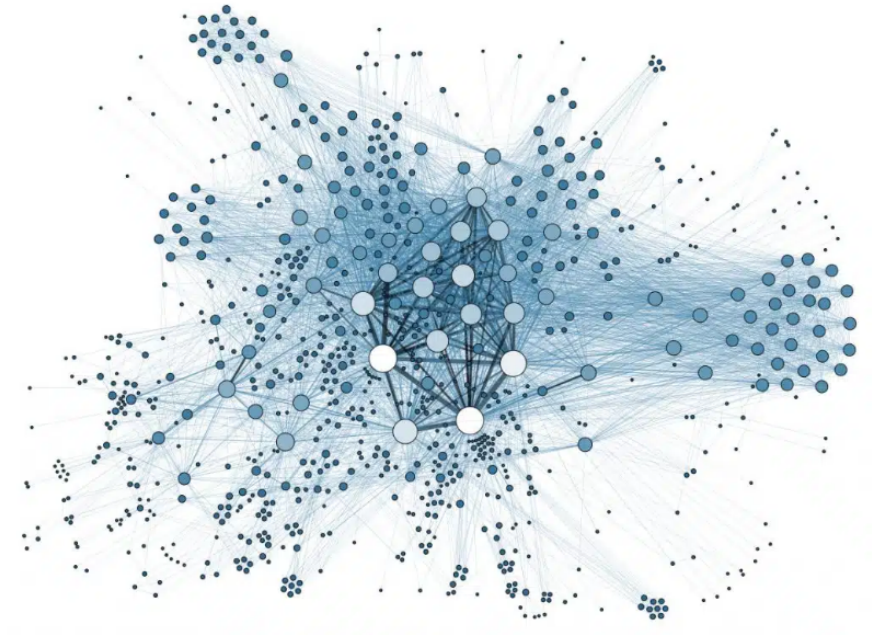


Figura 3 – Representação de Rede (DALLAQUA, 2016)

destinatário, a mensagem, o referente ou contexto e o código (LIMA, 2019), como se pode ver na Figura 4.

Figura 4 – Elementos da Comunicação (LIMA, 2019)

A conexão se relaciona diretamente com o canal de comunicação e na atualidade pode ocorrer das mais variadas formas e meios, podendo ser síncrona ou assíncrona. Para isso ocorrer são usadas redes de fios, sem fios, antenas, satélites, aplicações, entre inúmeros dispositivos e soluções. Tudo que pode possibilitar o aumento do alcance e a conexão entre pessoas ou máquinas.

A conectividade evolui a passos largos, expandindo a rede. Com tudo isso, se possibilitam soluções, novos avanços e como nem tudo são flores, novos problemas são criados.

3.1.4 Democratização Tecnológica

A democratização, em um contexto amplo, refere-se ao processo de tornar algo mais acessível e disponível para um público mais amplo, "tornar popular e acessível" (ECOA, 2019). Isso pode se aplicar a vários domínios, como tecnologia, educação, informação, entre outros.

A democratização tecnológica é um fenômeno intrinsecamente ligado à evolução tecnológica que tem moldado nossa sociedade nas últimas décadas. Essa democratização passa pela inclusão digital e na importância de corrigir a falta de infraestrutura em algumas regiões (CAMILO, 2019).

Como já discutido em capítulos anteriores, a revolução tecnológica trouxe consigo inúmeras transformações que impactaram profundamente como vivemos, trabalhamos e nos relacionamos. Nesse contexto, a democratização tecnológica desempenhou um papel fundamental na ampliação do acesso da sociedade à tecnologia e na criação de novas necessidades e expectativas. A falta de infraestrutura em algumas localidades evidencia a perspectiva de um crescimento ainda maior.

A revolução tecnológica promoveu o surgimento de tecnologias da Indústria 4.0. A inteligência artificial, a automação, a computação em nuvem, o *big data*, a robótica avançada, a manufatura digital, a manufatura aditiva, a integração de sistemas, os sistemas de simulação e a digitalização são os principais exemplos (CNI, 2020). Além disso, não se limita apenas ao desenvolvimento de novos dispositivos e sistemas, mas também à redução dos custos de produção que impacta diretamente a melhora no acesso dessas tecnologias pela sociedade.

Um aspecto importante apresentado por Gerbelli e Melo (2020) é que as tecnologias, notadamente aquelas voltadas para transportes e compras, aumentaram a concorrência e isto resultou na queda de preços, mantendo a inflação sobre controle no Brasil (GERBELLI; MELO, 2020). É defendido por Gerbelli e Melo (2020) que o consumo de novas tecnologias ajuda a manter a inflação baixa.

Embora os níveis de democratização tenham se acentuado nos últimos anos, a margem para crescimento é alta. Em países como o Brasil, que ainda não possuem uma cobertura de rede na totalidade de seu território ou com redes ineficientes em locais que ficam fora ao eixo de desenvolvimento, é possível encontrar regiões desprovidas ou com limitações

de acesso. Hoje, de acordo com o Instituto Brasileiro de Geografia e Estatística (IBGE), a internet chega a 90% dos domicílios do Brasil, sendo que na área urbana alcança 92,3% e na zona rural chega a 74,7%, como se pode observar na Figura 5 (IBGE, 2021).

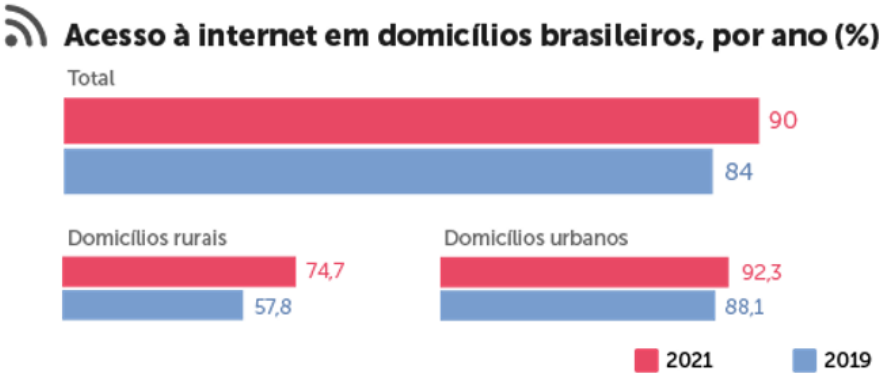


Figura 5 – Acesso à internet em domicílios brasileiros (IBGE, 2021)

Cada nova geração de produtos tecnológicos não apenas introduz avanços, mas também torna os modelos anteriores mais acessíveis, possibilitando que um público mais amplo participe do ciclo de adoção tecnológica. Isso tem um impacto direto na forma como as pessoas vivenciam a tecnologia em suas vidas diárias. Por exemplo, *smartphones*, que eram inicialmente dispositivos caros e exclusivos, estão agora nas mãos de bilhões de pessoas em todo o mundo, servindo como ferramentas essenciais para comunicação, trabalho, entretenimento e educação. No Brasil o equipamento mais usado para o acesso à internet em 2021 foi o *smartphone* (IBGE, 2021), conforme mostra a Figura 6.

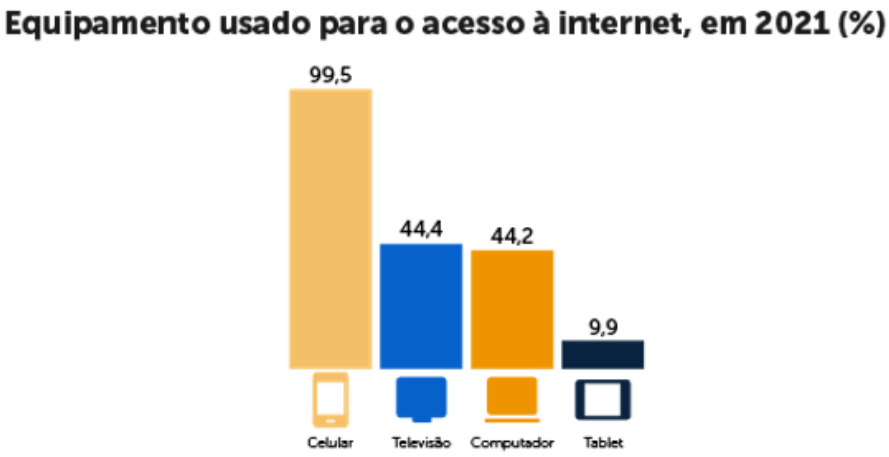


Figura 6 – Equipamento usado para o acesso à internet, em 2021 (IBGE, 2021)

No entanto, a democratização tecnológica não se limita apenas ao acesso físico a dispositivos. Ela também está relacionada à acessibilidade digital e à capacidade das pessoas de compreender e utilizar eficazmente as tecnologias disponíveis. O processo de popularização da tecnologia inclui a promoção da literacia digital, garantindo que todos

tenham a oportunidade de desenvolver habilidades tecnológicas essenciais. Os nativos digitais, designação utilizada pelo educador estadunidense Marc Prensky, aos nascidos após o ano de 1980, já são a base da população atual. Essa geração e as posteriores já tiveram seu desenvolvimento biológico e social em contato direto com a tecnologia, sendo que, a geração anterior, formada pelos imigrantes digitais, tiveram de se adaptar às novas tecnologias (GOULARTE, 2022).

Além disso, à medida que a tecnologia avança, novas necessidades e expectativas surgem na sociedade. Isso é evidente no contexto da IoT, que transformou a maneira como interagimos com o ambiente ao nosso redor. Dispositivos IoT, como termostatos inteligentes, assistentes virtuais e dispositivos vestíveis, agora fazem parte integrante de nossas vidas, atendendo a uma série de necessidades, desde o controle de temperatura em casa até o monitoramento da saúde pessoal.

A democratização tecnológica, portanto, não é apenas um processo de tornar a tecnologia mais acessível, mas também de redefinir constantemente as necessidades e expectativas da sociedade. À medida que as tecnologias se tornam mais presentes em nossas vidas, surgem novas oportunidades e desafios, que devem ser cuidadosamente considerados em nosso progresso em direção a uma sociedade cada vez mais conectada e tecnologicamente avançada. Nesse sentido, a democratização tecnológica é um fenômeno dinâmico e contínuo que continua a moldar nosso presente e futuro.

3.2 A Tecnologia em Tempo de Pandemia

O termo "Pandemia"é tradicionalmente utilizado para descrever a distribuição geográfica de uma doença e, em 2020, o mundo testemunhou a disseminação global do vírus SARS-CoV-2, causador da COVID-19, que afeta predominantemente o sistema respiratório (OPAS, 2019). No entanto, o objetivo deste tópico não é discorrer sobre os detalhes da pandemia em si, mas sim explorar o papel crucial desempenhado pela tecnologia em um período tão desafiador.

A pandemia de 2020, provavelmente originada na China (MATZA; YONG, 2023), espalhou-se rapidamente pelo mundo, revelando uma das principais características da sociedade em rede: a globalização. Embora este trabalho esteja focado nas tecnologias digitais, é importante notar que diversos outros setores e serviços também evoluíram, como os meios de transporte, que reduziram o tempo de deslocamento de dias para horas, conectando pessoas em diferentes continentes.

Desde a descoberta do vírus até a implementação das primeiras medidas de controle, muitas pessoas foram infectadas. Uma característica notável do SARS-CoV-2 é sua variação na manifestação de sintomas, incluindo casos assintomáticos, o que contribuiu para sua rápida disseminação e a classificação como pandemia. Segundo Sena (2023), os pacientes assintomáticos são agentes ativos na transmissão da doença, sendo disseminadores

invisíveis do vírus (SENA, 2023).

Entre as estratégias adotadas pelos governos para conter o contágio tivemos o distanciamento social como a principal, na tentativa de não colapsar a saúde. No Brasil, tal medida não foi suficiente (ECKER, 2021). O direito de ir e vir faz parte do conjunto de garantias fundamentais da constituição brasileira (BRASIL, 1988) e é conferido a todo cidadão de países signatários da Declaração Universal dos Direitos Humanos (DUDH) (ONU, 1948). Cercear o cidadão do direito de locomoção não foi uma medida bem recebida, mas até onde se sabia, necessária.

Nesse período, a tecnologia desempenhou um papel fundamental. Ela não apenas apoiou a ciência na busca por uma cura, mas também ajudou a sociedade a enfrentar as restrições impostas. Milhões de dados foram processados e inúmeras pesquisas, ensaios e testes foram conduzidos por laboratórios, universidades e governos. A ciência e a tecnologia foram testadas como nunca, com um objetivo maior em mente: superar a pandemia.

E uma frente, a tecnologia se aliou à ciência, acelerando o desenvolvimento de tratamentos e vacinas, e por outra, ela desempenhou um papel essencial na manutenção das atividades sociais e econômicas. A educação à distância se tornou a principal forma de ensino em todos os níveis e o trabalho remoto passou a ser explorado para manter empresas em funcionamento. O comércio eletrônico também viu um crescimento significativo, à medida que as pessoas buscavam alternativas para adquirir produtos sem sair de casa. Segundo Nitahara (2021):

> O coordenador do CGI.br, Márcio Migon, explica que a internet e os dispositivos móveis passaram a desempenhar papel central durante a pandemia, possibilitando a continuidade de atividades empresariais com o *home office*, do comércio com as vendas online, prestação de serviços públicos, atividades educacionais com o ensino remoto e de saúde com as teleconsultas. Porém, ele destaca que as desigualdades sociais foram agravadas pelas diferenças no acesso à tecnologia (NITAHARA, 2021).

A pandemia de 2020 serviu como um catalisador, acelerando a integração da tecnologia em todos os aspectos de nossas vidas. Ela demonstrou como a tecnologia pode ser uma aliada crucial em momentos de crise, oferecendo soluções inovadoras para desafios inesperados. A democratização do acesso à tecnologia desempenhou um papel fundamental, permitindo que um número cada vez maior de pessoas se beneficiasse dessas inovações.

Em resumo, a pandemia não apenas acelerou a digitalização da sociedade, mas também evidenciou a importância da tecnologia como uma ferramenta essencial para enfrentar desafios globais. Ela nos mostrou como a conectividade e a inovação tecnológica podem ser usadas para adaptar-nos a situações adversas e, ao mesmo tempo, manter nossa sociedade em funcionamento.

3.2.1 Transformações na Comunicação e Conectividade durante a Pandemia

Com o crescimento exponencial do uso da Internet, a infraestrutura digital tornou-se um componente vital da vida cotidiana em todo o mundo. As empresas de telecomunicações, provedores de acesso e de conteúdo, constantemente se adaptam para acomodar a demanda sempre crescente pelo uso da rede e seus recursos. Durante o auge da pandemia, a Internet se transformou em uma ponte vital para a continuidade das operações comerciais, a educação, o entretenimento e até mesmo para manter conexões pessoais e nesse sentido as empresas de tecnologia enfrentaram grandes desafios.

Plataformas de Educação a Distância (EAD) tiveram de ser criadas de um dia para o outro e partiram de tecnologias já existentes e foram melhorando durante o processo. Junto a isso, as empresas que se voltaram para o trabalho remoto, tiveram de adaptar suas políticas para a nova realidade. Mota e Silva (2023) dizem o seguinte:

> "A pandemia do coronavírus impôs à população mundial um isolamento forçado, e com ele a ressignificação das nossas relações sociais, de trabalho, de ensino-aprendizagem, afetando a nossa saúde física e mental. Fomos obrigados a lançar mão de tecnologias já existentes e outras que se desenvolveram para viver numa realidade que passou a depender muito do mundo virtual. As instituições de ensino, em todos os níveis de aprendizagem, viram-se obrigadas a se adaptar a essa realidade, muitas vezes sem a estrutura e recursos adequados para permitir uma transição tranquila, com os treinamentos e os equipamentos adequados para docentes e estudantes."(MOTA; SILVA, 2023)

É importante ressaltar que a transição para uma sociedade mais digital já ocorria e essa *abruptalidade* só serviu para impulsionar um processo que já existia, claro que não com a isenção dos desafios pertinentes a complexidade do momento. Nesta fase, o ensino remoto se deu de maneira emergencial, sem recurso e equipes preparadas para a oferta de conteúdos e atividades pedagógicas, diferente ao que já existia (HODGES et al., 2020). Muitas residências, escolas e empresas que antes dependiam apenas de conexões esporádicas ou limitadas à rede móvel tiveram de buscar soluções de conectividade mais robustas. Esse aumento na demanda expôs a necessidade urgente de infraestrutura digital equitativa, não apenas nas áreas urbanas, mas também nas regiões rurais e remotas.

Ficou evidente nesse momento as desigualdades tecnológicas vivenciadas pela sociedade. O poder público tomou medidas que não foram tão imediatas quanto a iniciativa privada. O ensino é um exemplo onde verificamos que a iniciativa privada, com o ensino particular, conseguiu por um grande momento estar à frente no que tange a adaptabilidade de sua prática educacional em relação ao ensino particular. Ferreira e Calixto (2021) colaboram com essa opinião com o seguinte:

> As escolas privadas, por possuírem recursos financeiros melhores, conseguiram se adaptar ao ensino remoto e fornecerem as condições necessárias para os alunos estarem presentes nas aulas onlines, utilizando

> recursos digitais combinados com vídeos gravados e ao vivo, tarefas integrativas e tutores, além disso, realizaram uma rápida organização, planejamento e formação dos professores e alunos (FERREIRA; CALIXTO, 2021).

A transformação digital não se restringiu apenas à conectividade. As tecnologias digitais que envolvem educação à distância e trabalho remoto já estavam em crescimento antes da pandemia, mas essa tendência foi amplificada durante a pandemia (AELA, 2021). O modelo tradicional de sala de aula ou de escritório sofreu uma revolução e muitos estão encontrando eficiência e flexibilidade no aprendizado e no trabalho remotos. Como resultado, mesmo com o fim da pandemia, muitas organizações e instituições estão adotando esses modelos de forma permanente, de forma híbrida ou plena. As mudanças vieram para ficar, estudo apresentado no artigo da AELA (2021) da Mackinsey reporta que as empresas acreditam nisso (AELA, 2021).

No entanto, é importante reconhecer que as transformações na comunicação e conectividade durante a pandemia também levantaram questões sobre a exclusão digital, a privacidade *online* e a segurança cibernética. À medida que mais aspectos de nossas vidas migram para o espaço digital, torna-se essencial abordar essas preocupações para garantir que todos tenham acesso igualitário aos benefícios da tecnologia.

À medida que nos adaptamos a essa nova realidade digital, é crucial continuar monitorando e regulamentando a evolução das tecnologias de comunicação e conectividade para garantir que elas sejam usadas para melhorar a qualidade de vida e a inclusão, sem comprometer a segurança e a privacidade dos indivíduos. A pandemia pode ter sido o catalisador, mas as transformações digitais vieram para ficar, moldando o futuro da comunicação e conectividade em todo o mundo.

3.2.2 Educação e Trabalho Remoto

Já mencionamos que o trabalho remoto e a educação à distância estavam em pleno desenvolvimento antes da pandemia e, devido às restrições de deslocamento e aglomerações impostas pelos governos em resposta à crise da COVID-19, tiveram um impulsionamento significativo. Muitos setores da sociedade não estavam preparados para essa rápida transição digital e, mesmo as grandes empresas de tecnologia, precisaram adaptar e desenvolver ferramentas para atender à crescente demanda. O cenário da pandemia forçou uma reestruturação profunda nos planos de negócios das organizações, que tiveram que se adaptar rapidamente para sobreviver.

Antes da pandemia, a educação à distância estava predominantemente concentrada em cursos superiores e os Ambiente Virtual de Aprendizagem (AVA) eram desenvolvidos com foco nesse público e em conceitos de usabilidade. No entanto, com a imposição das restrições e do isolamento social, a educação à distância teve de se adaptar para atender a todas as faixas etárias e níveis de ensino, desde o fundamental até o superior. Isso

representou um desafio significativo, uma vez que a infraestrutura de internet, embora amplamente disponível, não estava igualmente democratizada, o que prejudicou o ensino em regiões com baixa infraestrutura, especialmente em áreas periféricas e entre estudantes de baixa renda. Tal situação causou inclusive grande número de evasão escolar, principalmente entre estudantes cujo principal motivação foi a dificuldade do acesso remoto às aulas (FERREIRA; CALIXTO, 2021).

Durante esse período, várias ferramentas de ensino à distância foram testadas e utilizadas, incluindo plataformas como o *Slack, Skype, Microsoft Teams, Google Classroom e Zoom*, além das ferramentas adotadas por escolas particulares e sistema de ensino como o Positivo. As redes sociais também desempenharam um papel importante na educação à distância. Embora as ferramentas de EAD já estivessem disponíveis, a necessidade de impulsionamento as levou a um novo patamar de uso e desenvolvimento. Muitas dessas ferramentas já eram utilizadas por empresas para colaboração remota (AELA, 2021).

Paralelamente, as empresas também passaram por uma reestruturação para enfrentar os desafios impostos pela pandemia. Escritórios virtuais foram criados, permitindo que muitos colaboradores trabalhassem remotamente a partir de suas casas, utilizando seus próprios recursos ou recebendo algum tipo de apoio da empresa. Algumas empresas optaram por manter essa abordagem mesmo após o término da pandemia.

Avaliar os benefícios dessa rápida adaptação durante o período pandêmico é relativamente simples, pois não havia outra opção viável. A alternativa era não ter ensino formal e fechar empresas. No entanto, medir os impactos a longo prazo dessas transformações forçadas no período pós-pandemia exigirá mais tempo e análise. Uma coisa é certa: a educação e como conduzimos nossos negócios foram profundamente alteradas por essa experiência.

O trabalho proposto tem como motivação principal lançar luz sobre a questão crítica da segurança digital em um contexto em que empresas continuam a adotar o trabalho remoto e indivíduos se tornam cada vez mais interconectados. Uma preocupação central abordada será a crescente integração dos dispositivos IoT nas redes, muitas vezes sem a devida atenção à cibersegurança. Esse cenário levanta questões urgentes sobre como proteger eficazmente os dados e sistemas em um ambiente digital em constante evolução, onde as ameaças cibernéticas podem se manifestar de maneiras complexas e desafiadoras.

3.3 Redes de Computadores

O contexto atual das redes de computadores está profundamente ligado ao desenvolvimento e à integração de novas tecnologias, como a Internet das Coisas (IoT), que exigem a construção de infraestruturas robustas e seguras. As redes de computadores, desde seus primeiros modelos baseados na Teoria de Grafos de Euler (1736) até as redes complexas mais recentes, como as descritas por Barabási e Albert (1999), representam uma interco-

nexão dinâmica e em constante evolução de sistemas computacionais e elementos de rede. Como Tanenbaum (2021) destaca, "as redes de computadores não são apenas conexões físicas, mas sim uma estrutura de interligação entre dispositivos e sistemas que permite a troca de dados essenciais para o funcionamento das sociedades modernas"(TANENBAUM; FEAMSTER; WETHERALL, 2021).

Essas redes são fundamentais para a comunicação de dados e para o funcionamento de sistemas que suportam nossas atividades cotidianas. A topologia de rede, as camadas de comunicação e os protocolos que regem essas conexões formam a base sobre a qual as redes de computadores se expandem e evoluem. A capacidade dessas redes de crescer e se adaptar é uma característica central, e à medida que novas tecnologias emergem, como o 5G e os dispositivos IoT, as redes se tornam mais complexas e multifacetadas, possibilitando novos tipos de interação e novos usos. "O valor de uma rede cresce proporcionalmente ao quadrado do número de seus usuários"(Gilder, 1993) (**??**), o que exemplifica a importância de uma rede de comunicação bem estruturada e em constante expansão.

Analogamente às estradas que interconectam diferentes locais, as redes de computadores formam os meios pelos quais os dados (nosso "veículo"no caso) trafegam. A estrutura dessas redes, que pode ser feita por cabos ou sem fio, é crucial para garantir a eficiência e a redundância na transmissão de dados. Além disso, o crescimento e a qualidade das redes impactam diretamente a capacidade de conexão entre indivíduos e dispositivos, o que torna a infraestrutura de comunicação cada vez mais relevante.

Dentro desse contexto, surgem questões de segurança digital, especialmente quando se considera o crescente uso de dispositivos IoT, que são cada vez mais integrados às redes. Assim como as leis de trânsito priorizam a proteção do pedestre, nas redes de computadores, devemos focar na proteção dos dispositivos mais vulneráveis, como os dispositivos IoT. Isso porque, ao contrário de dispositivos como computadores e servidores, os dispositivos IoT, por sua natureza portável e frequentemente limitados em termos de capacidade de processamento e segurança, estão mais suscetíveis a ataques cibernéticos. Como aponta Casado et al. (2007), "em um ambiente de IoT, a segurança não pode ser tratada de forma isolada; é preciso integrar a proteção aos dispositivos em todos os níveis da rede"(CASADO et al., 2007. https://doi.org/10.1145/1282427.1282382).

Essa vulnerabilidade é exacerbada pelo aumento exponencial de dispositivos conectados às redes, o que exige novas abordagens para o gerenciamento e a segurança dessas redes. Abordagens inovadoras, como o Ethane, que propõe a separação entre os planos de controle e de dados, e o NOX, que atua como um sistema operacional para redes, estão sendo estudadas e implementadas para garantir um controle mais seguro e eficiente sobre o tráfego de dados, especialmente em ambientes IoT. Gude et al. (2008) explicam que "a segurança de redes complexas exige a implementação de camadas de controle, que proporcionam maior visibilidade e maior controle sobre as políticas de tráfego"(GUDE et al., 2008. https://doi.org/10.1145/1384609.1384625).

O contexto das redes de computadores, que abrange a evolução das topologias e a integração de novos dispositivos, também nos leva a refletir sobre as questões de segurança digital, especialmente no que diz respeito aos dispositivos IoT. Com o crescimento da rede e a crescente capilaridade das conexões, é imperativo considerar as novas vulnerabilidades e os desafios de segurança que surgem. Como afirmado por Tanenbaum (2021), "a segurança deve ser parte integrante da infraestrutura de rede, não algo adicionado após a implementação"(TANENBAUM; FEAMSTER; WETHERALL, 2021). A partir dessa base, o trabalho se propõe a explorar as vulnerabilidades específicas das redes de computadores, destacando a importância de medidas robustas de proteção cibernética para garantir a integridade e a confidencialidade dos dados em um mundo cada vez mais conectado.

Em resumo, assim como a legislação de trânsito prioriza a proteção do pedestre nas relações de trânsito, em se tratando das redes de computadores, é essencial focar na segurança dos dispositivos menos protegidos, como os dispositivos IoT. Estes, devido à sua natureza portável e muitas vezes com recursos limitados, são particularmente vulneráveis a ataques cibernéticos, exigindo cuidados especiais. Nos próximos tópicos, exploraremos sobre as Redes Definidas por Software (SDN), formas de proteção dessas redes, as vulnerabilidades e os desafios de segurança enfrentados por esses dispositivos, destacando a importância de medidas robustas de proteção cibernética para garantir a integridade e a confidencialidade dos dados em um mundo cada vez mais conectado.

3.3.1 Redes Definidas por Software - SDN

Quando na seção anterior (3.3) apresentamos a rede como uma representação física e em analogia a comparamos com o sistema rodoviário, especificamente a malha viária que interliga as cidades. Uma SDN seria nesse exemplo o controle dessa malha, a mudança de sentido de via quando necessário, os semáforos e a sinalização.

SDN é uma filosofia que usa controladores para direcionar o tráfego na rede e se comunicar com a infraestrutura de hardware subjacente (LEVINE; YOUNG, 2011). Elas criam uma interface lógica bem definida para o controle da rede, tendo esta camada a função de abstrair a rede e fornecer diversos serviços que permitam reconfigurabilidade em tempo de execução (OLIVEIRA, 2019).

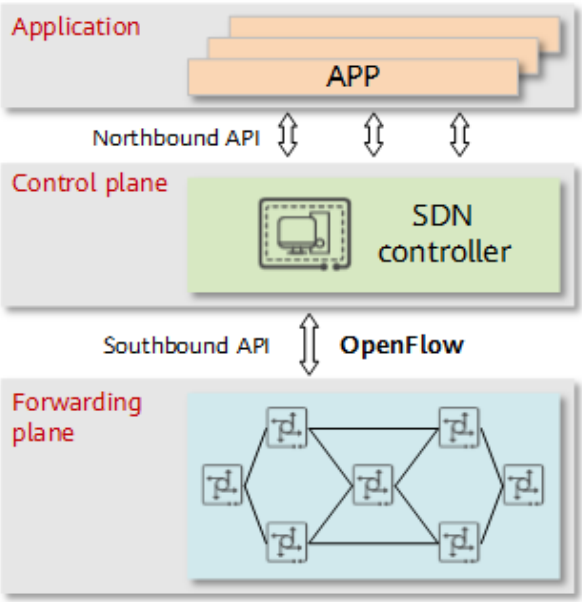
A comparação com o sistema rodoviário é pertinente, mas a amplitude do controle da rede é muito maior. Não é possível, por exemplo, em um curto espaço de tempo mudar o sentido e circulação de veículos sem provocar grandes transtornos. Na rede definida por software isso pode ocorrer de forma muito mais rápida.

A rede tradicional é engessada no sentido de necessitar de um maior número de hardware ou equipamentos específicos para suprir as necessidades de conexão, incluindo ações humanas. Para cada novo desmembramento uma nova gama de equipamentos é necessária várias configurações manuais. De maneira mais formal:

> "...podemos dizer que uma Rede Definida por Software (SDN) é caracterizada pela existência de um sistema de controle (*software*) que pode controlar o mecanismo de encaminhamento dos elementos de comutação da rede por uma interface de programação bem definida. De forma mais específica, os elementos de comutação exportam uma interface de programação que permite ao software inspecionar, definir e alterar entradas da tabela de roteamento do comutador, como ocorre, por exemplo, com comutadores *OpenFlow*". (GUEDES et al., 2012)

SDN viabiliza a separação do Plano de Controle do Plano de Dados e por sua vez o *OpenFlow* introduz o conceito de tabela de fluxo, com base na qual comutadores encaminham *frame* de dados (YANGYANG, 2021). O *OpenFlow* funcionaria como uma interface de comunicação sul (**SBI!** (**SBI!**)), como se pode ver na Figura 7.

Figura 7 – *OpenFlow* na arquitetura SDN



Fonte: (YANGYANG, 2021)

De maneira bastante simples, para o perfeito entendimento do leitor, apresentamos a Figura 8. Uma topologia simples, similar àquela provida pelo MAIOS.

3.3.2 Aplicações de Proteção de Rede

Nesta seção serão exploradas algumas das principais aplicações de proteção de rede, com foco no *pfSense*[1] (RIBEIRO, 2022). Em um mundo cada vez mais digitalizado, onde os dados se tornaram um ativo para organizações, a segurança da rede é fundamental. A proteção dos dados, seja no nível físico de hardware ou no nível lógico de software, é uma prioridade para pessoas, organizações e governos em todos os setores que presam por seus dados.

[1] pfSense é um *open source*, licenciado sob BSD *License*, baseado no sistema operacional FreeBSD e adaptado para assumir o papel de um firewall e roteador.

Figura 8 – Topologia simples

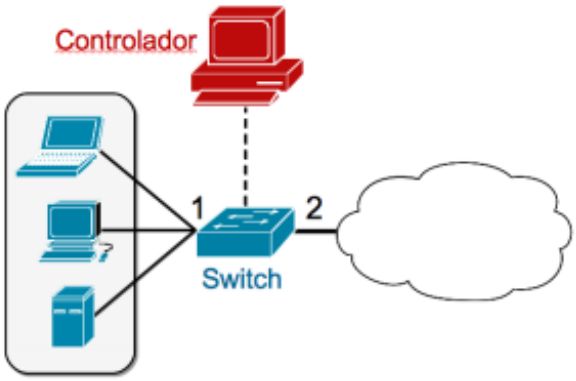


Figura 7. Topologia simples

Fonte: (GUEDES et al., 2012)

Nas seções anteriores, foi discutida a evolução da sociedade em direção a uma era de informação. No entanto, com a crescente importância das informações, surge a necessidade de garantir a segurança e a integridade dessas informações. Ao projetar uma rede, seja em um ambiente privado ou governamental, diversos fatores devem ser considerados, desde questões de redundância, disponibilidade e integridade até a segurança física e lógica dos sistemas.

Na concepção de uma rede interna, em meio privado ou governamental, muitos fatores devem ser levados em conta no planejamento. Postulados da proteção de dados devem ser observados com as questões de redundância, disponibilidade e integridade. No que tange aos aspectos físicos de proteção da rede, empresas devem se atentar onde serão armazenados os servidores de dados, se estão seguros, com acesso restrito, longe de intempéries e em local climatizado.

Aplicações de proteção de rede são um conjunto diversificado de ferramentas e tecnologias projetadas para fortalecer a segurança das redes, garantindo que os dados sejam transmitidos e recebidos com integridade, confidencialidade e disponibilidade. Elas atuam como guardiãs vigilantes, monitorando o tráfego de rede, identificando atividades suspeitas e implementando medidas proativas para impedir violações de segurança.

Existem inúmeras aplicações projetadas para proteger redes em um cenário digital cada vez mais complexo. Estas ferramentas não apenas protegem contra ameaças, mas também podem trabalhar em conjunto, ampliando sua eficácia com métodos personalizados. Algumas das principais aplicações incluem:

- *Firewalls*: Responsáveis por monitorar e controlar o tráfego entre uma rede privada e a internet, estabelecendo uma barreira fundamental contra acessos não autorizados e ataques cibernéticos;
- Servidores de E-mail com Filtro de SPAM: Estes servidores filtram mensagens in-

desejadas, protegendo contra *phishing* e outros tipos de ataques por e-mail;

- Antivírus e *Antimalware*: Detectam, bloqueiam e removem programas maliciosos que possam infectar sistemas, garantindo que dispositivos estejam livres de ameaças;
- Segmentação: Divide a rede em segmentos menores, isolando partes dela, sendo que se um segmento for comprometido, a infecção não se espalha para toda a rede;
- Controle de Acesso: Gerencia quem pode acessar quais recursos na rede, minimizando vulnerabilidades e impedindo acessos não autorizados;
- Virtualização: Cria ambientes virtuais isolados para testes e desenvolvimento, protegendo a infraestrutura principal de possíveis danos;
- *Virtual Private Network* (VPN): Cria uma conexão segura entre dispositivos em redes diferentes, protegendo a comunicação contra interceptação; e
- *Network Intrusion Detection System* (NIDS): Sistema de Rede de Detecção de Intrusão, componente fundamental no MAIOS.

Essas ferramentas, quando configuradas corretamente e orquestradas, fortalecem significativamente a segurança de uma rede. Além disso, elas podem ser personalizadas para atender às necessidades específicas de uma organização, oferecendo uma defesa robusta contra um cenário em constante mudança de ameaças digitais.

No mercado atual, existem várias empresas e soluções especializadas em segurança de informações, oferecendo software dedicado para monitoramento e proteção contra intrusões, além de profissionais especializados na área. Entre as muitas opções disponíveis, destacamos o *pfSense*, com funcionalidades comparáveis às de sistemas comerciais de alto custo (RIBEIRO, 2022), substituindo com sucesso - na maioria das necessidades - as versões pagas.

A escolha do *pfSense* se justifica pela sua relevância na abordagem de proteção que será detalhado nos próximos capítulos. Como um *firewall*, tem a função de estabelecer uma barreira de proteção a rede. O *pfSense* possui funcionalidades avançadas no que tange a proteção de rede e pode incluir diversos pacotes de software livre de terceiros, que estendem ainda mais qualidades. Segundo Ribeiro (2022), as aplicações mais comuns seriam:

- Roteador;
- Servidor, que pode variar entre *Dynamic Host Configuration Protocol* (DHCP) e *Domain Name System* (DNS);
- Pontos de Acesso WiFi;
- Servidor *Proxy* Squid transparente;
- *Network Address Translation* (NAT); e
- Servidor VPN.

Ribeiro (2022) completa que tudo isso é disponível no mesmo dispositivo, que tem inúmeras funções quando somado ao *pfSense* (RIBEIRO, 2022). Em nosso modelo conceitual, será utilizado, principalmente, para a função de roteamento.

3.3.3 Cibersegurança

Na era da informação, na qual dados são o novo ouro, a cibersegurança emerge como uma pedra angular da sociedade digital. Mais do que uma questão técnica, a cibersegurança transcende às barreiras dos Departamentos de Tecnologia da Informação (TI) e Segurança Digital. É uma questão estratégica que permeia os alicerces dos negócios modernos. Aspectos legais, regulatórios, fraudes e de gestão de riscos também estão envolvidos.

Em definição, a cibersegurança refere-se à proteção dos sistemas, redes e dados contra ameaças digitais. Todavia, vai muito, além disso. É uma sinfonia complexa entre tecnologia, estratégia, processos e conscientização (pessoas). Em um mundo onde a evolução tecnológica é constante, novas oportunidades para cibercriminosos surgem, criando um ciclo ininterrupto de inovação e adaptação. Assim, a cibersegurança deve evoluir em paralelo, defendendo contra ameaças cada vez mais sofisticadas.

Cibersegurança tem tudo a ver com a continuidade dos negócios, não servindo apenas para mediadas preventivas. Preparar-se para possíveis ataques, desastres ou danos cibernéticos de modo a evitar impactos financeiros e proteger a reputação da empresa é fundamental dentro do contexto atual de sociedade que vivemos. As empresas precisam ter a capacidade de repostas eficazes diante de quaisquer tipos de incidentes cibernéticos.

Contudo, a cibersegurança não é uma batalha travada apenas com *firewalls* e algoritmos avançados. Ela está entrelaçada com a estratégia de negócios, incorporando regulamentações rigorosas e promovendo a conscientização dos colaboradores. As regras de negócios bem definidas atuam como guardiãs, delineando políticas claras para proteger dados. Simultaneamente, a conscientização de colaboradores se torna a primeira linha de defesa, transformando cada colaborador em um 'escudo' humano contra ameaças cibernéticas.

Nesse cenário, a proliferação de dispositivos IoT adiciona uma camada de complexidade. À medida que nossas casas, escritórios e até cidades inteiras se tornam mais conectadas, garantir a segurança dos dispositivos IoT torna-se crucial. Eles não apenas expandem nossa eficiência e conveniência, mas também aumentam as potenciais vulnerabilidades, exigindo uma atenção especial.

Ao explorar a evolução tecnológica, as redes de computadores e as transformações na comunicação se percebe que a cibersegurança é um fio condutor essencial que costura esses avanços. É a garantia de que nossas comunicações permaneçam seguras, nossos dados permaneçam íntegros e nossa sociedade digital continue a prosperar.

Em última análise, a cibersegurança não é apenas um protocolo; é um estado de espírito. É a compreensão de que, em uma era onde a informação é o principal ativo, proteger essa informação é proteger o cerne da nossa sociedade digital. Por meio de uma abordagem holística, incorporando estratégia, regulamentação e conscientização, estamos construindo um futuro digital mais seguro, um byte de cada vez.

3.4 Automação

Esta seção abarca o universo da automação, um domínio tecnológico que tem desencadeado uma transformação profunda em diversos setores da sociedade moderna. A automação, catalisada pelo avanço contínuo em campos como inteligência artificial, ciência de dados e IoT, não apenas revoluciona os processos industriais, mas também permeia nossas residências e ambientes de trabalho, redefinindo padrões e expectativas.

3.4.1 Automação Industrial

Esta seção discute Indústria 4.0 ou Quarta Revolução Industrial. Diferentemente das revoluções industriais anteriores, experimenta-se um impacto ainda maior devido à nossa sociedade cada vez mais conectada. Esta revolução é impulsionada pela interconectividade sem precedentes entre dispositivos e sistemas, transformando fundamentalmente a maneira como vivemos e trabalhamos.

Ao longo da história, a indústria tem utilizado a tecnologia para estabelecer padrões de produção mais eficientes. Há muito tempo, sistemas computadorizados, sensores, atuadores e outros dispositivos são empregados para automatizar tarefas e operações, que antes eram realizadas manualmente. Contudo, na fase atual da evolução tecnológica, esses dispositivos adquiriram uma nova dimensão, orientada à conectividade.

Na indústria moderna, esses dispositivos não apenas auxiliam na produção, mas também fornecem dados valiosos que auxiliam na tomada de decisões estratégicas. Informações cruciais sobre equipamentos, produção, eficiência e operacionalidade agora podem ser acessadas em tempo real, transcendendo limites físicos. Essa conectividade sem precedentes não só otimiza processos industriais, mas também permite uma análise de dados em larga escala, proporcionando *insights* preciosos para melhorar a eficiência, economizar recursos e impulsionar a inovação.

Nesta era de automação avançada e conectividade onipresente, a indústria está testemunhando uma transformação radical. Tecnologias como a IoT e a IA estão redefinindo os limites do que é possível na produção industrial. Estamos no epicentro de uma revolução que não apenas melhora a eficiência e a qualidade, mas também catalisa a criação de novos modelos de negócios e impulsiona a competitividade global.

O fato de referenciarmos a automação industrial se deve ao seu desenvolvimento no que tange a adoção de IoT, o que possibilita utilizar em ambientes fora de fábricas. A interconexão entre a indústria e as residências ocorre no compartilhamento de tecnologias e conceitos. Por exemplo, os sensores avançados usados na indústria para monitorar equipamentos e processos também são empregados em residências para detectar movimentos, temperatura e condições ambientais. Além disso, os sistemas de automação industrial, que otimizam operações e coletam dados em tempo real, servem de modelo para sistemas

de automação residencial, permitindo o controle remoto de dispositivos e o monitoramento em tempo real das atividades domésticas.

A automação industrial desempenha um papel crucial na evolução tecnológica, estendendo suas inovações para além das fábricas e alcançando nossas casas. Podemos comparar esse fenômeno ao desenvolvimento de tecnologias em carros de Fórmula 1 que, eventualmente, são incorporadas aos carros comuns. Da mesma forma, os dispositivos de automação industrial estão migrando para nossos lares, transformando a maneira como vivemos e interagimos com nossos espaços.

3.4.2 Automação Residencial

Tendo a revolução industrial como precursora, que transformou o cenário de fábricas e indústrias, a mesma inovação tecnológica começou a bater à porta de nossas casas. A automação residencial, como uma extensão direta da automação industrial, não é, para muitos, apenas um luxo moderno, mas uma necessidade crescente em nossas vidas interconectadas.

Esses dispositivos não apenas resolvem problemas, antes desconhecidos por pessoas em geral, mas também apresentam desafios inéditos. Imagine chegar em casa e, com um simples toque no seu *smartphone*, acender as luzes, ajustar a temperatura ambiente e reproduzir sua música favorita. Ou estar em férias e poder monitorar a segurança de sua casa em tempo real, garantindo tranquilidade mesmo a milhares de quilômetros de distância. Isso é apenas um vislumbre do que a automação residencial oferece.

À medida que dispositivos de automação residencial são criados e suas funcionalidades exploradas, testemunha-se um crescimento exponencial. Eles promovem o bem-estar e integram um conjunto de tecnologias voltadas para a gestão e auxílio em atividades diárias. Sua utilização tem por objetivo proporcionar um maior nível de conforto, comodidade e segurança (BOLZANI, 2004).

Um dos pilares da automação residencial é a conectividade total, abordada na seção 3.5. Dispositivos inteligentes agora estão interligados em uma rede digital, permitindo comunicação instantânea e colaboração entre diferentes sistemas. De termostatos, que aprendem preferências de temperatura, a geladeiras, que mantêm inventários automáticos, nossa casa está se tornando verdadeiramente inteligente.

3.4.3 Aplicações na Automação: Desafios na Era da IoT

No universo de tecnologias, as aplicações são a essência da interação entre hardware e funcionalidade, uma relação *sine qua non*, onde uma sem a outra é destituída de significado. As aplicações convergem para facilitar atividades repetitivas, agregando o benefício da execução desprovida de intervenção humana. Sem a interação habilidosa entre o hardware e seu propósito funcional, a automação perderia sua essência.

Uma aplicação eficaz precisa aspirar à exploração máxima das funcionalidades do hardware, utilizando-o de maneira eficiente e precisa. O que se busca automatizar deve operar de acordo com seu propósito final e uma aplicação bem elaborada assegura essa sinergia.

No cenário de IoT, diversas aplicações podem ser imaginadas e criadas para satisfazer as mais variadas áreas. Seja no setor de transportes, interagindo com veículos autônomos, ou na saúde, com dispositivos aferindo dados médicos de usuários. São muitas as aplicações possíveis e a todo momento se melhora a qualidade e eficiência dos dados coletados.

Atualmente, estamos testemunhando a busca por sistemas automatizados com intervenção humana mínima, ampliando os horizontes da comunicação máquina-máquina. Por exemplo, um dispositivo pode receber informações de um segundo e, com base nesses dados, iniciar um processo em um terceiro dispositivo. Este cenário complexo é implementado, onde condicionalidades precisas são votadas à lógica algorítmica.

Ocorre que com as especificidades de cada produto, aliado com o interesse das empresas que os produzem, cada fabricante adota interfaces próprias que em muitos casos não interoperam com outras. Tal problema poderia ser contornado com a adoção de protocolos comuns que permitissem maior interação e não deixaria o usuário refém de fabricantes.

A falta de uma padronização pode ser o momento que vivemos de total dinamicidade, ao chegarmos em uma maior propagação desse tipo de recurso será inevitável. Até lá a preocupação com segurança traz desafios maiores.

É evidente que em um mundo em rede e interconectado, cada vez mais automatizado, as aplicações desempenham um papel fundamental na realização da automação de maneira eficiente e eficaz. No entanto, a falta de padronização entre dispositivos de diferentes fabricantes representa um desafio significativo para a plena realização do potencial da IoT.

3.5 Internet das Coisas (IoT)

O termo IoT foi cunhado a partir da frase *Internet of Things* (Internet das Coisas) usada pelo pesquisador britânico Kevin Ashton. O acrônimo IoT tem sua origem na rede social X, que em seu início tinha limite de caracteres e o usuário abreviava suas palavras para economizar espaço. Mas o que é e o que representa o IoT hoje?

Definir IoT como coisas conectadas na rede é um tanto quanto simplório, mas não distante da realidade. O segredo está ligado a saber o que fazer com essas coisas e tirar proveito do produto gerado. Sacomano et al. (2018) dizem o seguinte:

> "IoT consiste em conectar objetos usados diariamente, como máquinas, veículos, aparelhos eletrodomésticos, à internet, para poderem ser acessados remotamente, por dispositivos móveis, como celulares, *notebooks* e *tablets* ou fixos, como *desktop* ou outros, que tenham conexão com a internet (SACOMANO et al., 2018)."

Graças a indústria já havia muitos sensores operando em fábricas, e a conexão destes sensores trouxe implicaram em IoTs. Sensores de temperatura, de umidade, de gás e CO_2, de porta e janela, de presença, de fumaça e incêndio são só alguns exemplos que agora estão presentes nas residências.

Apesar no tema parecer novo, a ideia de conectar "coisas" já era discutida desde o desenvolvimento do protocolo TCP/IP. Em 1990, por exemplo, John Romkey criou o primeiro equipamento conectado à Internet, uma torradeira que podia ser ligada por meio de uma conexão com a Internet (GODOI; AND, 2018).

O IoT 'puro' é aquele que independe da ação humana e se baseia unicamente na interação máquina a máquina MTC. Evidentemente, existem aqueles que permitem a interação (*input*) humana, com interface para que uma pessoa atuar (IT, 2017).

A ideia de conectar objetos do cotidiano à internet e permitir que eles interajam uns com os outros não é apenas uma evolução tecnológica: é uma transformação fundamental na forma como vivemos e interagimos com o mundo ao nosso redor.

Hoje, a IoT se manifesta em uma variedade de aplicações, desde assistentes pessoais ativados por voz, que controlam nossas casas e fornecem informações instantâneas, até sistemas de saúde que monitoram remotamente sinais vitais e alertam médicos em tempo real. A IoT se tornou um tecido invisível que permeia todas as esferas de nossas vidas.

Na automação residencial, a IoT transformou casas em lares inteligentes, onde luzes, termostatos e sistemas de segurança são controlados por meio de *smartphones*. As geladeiras agora podem fazer pedidos de supermercado automaticamente quando você está ficando sem itens essenciais. Esse nível de automação não é apenas conveniente; é um testemunho da capacidade da IoT de otimizar nossas vidas diárias.

Contudo, apesar de todo esse potencial, a IoT não está sem seus desafios. A segurança é uma preocupação constante. À medida que mais dispositivos estão conectados, mais pontos de vulnerabilidade surgem. Além disso, a questão da padronização e interoperabilidade ainda não está resolvida, criando um cenário onde o potencial total da IoT ainda não foi totalmente explorado.

Atualmente a IoT compreende plataformas orientadas verticalmente e, em sua maioria, fechados. Os desenvolvedores precisam negociar o acesso individualmente e se adaptar à API específica da plataforma e aos modelos de informação, o que dificulta a criação de ecossistemas IoT(BRORING et al., 2017).

Podemos destacar, também, que, devido a algumas aplicações disponíveis em nuvem, com aplicativos para *smartphones* específicos, a interoperabilidade se torna um grande problema, pois as coisas estão efetivamente conectadas à Internet, mas totalmente desconectadas umas das outras(ANIL, 2016. https://doi.org/10.1109/INCITE.2016.7857619).

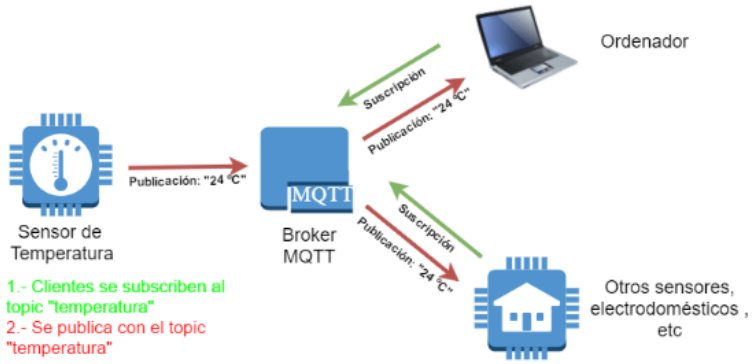
Ao superar os desafios de segurança e interoperabilidade, nossa proposta no trabalho, a IoT tem o potencial de não apenas tornar nossas vidas mais convenientes, mas também mudar nossa forma de interagir com o mundo.

3.5.1 Conexão de IoT

Um dispositivo IoT pode se conectar a redes de muitas formas possíveis, desde que, adaptada para os diferentes cenários, tais como *Wi-Fi*, *Bluetooth*, Banda Larga Móvel (3G/4G/5G), *Long Range Wide Area Network* (LoRaWAN), *Low Power Wide Area Network* (LPWAN), *Near Field Communication* (NFC), Satélite etc. Desde dispositivos residenciais inteligentes até soluções industriais avançadas, a diversidade de opções de conectividade permite que a IoT atenda aos mais variados objetivos.

Um modelo de comunicação entre dispositivos IoT utiliza uma camada de conectividade máquina à máquina MTC, baseado no padrão de projeto *Publisher-Subscriber* (P/S), conforme se pode ver na Figura 9. Mensagens são recebidas e distribuídas por meio de um concentrador (P/S) e a transmissão das mensagens ocorre através do protocolo TCP.

Figura 9 – Funcionamento do MQTT



Fonte:(INDELMAR, 2017)

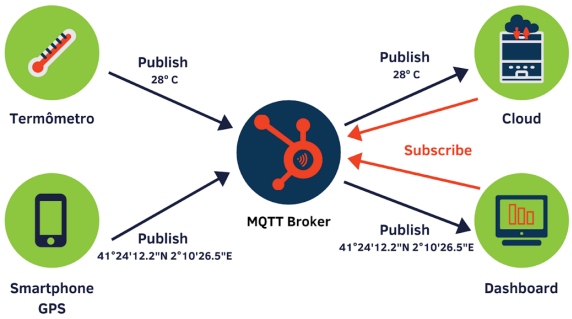
As mensagens seguem uma estrutura em que é definido o tipo de mensagem, um indicador de mensagem duplicada, um indicador para *Quality of Service* (QoS), indicação referente a retenção ou não da mensagem e o tamanho da mensagem que pode ser enviada.

O QoS define a quantidade de mensagens trocadas entre dispositivos, se os servidores devem utilizar os indicadores no máximo uma vez ou pelo menos uma vez e se será necessário reservar recursos para evitar o envio em duplicidade das mensagens ao utilizar o indicador exatamente uma vez.

Um protocolo muito utilizado é o *Message Queuing Telemetry Transport* (MQTT), criado pela *International* Business Machines (IBM), e desde o ano de 2014 está a cargo da OASIS, apresentado na Figura 9. Ele é um protocolo simples e rápido para transmissão de mensagens e se localiza nas camadas superiores do modelo *Open System Interconnection* (OSI), o que significa que necessitam ter uma pilha TCP (INDELMAR, 2017).

A Figura 10 apresenta uma atuação do protocolo MQTT, como um concentrador, responsável pela comunicação da rede IoT, seja entre dispositivos ou uma central *dashboard*.

Figura 10 – Exemplo de comunicação MQTT



Fonte:(AFONSO, 2020)

3.5.2 Segurança em IoT

Cada dispositivo conectado à internet representa uma potencial ameaça, uma porta de entrada para ataques virtuais de criminosos. Para as empresas, essa preocupação é ainda maior, considerando os prejuízos que esses tipos de ataques podem causar às operações. A preocupação também é relevante ao nível pessoal, especialmente porque muitas empresas estão adotando o modelo de trabalho remoto (*home office*). Neste cenário, os funcionários se conectam à empresa por meio de conexões privadas e realizam suas atividades em seus lares.

A situação torna-se mais crítica à medida que mais empresas adotam o modelo de trabalho remoto, conectando-se a redes corporativas por meio de dispositivos pessoais. Cada dispositivo IoT em uma rede representa uma potencial porta de entrada para cibercriminosos. Por essa razão, é crucial implementar medidas de segurança robustas para proteger tanto as empresas quanto os usuários domésticos.

Em um ambiente totalmente conectado, onde dispositivos IoT estão interligados em casas ou empresas, o acesso não autorizado ou a perda do controle sobre esses dispositivos podem gerar grandes prejuízos. Confiar em dispositivos para automatizar várias tarefas é prático, mas a perda de controle pode resultar em danos financeiros e à privacidade. A segurança deve ser uma consideração central desde o projeto inicial desses dispositivos até sua implementação, garantindo que sejam à prova de violações e que os usuários tenham total controle sobre suas operações.

Apesar da facilidade de operação dos dispositivos IoT, onde o usuário final não precisa se preocupar com configurações complexas para a instalação, essa simplicidade pode gerar problemas no que diz respeito à privacidade. Tudo é transparente ao usuário, e informações pessoais passam a ser compartilhadas com os fabricantes. É essencial que os usuários estejam cientes desses aspectos e estejam atentos à proteção de sua privacidade ao utilizar dispositivos IoT.

Em um mundo cada vez mais interconectado, a segurança dos dispositivos IoT não é apenas uma preocupação técnica, mas uma questão que afeta diretamente a privacidade e a integridade das informações pessoais e corporativas. A implementação eficaz de medidas

de segurança desde a fase de design até a utilização cotidiana é crucial para proteger contra ameaças cibernéticas. Ao adotar uma abordagem proativa para a segurança dos dispositivos IoT, podemos aproveitar as conveniências da tecnologia moderna enquanto protegemos nossa privacidade e segurança digital.

Capítulo 4

MAIOS: Proposta de um Switch com porta orientada a IoT

Nesta seção, será detalhado o método de pesquisa adotado para o desenvolvimento do *Switch* orientado a IoT, utilizando *PfSense* e garantindo interoperabilidade por meio do *HomeAssistant*. O método foi estruturado em diferentes etapas para abordar de forma eficaz os desafios identificado.

4.1 Caracterização do Problema

Amparados pela disciplina do processo unificado (UP - *Unified Process*), esta seção será dedicada para descrever em maior granularidade as etapas do desenvolvimento.

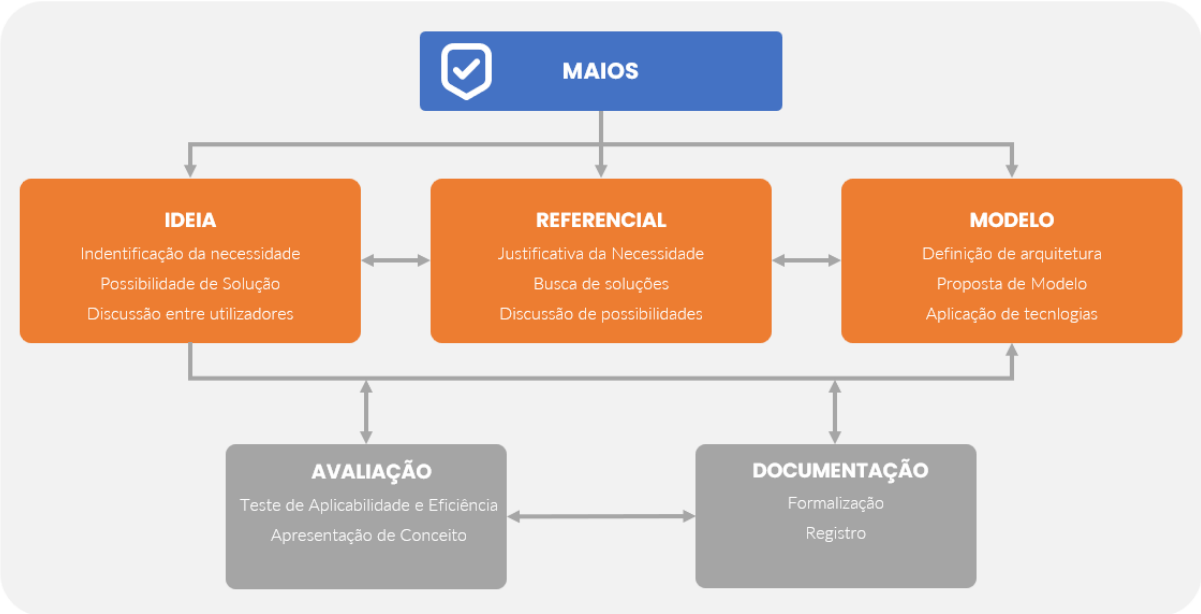
4.1.1 Percepção

Os dispositivos IoT tiveram sua origem em sensores utilizados nas indústrias e migraram para as residências à medida que se tornaram acessíveis e capazes de proporcionar algum conforto, alimentados pela ideia de elevar o bem-estar. No cenário atual, em que as empresas estendem seus escritórios para a residência de seus colaboradores com o *home office*, é vital garantir o mínimo de segurança nesses novos ambientes de trabalho, já que eles precisam estar conectados às empresas. Não obstante a isso, o aumento da rede doméstica com inúmeros dispositivos pode significar um caminho aberto para a utilização de cibercriminosos.

Esse trabalho tem sua concepção idealizada pela solução desse problema, que motivou os objetivos descritos na Seção 1.2 (Objetivos) e a busca de soluções para seus cumprimentos. A pesquisa como um todo seguiu um modelo de trabalho com constante observação dos cenários apresentados e em plena atualização. A Fig. 11 apresenta o método adotado.

Conforme ilustrado na Fig. 11, o trabalho surgiu da identificação de uma necessidade e a possibilidade de solução, que a partir da discussão entre utilizadores de dispositivos

Figura 11 – Método de Pesquisa e Desenvolvimento



Fonte: Próprio autor

IoT e entusiastas de tecnologia propiciou o surgimento da ideia.

De posse da ideia inicial foi possível a busca de um referencial teórico e tecnológico capaz de justificar a real necessidade da busca de soluções para o problema outrora evidenciado. Com base em extensa pesquisa se discutiu as possibilidades, com foco naquelas que permitissem ao usuário comum prover de segurança seus dispositivos.

Dos efeitos às causas foi possível a concepção de um modelo conceitual capaz de ser aplicado ao problema visualizado. Esse modelo partiu de aplicações de tecnologias já existentes, mas com um foco específico e ainda não explorado, que culminou com o MAIOS, um *swith* orientado a IoT.

As etapas que se sucedem são de avaliação e documentação, nas quais é verificado o conceito em funcionamento de forma amostral. Apesar do projeto ser apresentado de forma sequencial, cada etapa se relaciona diretamente com a anterior e posterior, se alimentando uma das outras. Eventualmente, houve revisitas a etapas.

A estruturação do método de pesquisa foi essencial para enfrentar a complexidade da segurança em uma residência conectada à Internet, ponto de interconexão com uma rede de alcance mundial. Em cascata, todos os dispositivos que se conectam ao concentrador/roteador da casa também fazem parte dessa mesma rede e é um ponto de entrada e saída. Temos uma Rede maior de alcance mundial e diversas outras redes menores com potencial de alcance similar, visto que, eventualmente sem nenhuma proteção, o dispositivo alcança e é alcançável pela rede, como mostra a Fig. 12.

Atualmente, não se veem soluções voltadas especificamente para o público doméstico, que possuam usabilidade, transparência e tenha um custo acessível. Nem mesmo um padrão é seguido pelos fabricantes dos dispositivos que se proliferam na rede com cada

Figura 12 – Conexão IoT Casa

Fonte: Próprio autor

vez mais intensidade. São inúmeras marcas e soluções diferentes que adotam plataformas próprias e sem preocupação com a interoperabilidade.

4.1.2 Análise

Considerando que dispositivos IoT possuem como característica a capacidade de interação, seja com o operador ou com outros dispositivos, e que tal fato melhora as potencialidades das ferramentas em prover o almejado bem-estar doméstico para seus utilizadores, é primordial a manutenção dessa característica. Ou seja, os dispositivos devem ser bem-vindos na rede, mas de maneira mais segura.

Em um dos parágrafos da seção **??** do capítulo 3, comparamos os dispositivos IoT com os pedestres no trânsito, que em sentido geral são a parte mais frágil em seus respectivos sistemas. Os IoT em redes domésticas são vulneráveis a ataques cibernéticos, entre outros fatores, devido à falta de padronização e segurança. A diversidade de marcas e plataformas dificulta a implementação de medidas de segurança uniformes, deixando as redes domésticas suscetíveis a invasões e utilização indevida.

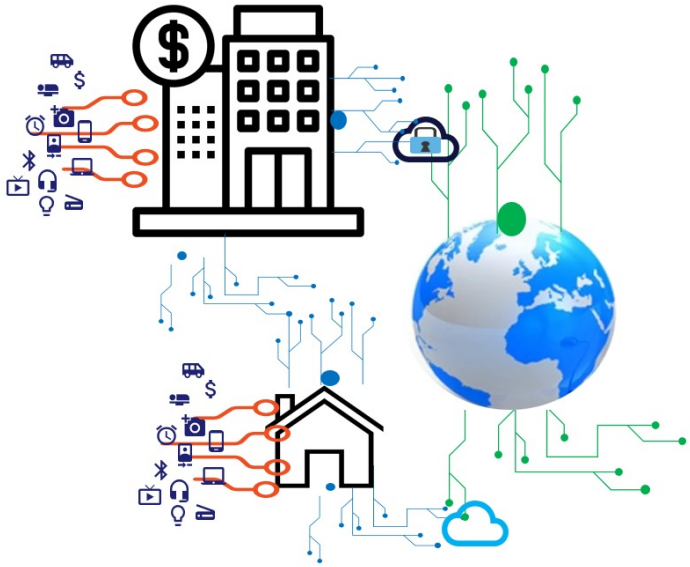
Em se tratando da conjuntura atual de mundo em que cada vez mais as empresas adotam o trabalho remoto, há que os dispositivos possam ser empregados de maneira criminosa nas empresas com ligação direta a casas inteligentes por intermédio de seus funcionários.

Uma empresa com conexão à Internet seguirá a mesma lógica de uma casa igualmente conectada, com o diferencial que, muitas investem em cibersegurança. Este investimento

pode influenciar no fato de dispositivos presentes nela não serem tão facilmente alcançáveis.

Se o funcionário trabalha remotamente, ele acaba por ligar duas redes, uma empresarial e outra residencial, a primeira possivelmente mais segura que a segunda. Deste modo, ambas não estarão protegidas, a depender essencialmente das políticas de segurança adotadas por essas e do nível de assimilação de seus funcionários. A Fig. 13 representa este cenário.

Figura 13 – Conexão IoT Casa <-> Empresa



Fonte: Próprio autor

MAIOS é uma aplicação possível de ser implementada em hardware que tem como objetivo monitorar os tráfegos de dispositivos IoT presentes na rede de modo a mitigar ao máximo as possibilidades de ataque ou utilização indevida desses.

4.1.3 Necessidades e Desafios

A necessidade de segurança em redes domésticas com dispositivos IoT requer uma abordagem que seja usável, transparente e eficaz. Os desafios incluem encontrar uma solução que além da segurança garanta a interoperabilidade entre dispositivos diversos, enquanto mantém a capacidade de interação dos dispositivos IoT na rede. A Fig. 14 representa essa necessidade.

Figura 14 – Conexão IoT Casa <-> Empresa <-> Segura

Fonte: Próprio autor

A usabilidade é a característica necessária para que usuários finais tenham à disposição interfaces intuitivas e amigáveis que permitam a operacionalização de todo o sistema, configurando facilmente as políticas de segurança para dispositivos IoT. Pode ser relacionada também à camada de aplicação em uma arquitetura SDN. A usabilidade está intrinsecamente ligada à capacidade de configurar regras de segurança de forma clara e compreensível, garantindo que as políticas sejam facilmente ajustáveis de acordo com as necessidades dos usuários domésticos.

Por outro lado, a transparência está associada ao plano de controle em uma arquitetura SDN. Aqui, os controladores SDN gerenciam e distribuem políticas de segurança de forma centralizada para os dispositivos na rede. A transparência refere-se ao fato de que os dispositivos IoT na rede não precisarem entender os detalhes das políticas de segurança; eles apenas aplicam as instruções do controlador SDN. Essa abordagem centralizada permite uma visibilidade clara das políticas de segurança, garantindo uma aplicação consistente em toda a rede doméstica. A propósito, a existência de um plano de controle é muito bem-vinda em redes corporativas.

Por fim, a eficácia do plano de dados pode ser incrementada em uma arquitetura SDN. Nesta camada, a eficácia de políticas de segurança são aplicadas em tempo real. O controlador SDN pode detectar padrões de tráfego suspeitos, isolar dispositivos comprometidos e aplicar regras dinâmicas para prevenir possíveis ataques. A capacidade de resposta instantânea do SDN às ameaças no plano de dados demonstra a eficácia das políticas de segurança implementadas, protegendo os dispositivos IoT de intrusões indesejadas.

4.2 Metodologia de Desenvolvimento

Nessa seção, será apresentada a Metodologia de Desenvolvimento adotada para criar a solução proposta para os desafios identificados. Serão abordados os métodos, ferramentas e técnicas empregados, assim como os critérios de avaliação utilizados para validar a eficácia da solução.

4.2.1 Requisitos Funcionais - RF

Neste tópico são descritos os requisitos funcionais contendo as principais funcionalidades oferecidas aos usuários. Cada requisito, condição ou capacidade de satisfazer as necessidades do usuário, é apresentado na Tabela 1 que contém o Código identificador, o Nome, a Descrição e a Prioridade.

Tabela 1 – Requisitos Funcionais

REQUISITO	DESCRIÇÃO	PRIORIDADE
RF-01	Adiciona dispositivo IoT	**MÉDIA**
RF-02	Atualiza dispositivo IoT	**MÉDIA**
RF-03	Remove dispositivo IoT	**MÉDIA**
RF-04	Lista Dispositivos IoT	**MÉDIA**
RF-05	Bloqueia Dispositivo IoT	**ALTA**
RF-06	Monitora Rede	**ALTA**
RF-07	Alarma Incidente	**ALTA**
RF-08	Insere Base de Assinaturas IoT	**BAIXA**
RF-09	Atualiza Base de Assinaturas IoT	**BAIXA**
RF-10	Remove Base de Assinaturas IoT	**BAIXA**
RF-11	Lista Base de Assinaturas IoT	**MÉDIA**
RF-12	Bloqueia Base de Assinaturas IoT	**ALTA**
RF-13	Insere Base de pacotes Maliciosos	**BAIXA**
RF-14	Atualiza Base de pacotes Maliciosos	**BAIXA**
RF-15	Remove Base de pacotes Maliciosos	**BAIXA**
RF-16	Lista Base de Base de pacotes Maliciosos	**MÉDIA**
RF-17	Bloqueia Base de Base de pacotes Maliciosos	**ALTA**

Fonte: Próprio autor

Na Tabela 1 os requisitos são codificados de Requisito Funcional (RF)-01 até RF-17, para os quais a prioridade no sistema são avaliadas como Alta, Média ou Baixa, respectivamente nas cores vermelha, laranja e verde.

Embora não esteja especificado na Tabela 1, cada RF pode estar relacionado diretamente a um ou mais RFs. Estes requisitos estabelecem as condições necessárias para o cumprimento das funcionalidades do MAIOS, nesta versão.

Os requisitos listados na tabela 1 estarão disponíveis ao usuário, para alterações que se julgarem importantes, em modo personalizado. Todavia, o sistema deverá ser capaz de

identificar cada dispositivo conectado na rede com base em listas de assinaturas padrões previamente instaladas e atualizáveis via plano de dados. Apesar das listas também serem editáveis através de comandos do usuário, o sistema tem a pretensão de disponibilizar esse recurso de maneira transparente e dinâmica.

Funcionalidades referentes a várias demandas inerentes a um sistema SDN já estão presentes de maneira nativa em aplicações utilizadas em nosso projeto, sendo os requisitos listados, uma amostra daquilo que foi julgado de extrema importância para o cumprimento do objetivo proposto.

Os próximos tópicos apresentam requisitos não diretamente ligados às funcionalidades (Requisito não Funcional (RNF)), que lidam diretamente com as possíveis limitações do produto proposto no processo de desenvolvimento ou produção/operação.

4.2.2 Requisitos Não Funcionais

Os RNFs são aqueles relacionados ao uso da aplicação, neste caso, o conjunto que engloba as tecnologias aplicadas para o cumprimento da proposta. Nas alíneas abaixo são apresentadas aquelas mais importantes:

a) **Requisitos de Desempenho:** Nas configurações propostas o sistema comportará a quantidade de pelo menos 250 dispositivos IoT conectados, usando uma rede *Wireless Fidelity* (WI-FI) de 2.4GHz. O sistema funcionará em modo local e poderá ser acessado remotamente pela internet com largura de banda de taxas usuais para *donwload* e *upload*;

b) **Requisitos de Usabilidade:** Requisito fundamental, a usabilidade será garantida com uma interface limpa, de fácil compreensão e com curva de aprendizado baixa. Além disso, o sistema terá uma configuração padrão que permitirá a instalação de dispositivos no modo *plug and play*, com intervenção mínima do usuário;

c) **Requisitos de Disponibilidade:** No modo local em condições de infraestrutura ideais e com carga energética fluindo normalmente entre todos os dispositivos a disponibilidade, ou seja, a capacidade do sistema estar disponível ao usuário deverá ser de pelo menos 99,9%. Para o acesso remoto mantendo a carga energética nas mesmas condições e conexão de internet sem interferências, almejamos a disponibilidade de 99,8%;

d) **Requisitos de Segurança:** Todos os dispositivos conectados no MAIOS, terão uma porta dedicada com faixa de IP própria e total segmentação em relação as outras portas por meio de tecnologias de SDN e, em adição, o sistema contará com IDS e *Intrusion Prevention System* (IPS) com monitoramento constante dos pacotes trafegados pela rede e sistema de alarmes, sendo que as listas de pacotes suspeitos serão sempre atualizadas no plano de controle;

e) **Requisitos de interoperabilidade:** Qualquer dispositivo IoT poderá ser conectado ao sistema e realizar comunicação MTC. Nessa configuração temos como foco dispositivos com conexão WI-FI de 2.4GHz. Entretanto, a depender de instalação de receptores de outros tipos de protocolo como Zigbee ou *Bluetooth* por exemplo, podem ser considerados. As listas de assinaturas dos dispositivos e protocolos aceitos serão sempre atualizadas no plano de controle;

f) **Requisitos de Manutenção:** As atualizações de segurança ou melhorias do sistema serão implementadas no sistema de forma automática com intervenção miníma do usuário. Será possível o *downgrade* do sistema mediante comando do usuário com consentimento das implicações de segurança. A parte de hardware do sistema deverá ser assistidas por técnicos da área com especialidades voltadas para equipamentos de rede;

g) **Requisitos de Documentação:** O sistema contará com manual de usuário abrangente que cobrirá todas as funcionalidades, com exemplos de utilização em diversos cenários possíveis. Toda requisição ao suporte e possíveis soluções a problemas específicos será documentado e os recorrentes serão disponibilizados na página principal do suporte; e

h) **Requisitos de Integração:** Todos os componentes do sistema, poderão se intercomunicar, respeitando suas características e necessidades.

4.2.3 Arquitetura Proposta

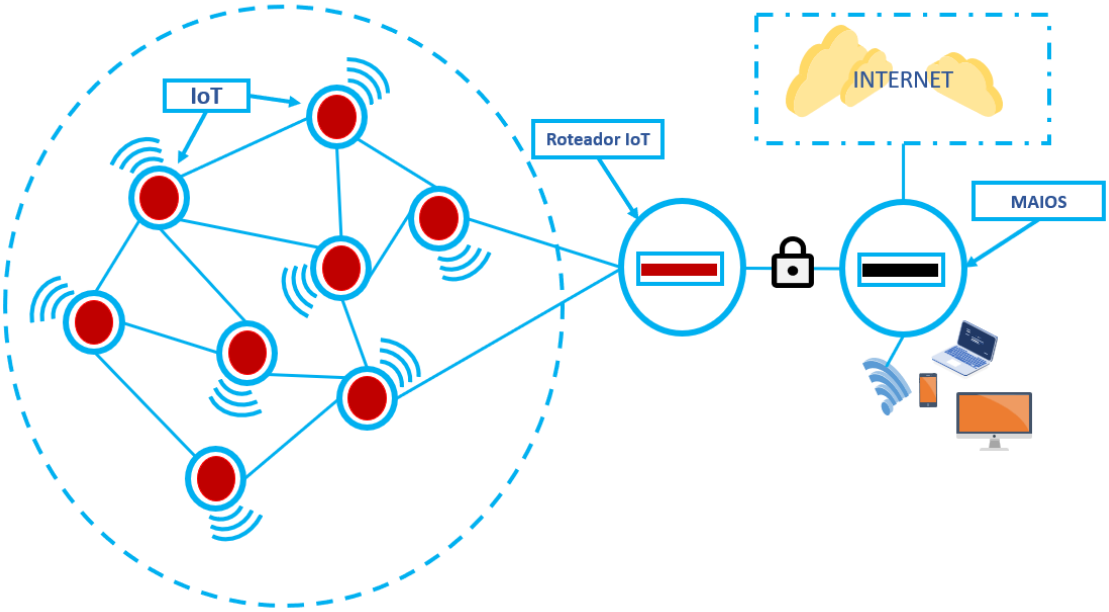
Em um mundo onde a informação é um capital importante tanto para governos ou empresas a busca por soluções que possam proteger esse capital se torna uma necessidade prioritária. Logo os gastos para este tipo de serviço tendem a se elevar. Por outro lado, o cidadão comum não possui o mesmo grau de preocupação ou (in)formação suficiente.

Essa desproporção na balança, em que uma parte está sempre em busca de melhores soluções acaba por aumentar a vulnerabilidade da outra parte que não está. À medida que cibercriminosos também evoluem na busca de brechas.

O sistema MAIOS apresenta como proposta uma equalização nessa balança, se voltando principalmente ao público mais vulnerável dessa corrente. Apresentando uma solução viável, de baixo custo e de simples implementação. Na Fig. 15 é possível visualizar o panorama geral de serviço do MAIOS.

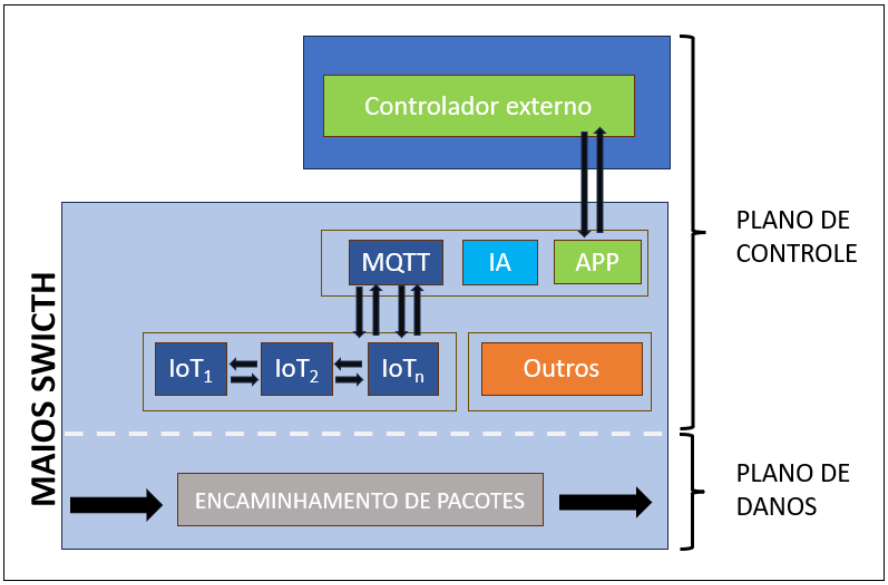
A organização em camadas proposta através da Fig. 16 se baseia da divisão do Plano de Controle e Plano de dados, especificados pelo padrão SDN, introduzido na seção 3.3.1. Dessa forma, as aplicações contidas no MAIOS poderão ter suas bases atualizadas por um controlador da rede e de igual forma esse controlador poderá receber informações de tráfego capaz de retroalimentar sua base de informações (*dataset*).

Figura 15 – Arquitetura Geral - MAIOS



Fonte: Próprio autor

Figura 16 – Organização em Camadas - MAIOS

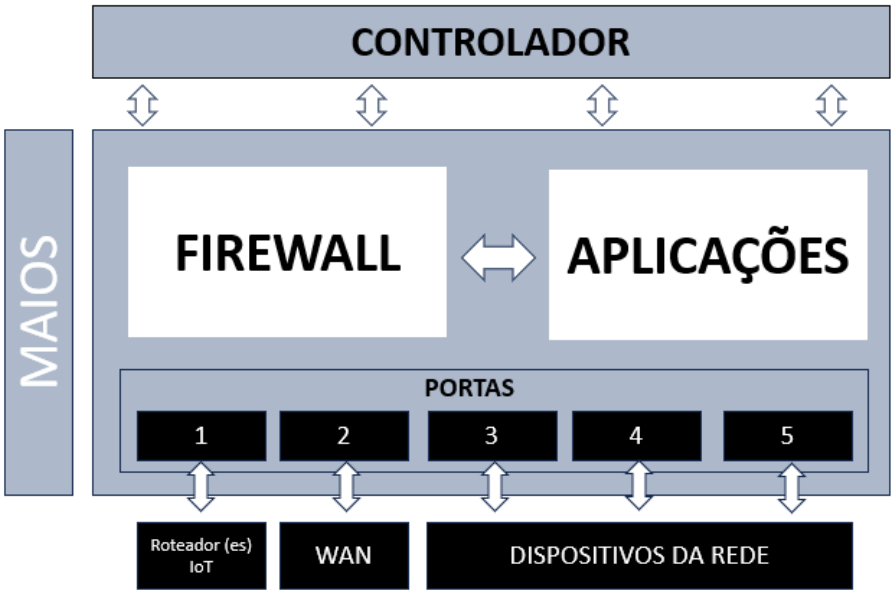


Fonte: Próprio autor

Com base nos RF, apresentados na Tabela 1, nos RNF, descritos na seção 4.2.2, e no escopo do trabalho, a arquitetura proposta apresenta um plano de controle capaz de governar e se retroalimentar de informações do plano de Dados. O plano de Dados, por sua vez, será capaz de garantir a entrega de pacotes. A organização da arquitetura proposta é representado na Fig. 17.

A versão inicial do MAIOS é voltada para o público doméstico, com arquitetura similar

Figura 17 – MAIOS: Arquitetura proposta



Fonte: Próprio autor

a roteadores existentes, com a adição da porta dedicada a IoT. Como *Switch*, MAIOS terá missão de segmentação e inteligência necessárias para elencar funções distintas a cada porta. De maneira *default* será entregue com a segmentação da porta dedicada a dispositivos IoT, porta para conexão *Wide Area Network* (WAN) e demais portas *bridge* para conexão geral.

4.2.3.1 Cenário Residencial

Em busca da usabilidade, o MAIOS terá aparência e funções similares a um roteador comum. O usuário doméstico, acostumado ao padrão das operadoras de *internet*, não terá dificuldade em configurar sua conexão e utilizar a internet.

Ao utilizar o sistema, o usuário conectará seu link de internet na porta WAN e este será distribuído para as portas subjacentes. O *switch* também poderá contar com conexão WI-FI. A diferença será a porta destinada aos dispositivos IoT em que os dispositivos pertinentes serão conectados conforme a Fig. 15.

A conexão que se fizer necessária na porta destinada aos dispositivos IoT será oriunda de concentradores de protocolos diversos, como Zigbee e outros. O MAIOS contará com rede de WI-FI de 2.4GHz, comum a maioria dos dispositivos desse gênero no mercado, compartilhando da mesma segurança da porta dedicada.

4.2.3.2 Cenário Empresarial

Em um cenário empresarial, o MAIOS poderá ter versão com maior quantidade de portas e preparado para ser acoplado em *hack* dentro de estruturas de Centro de Processamento de Dados (CPD) (*datacenter*) junto aos demais equipamentos de TI da empresa.

O MAIOS será dotado de *firewall* e poderá ser utilizado para segurança e configuração de toda rede de maneira independente. Além do aumento do número de portas normais, poderão ser incrementadas portas dedicadas a dispositivos IoT adicionais.

É importante salientar que em um ambiente empresarial se pressupõem a presença de profissional ou empresa especializada contratada com capacidade técnica para configurações avançadas. Todavia, o sistema básico seguirá as diretrizes do ambiente doméstico.

Em empresas de pequeno porte, o MAIOS, com sua configuração padrão, garantirá as mesmas condições de segurança dos dispositivos IoT de residências.

4.2.3.3 Aplicativos do MAIOS

Na camada de controle do MAIOS, haverá uma série de aplicações capazes de gerir e garantir o cumprimento dos objetivos propostos na seção 1.2. Uma interface clara e objetiva, com abordagem voltada para usabilidade e decremento da curva de aprendizado, garantirá um ambiente amigável a qualquer nível de usuário. As principais aplicações presentes são:

- ***Firewall***: Inicialmente será utilizado um serviço *OpenSource* e, entre os disponíveis, optou-se pelo ***pfSense*** por sua robustez e presença de mercado;
- **Controle IoT**: O MAIOS será dotado de um sistema de controle central para dispositivos domésticos e para tal foi escolhido o *Home Assitant* que também é de código aberto;
- **MQTT**: Embora não seja uma aplicação em si, o protocolo MQTT será utilizado para a comunicação MTC que auxiliará o MAIOS na autenticação de dispositivos;
- **IA**: O sistema MAIOS será capaz de aprender e retroalimentar o controle central com informação acerca de pacotes maliciosos encontrados da rede, desde que, autorizado pelo usuário;
- **Análise de Tráfego**: Para detecção de intrusão o MAIOS fará uso de tecnologia capaz de analisar o trafego em tempo real, para tanto foi escolhido o *Snort*, que opera como *plugin* instalável no *firewall*, com capacidade de operar como NIDS, atuando tanto na prevenção IPS como na detecção IDS;
- **Sistema de controle local**: Será um facilitador para a configuração básica dos serviços do MAIOS e responsável pela busca junto ao sistema de controle geral de atualizações acerca de listas de pacotes maliciosos e de listas de IoT;
- **Sistema de controle geral**: responsável pelo provimento de listas atualizadas de pacotes maliciosos encontrados na rede, principalmente os relacionados a IoT e suas novas assinaturas.

O conjunto de aplicações apresentado tem o potencial de ser unificado em um Sistema Operacional (SO) *LINUX*, dedicado ao MAIOS.

O *firewall* embarcado será o responsável pela segmentação das portas, que terão *gateways* próprios e propagarão suas próprias redes. Juntamente com sistema de detecção de intrusão que monitorará os pacotes em tempo real observando o tráfego existente na porta dedicada a IoT.

Importante destacar o sistema de controle local, que proverá o usuário com informações pertinentes sobre o sistema, por meio de *dashboard* intuitivo, e com formulários de cadastros. Esse sistema será responsável pela comunicação com o sistema de controle geral.

Embora o usuário possa ter total controle da ferramenta, o sistema MAIOS se encarregará de executar todas as tarefas de maneira automática com intervenção humana miníma.

Capítulo 5

Experimentos e Análise dos Resultados

O trabalho tem como meta o cumprimento de pontos relevantes que em conjunto possuem o potencial de tornar o MAIOS uma solução inovadora. De maneira geral, temos a segmentação de rede e o monitoramento em tempo real da rede voltada para IoT. Além disso, o controle externo (SDN) que garantirá uma atualização constante do sistema.

Inicialmente, será feita simulação da infraestrutura proposta usando o GNS3, que é um simulador de redes amplamente reconhecido. Posteriormente, a materialização física da solução será desempenhada por meio da instalação dos sistemas necessários em um ambiente preparado com placas de rede adicionais.

5.1 Ambiente de Simulação e Prototipagem

Foi escolhido o GNS3, pois oferece suporte a diversos sistemas operacionais e capacidade de criar ambientes 'virtuais realistas'. Essa escolha se alinha à busca por simular o comportamento de redes reais, proporcionando um ambiente controlado e flexível, que permita a verificação.

O ambiente simulado é composto por um servidor *pfSense*, para a segmentação da rede, e um servidor *Home Assistant*, para a interoperabilidade de dispositivos IoT heterogêneos. Esses servidores estarão interconectados com máquinas virtuais que também estarão presentes na simulação, fornecendo a possibilidade de incorporar aspectos reais de uma rede convencional.

Para avaliar a robustez do MAIOS em condições adversas do mundo real, são incorporados testes de segurança que incluem o uso de listas de pacotes infectados. Essa abordagem prática permitirá avaliar a capacidade do sistema em detectar, isolar e neutralizar ameaças potenciais.

A inclusão de dispositivos IoT reais na simulação proporcionará um ambiente híbrido, permitindo-nos avaliar o desempenho e a eficácia da solução proposta em condições próximas à realidade. Essa abordagem integrada busca superar as limitações de muitos am-

bientes puramente virtuais, considerando a diversidade e complexidade dos dispositivos IoT presentes nos lares modernos.

Este capítulo explora as nuances da simulação GNS3, desde a configuração inicial até a implementação e teste das soluções de segurança propostas pelo MAIOS. A transição subsequente para o protótipo físico garantirá a verificação prática de nossa abordagem, destacando os desafios encontrados, ajustes realizados e os resultados obtidos em ambientes simulados e reais.

5.1.1 Instalação do GNS3

A instalação do simulador GNS3 pode variar um pouco a depender do sistema operação utilizado. Embora possua suporte para outros sistemas como LINUX e macOS, em nossa abordagem utilizaremos o sistema operacional *Windows* da *Microsoft*. Os requisitos recomendados para instalação do simulador no *Windows*, segundo a documentação da ferramenta são:

- **Sistema operacional**: *Windows* 7 (64 bit) ou superior;
- **Processador**: 2 ou mais núcleos;
- **Memória RAM**: 4 GB;
- **Capacidade de virtualização**: habilitada na *Basic Input Output System* (BIOS) do computador; e
- 1 GB de espaço livre.

É imperativo informar que essas são as configurações mínimas apenas para instalação do simulador. Como nossa simulação contará com máquinas virtuais interligadas pela rede, é mandatório incorporar os requisitos desses servidores no ambiente. Assim sendo, em nossa simulação usamos um computador com as seguintes características:

- **Sistema operacional**: *Windows* 11 (64 bit);
- **Processador**: Ryzen 5 (seis núcleos);
- **Memória RAM**: 16 GB;
- **Capacidade de virtualização**: habilitada na BIOS do computador;
- **Espaço livre em disco**: 2 TB de espaço livre.

O site oficial para download da ferramenta é o: https://www.gns3.com. Durante o processo são sugeridos componentes adicionais como o GNS3 VM (uma máquina virtual

para melhor desempenho), o *Dynamips/Dynagen*, o *Wireshark Integration* e o *WinPcap*, que neste caso foram todos aceitos e instalados.

Resumidamente, o *Dynamips/Dynagen* permite a utilização de imagens com o sistema operacional Cisco *Internetwork Operating System* (IOS) em ambiente virtual e a possibilidade de utilizar linhas de comandos para suas respectivas configurações. Já o *Wireshark Integration* serve para análise de protocolo e captura de pacotes. O *WinPcap* é um *driver* de captura de pacotes para sistemas operacionais *Windows*.

Para a virtualização optamos pelo *VMware workstation player* 17, última versão da ferramenta obtida no site: https://www.vmware.com. O GNS3 oferece suporte também para o *Oracle VirtualBOX*. Para utilização no sistema operacional *Windows* 11, é obrigatória a última versão do VMware.

Toda gestão das máquinas virtuais serão feitas pelo software de virtualização escolhido. O GNS3 possui a funcionalidade de se conectar com essas ferramentas e incorporar a rede simulada às máquinas instaladas dessas aplicações. Além disso, o GNS3 suporta a importação de "*appliances* virtuais", de vários fabricantes, e isso facilita o processo de inclusão de dispositivos virtuais, pois se refere a máquinas virtuais com configuração prévia e funções específicas, como de roteadores, servidores DNS, DHCP entre tantos outros.

5.1.2 Configuração Inicial

Antes de começar a implementar o MAIOS é necessário configurar a máquina virtual GNS3 VM, ajustando parâmetros de memória, *Central Processing Unit* (CPU) e outras configurações críticas para maximizar o desempenho. Em nosso experimento optamos por configurar essa máquina com um processador de 2 (dois) núcleos, 2 GB de memória *Random Acess Memory* (RAM) e 10 GB de espaço em disco.

Para que a rede externa seja acessada, a interface do adaptador de rede deve estar em *Bridge*, configuração que desativa o recurso NAT no *modem*, permitindo que um roteador funcione como um servidor DHCP, sem conflito de endereço IP, e é necessário também configurar um IP válido para essa VM na faixa da rede real, ou seja, a GNS3 VM estará na mesma sub-rede que a rede física utilizada. Deveremos apontar a aplicação GNS3 para sua máquina virtual, sendo assim, em `editar > preferencias` selecionamos "GNS3 VM" na barra lateral e em `Redes`, configuramos para interface de rede correta.

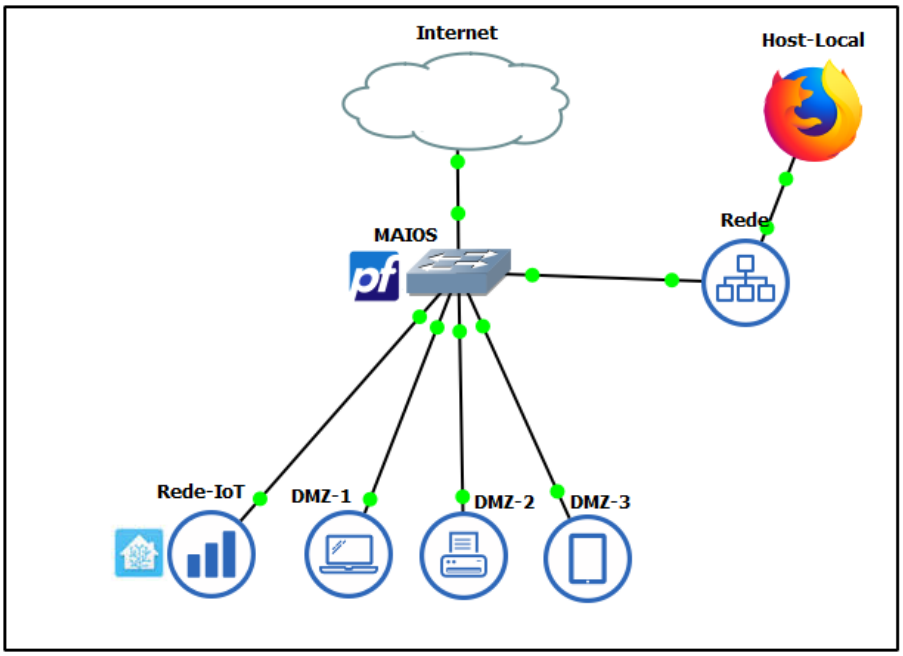
No sistema operacional principal, temos de certificar de que a rede permita a comunicação com uma sub-rede virtual. Para os testes optamos em desativar os *firewalls* temporariamente. Em uma melhor abordagem é preferível liberar as portas e aplicações voltadas para o laboratório no *firewall*, voltando ao estado anterior ao término dos testes.

Antes de iniciar os experimentos, foram implementadas medidas para garantir a consistência e precisão da simulação. Isso incluiu a verificação cuidadosa das configurações de cada dispositivo virtual, a alocação adequada de recursos, e a correta interconexão

entre os componentes da rede. O principal dessa etapa é ter o entendimento de que em nossa simulação o conceito de rede hibrida exige um nível de abstração maior, visto que, incorporamos aspectos de uma rede real em nossa simulação.

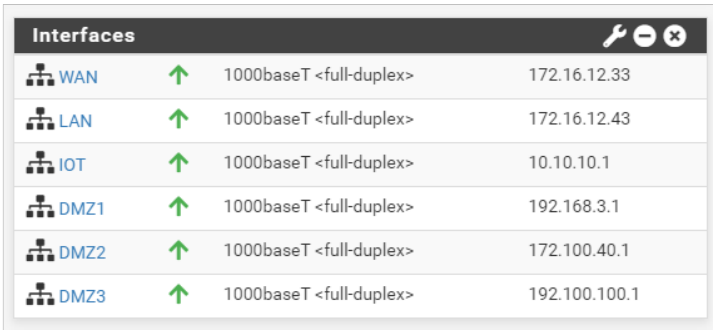
No GNS3 montamos um laboratório hibrido, ou seja, componentes virtuais mesclados com uma rede real. De acordo com a Fig. 18 há o MAIOS, com o *firewall pfSense* integrado, conectado a ele por nossa porta orientada a IoT, o servidor *Home Assitant* na entrada de internet e a conexão com a rede local também são representadas.

Figura 18 – Topologia da simulação no GNS3



A rede local está configurada na faixa de endereço IP 172.16.12.0/24, a rede IoT na faixa de endereço IP 10.10.10.0/24 e a DMZ, respectivamente com a faixa de endereço IP 192.168.3.0/24 e os endereços IPs 172.100.40.1 e 192.100.100.1. O MAIOS/*pfSense* está configurado com o endereço IP estático 172.16.12.43 e o servidor IoT (*Home Assistant*) está configurado com o endereço IP estático 10.10.10.100.

Figura 19 – Interfaces MAIOS/*pfSense*



Interfaces			
WAN	↑	1000baseT <full-duplex>	172.16.12.33
LAN	↑	1000baseT <full-duplex>	172.16.12.43
IOT	↑	1000baseT <full-duplex>	10.10.10.1
DMZ1	↑	1000baseT <full-duplex>	192.168.3.1
DMZ2	↑	1000baseT <full-duplex>	172.100.40.1
DMZ3	↑	1000baseT <full-duplex>	192.100.100.1

5.1.3 Adição de Dispositivos Virtuais

O processo de adição de dispositivos virtuais no GNS3, utilizando o VMware como plataforma de virtualização, é crucial para a construção eficaz da simulação. Nesta seção são detalhados os passos para incorporar dispositivos como *pfSense* e *Home Assistant* à topologia da rede.

- **Preparação das Imagens Virtuais**: As imagens das máquinas virtuais foram obtidas nos sites de seus desenvolvedores, sendo o *pfSense* encontrado em sua última versão no site: https://pfsense.org. O *Home Assitant* foi obtido no site: https://www.home-assistant.io em sua versão de sistema operacional baseada no Linux.

- **Configuração do GNS3 para VMware**. No GNS3 é preciso acessar o menu "`Edit`"e selecionar "`Preferences`". Após isso, em "`Virtualization`", escolha "`VMware`"como servidor de virtualização. Adicione o caminho para o executável do VMware Workstation Player;

- **Integração com VMware**: Novamente em "`Preferences`", é selecionada a opção "`VMware`"na barra lateral e configurados detalhes como endereço do servidor e credenciais de login, sendo necessário o ajuste das configurações de rede para garantir conectividade entre a sub-rede virtual e a rede física;

- **Adição de Dispositivos à Topologia no GNS3**: No painel principal, arrastam-se os dispositivos desejados da barra lateral para a área de trabalho, configurando as opções específicas para cada dispositivo, como interfaces de rede, alocação de RAM, etc. e, nesse momento, são selecionadas as máquinas virtuais necessárias para simulação;

- **Conexão e Interligação**: é usado o recurso de conexão para criar `links` lógicos entre as interfaces dos dispositivos conforme a topologia desejada;

- **Inicialização e Configuração**: são inicializados os dispositivos virtuais no GNS3 e monitorado o console para verificar a inicialização adequada, sendo configurados cada dispositivo conforme necessário, incluindo endereços IP, configurações de *firewall*, entre outros.

A configuração correta das interfaces de rede no GNS3, especialmente ao integrar com o VMware, é necessária para garantir que as máquinas virtuais estejam na mesma sub-rede virtual. Além disso, devem ser verificadas as configurações de rede no VMware para assegurar a conectividade adequada entre a sub-rede virtual e a rede física.

5.1.4 Configuração Específica para a Simulação

Ao realizar simulações no GNS3, com dispositivos virtuais no VMware, é importante atentar para configurações específicas que asseguram eficácia e fidelidade. Primeiramente, configuram-se cuidadosamente as interfaces de rede, atribuindo endereços IP e garantindo conexões adequadas. De maneira geral esse é o ponto mais delicado da simulação e por vezes mencionado.

Deve ser ajustada a alocação de memória e recursos conforme as recomendações de cada dispositivo para garantir um desempenho otimizado durante a simulação. Verifique também a conectividade entre a sub-rede virtual do GNS3 e a rede física no VMware, evitando problema de comunicação. Em nosso caso seguimos as configurações minímas exigidas por desenvolvedores.

Ao iniciar os dispositivos virtuais, é preciso monitorar o console para garantir uma inicialização sem erros. Em cada mudança significativa nas configurações realizamos *backups* ou *snapshots*, permitindo a restauração a um estado anterior em caso de contratempos.

Para os testes ocorrerem sem maiores complicações, os recursos do sistema devem ser monitorados, avaliando o consumo de CPU, memória e outros durante a simulação, identificando possíveis gargalos de desempenho.

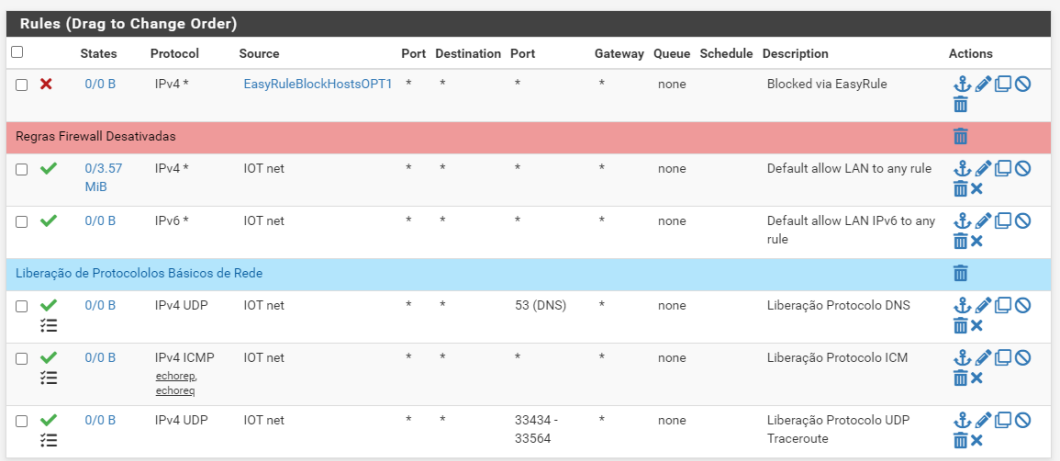
5.1.5 Verificação da Integridade da Simulação

A integridade da simulação é de fundamental importância para garantir a validade e a confiabilidade dos resultados obtidos. Nesta seção, os procedimentos adotados para verificar a integridade da simulação, abordando aspectos relacionados à configuração, execução e monitoramento dos experimentos, serão enumerados.

5.1.5.1 Verificação de Conectividade

Após a configuração inicial, procedeu-se à verificação da conectividade entre os dispositivos virtuais. Isso envolveu a execução de verificação de disponibilidade de equipamentos conectados, *ping* e a análise de *logs* para identificar eventuais problemas de comunicação. A garantia de que todos os dispositivos estavam interligados corretamente foi crucial para simular um ambiente realista.

Nesta etapa deve-se atentar para a liberação de regras no servidor *pfSense* dentro do MAIOS.



Rules (Drag to Change Order)

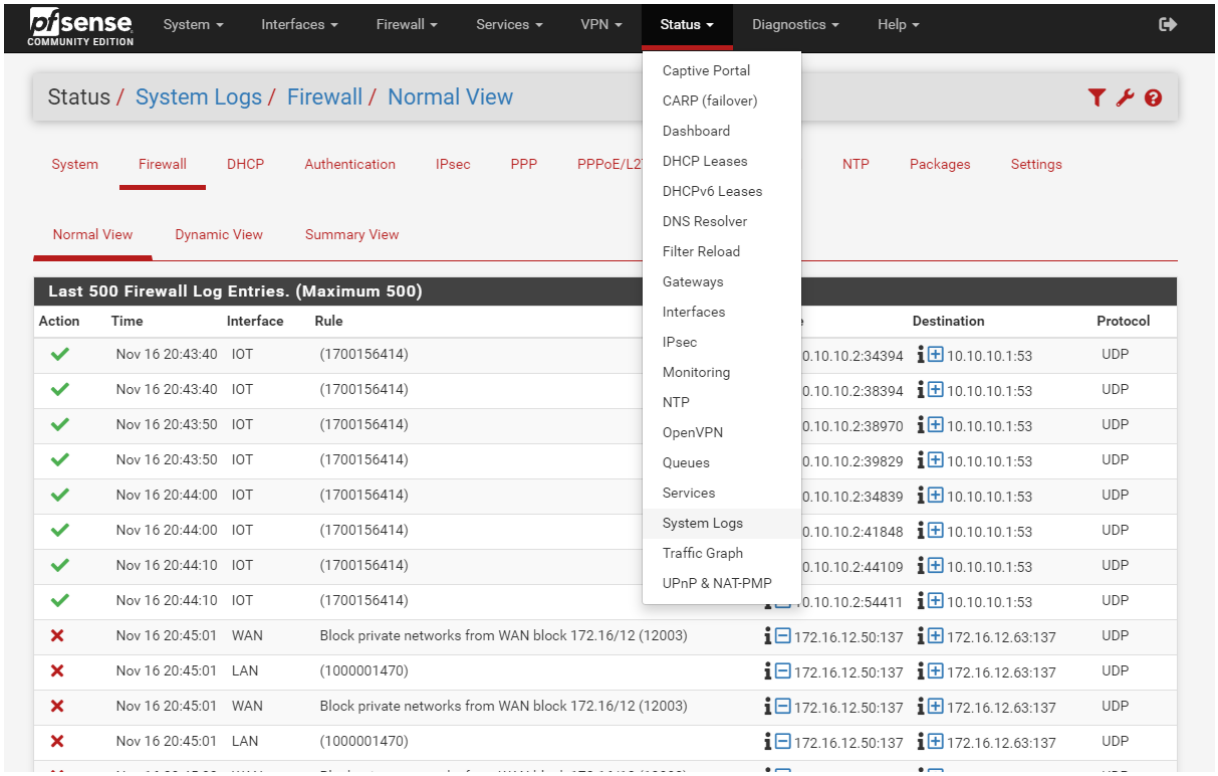
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	EasyRuleBlockHostsOPT1	*	*	*	*	none		Blocked via EasyRule	
Regras Firewall Desativadas										
0/3.57 MiB	IPv4 *	IOT net	*	*	*	*	none		Default allow LAN to any rule	
0/0 B	IPv6 *	IOT net	*	*	*	*	none		Default allow LAN IPv6 to any rule	
Liberação de Protocololos Básicos de Rede										
0/0 B	IPv4 UDP	IOT net	*	*	53 (DNS)	*	none		Liberação Protocolo DNS	
0/0 B	IPv4 ICMP echorep, echoreq	IOT net	*	*	*	*	none		Liberação Protocolo ICM	
0/0 B	IPv4 UDP	IOT net	*	*	33434 - 33564	*	none		Liberação Protocolo UDP Traceroute	

Figura 20 – Regras de *Firewall*

5.1.5.2 Monitoramento em Tempo Real

Durante a execução da simulação, foi realizado um monitoramento constante. Utilizando as ferramentas integradas do GNS3 e do VMware, registramos métricas de desempenho, como utilização de CPU, consumo de memória e taxa de transferência de rede. Qualquer anomalia foi investigada para garantir a integridade dos resultados.

Com o sistema em operação, também, é possível o monitoramento via *pfSense* através da função `Status/System Logs`.



pfsense COMMUNITY EDITION — System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help

Status / System Logs / Firewall / Normal View

System | Firewall | DHCP | Authentication | IPsec | PPP | PPPoE/L2 | NTP | Packages | Settings

Normal View | Dynamic View | Summary View

Captive Portal
CARP (failover)
Dashboard
DHCP Leases
DHCPv6 Leases
DNS Resolver
Filter Reload
Gateways
Interfaces
IPsec
Monitoring
NTP
OpenVPN
Queues
Services
System Logs
Traffic Graph
UPnP & NAT-PMP

Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule		Destination	Protocol
✓	Nov 16 20:43:40	IOT	(1700156414)	0.10.10.2:34394	10.10.10.1:53	UDP
✓	Nov 16 20:43:40	IOT	(1700156414)	0.10.10.2:38394	10.10.10.1:53	UDP
✓	Nov 16 20:43:50	IOT	(1700156414)	0.10.10.2:38970	10.10.10.1:53	UDP
✓	Nov 16 20:43:50	IOT	(1700156414)	0.10.10.2:39829	10.10.10.1:53	UDP
✓	Nov 16 20:44:00	IOT	(1700156414)	0.10.10.2:34839	10.10.10.1:53	UDP
✓	Nov 16 20:44:00	IOT	(1700156414)	0.10.10.2:41848	10.10.10.1:53	UDP
✓	Nov 16 20:44:10	IOT	(1700156414)	0.10.10.2:44109	10.10.10.1:53	UDP
✓	Nov 16 20:44:10	IOT	(1700156414)	0.10.10.2:54411	10.10.10.1:53	UDP
✗	Nov 16 20:45:01	WAN	Block private networks from WAN block 172.16/12 (12003)	172.16.12.50:137	172.16.12.63:137	UDP
✗	Nov 16 20:45:01	LAN	(1000001470)	172.16.12.50:137	172.16.12.63:137	UDP
✗	Nov 16 20:45:01	WAN	Block private networks from WAN block 172.16/12 (12003)	172.16.12.50:137	172.16.12.63:137	UDP
✗	Nov 16 20:45:01	LAN	(1000001470)	172.16.12.50:137	172.16.12.63:137	UDP

Figura 21 – Monitoramento de logs MAIOS/*pfSense*

Outro painel capaz de trazer informações em tempo real é o gráfico de tráfego mostrado na Fig. 22, do lado esquerdo, mostra o sistema sem nenhuma requisição, podendo notar que não há alteração aparente na linha mostrada no gráfico, em que a parte azul representa a entrada e a parte laranja representa a saída.

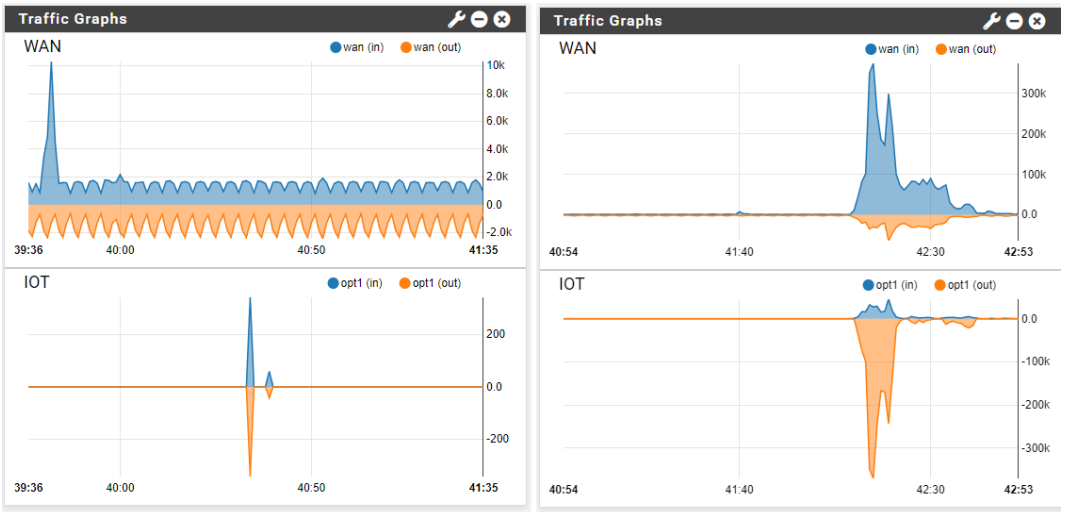


Figura 22 – Monitoramento de Tráfego MAIOS/*pfSense*

Na figura é possível verificar a interação entre a rede IoT e a rede WAN em que o sentido de requisição é invertida. A requisição sendo feita na rede IoT terá sentido de saída enquanto na rede WAN o sentido é de entrada.

5.1.5.3 Verificação de *Logs* e Mensagens do Sistema

Os *Logs* detalhados foram gerados e analisados para identificar possíveis erros ou comportamentos inesperados durante a simulação. Isso incluiu *logs* dos dispositivos virtuais, do GNS3 e do VMware. Os erros encontrados foram tratados e resolvidos de maneira a manter o sistema em funcionamento.

5.1.5.4 Validação dos Resultados Esperados

Ao finalizar cada experimento, os resultados foram comparados com as expectativas previamente definidas. Isso envolveu a análise das métricas de desempenho, a verificação da eficácia das soluções propostas pelo MAIOS e a avaliação da segurança em condições adversas. Resultados inconsistentes foram investigados e a simulação foi ajustada conforme necessário para melhor expressar a realidade.

A abordagem abrangente adotada para a verificação da integridade da simulação visa assegurar que os dados coletados e as conclusões derivadas sejam confiáveis, replicáveis e representativos do cenário proposto. Qualquer desvio ou anomalia teria de ser documentado e discutido, garantindo a transparência e robustez dos experimentos conduzidos.

5.2 Simulação no GNS3

No simulador GNS3 há a condição de iniciar serviços diversos incorporando servidores ou dispositivos virtuais com a possibilidade de integração com a rede local. Nossa simulação constante na Fig. 18 tem como principal vantagem a possibilidade de integrar dispositivos IoT e testar pacotes maliciosos em um ambiente controlado capaz de prover informações relevantes para o projeto.

5.2.1 Integração do *pfSense*

O *pfSense* foi integrado a nossa simulação através de recursos do próprio GNS3, em que imagens de dispositivos podem ser incluídos através de *templates* a nossa máquina virtual GNS3 *server* (opção recomendada). Desta forma temos em nossa rede virtual todas as funcionalidades desse *firewall* e pela característica hibrida do simulador podemos incorporar dispositivos externos ao simulador que estão presentes em nossa rede local.

5.2.2 Integração com *Home Assistant*

O *Home Assistant* foi integrado a simulação por meio da rede local, instalado como máquina virtual no VMWare. Ele é localizável e, em nosso caso, integrado à rede IoT. Essa abordagem foi escolhida para mantermos os IoT em uma mesma interface, todavia, tínhamos a opção de incluir esse servidor através da integração nativa que o GNS3 oferece através de seu virtualizador.

5.2.3 Testes Iniciais

Os testes realizados em nossa simulação visaram atender aos objetivos do projeto no que tange a segmentação de rede, interoperabilidade de dispositivos e detecção/prevenção de intrusão.

5.2.3.1 Segmentação de rede

O MAIOS, concebido como um *switch* inteligente, destaca-se pela implementação de uma segmentação física em suas portas de rede, conferindo inteligência às conexões. Quando integrado ao *pfSense*, que assume as seis interfaces *Ethernet* da máquina virtual, as configurações iniciais estabelecem a interface WAN e *Local Area Network* (LAN) como habilitadas, embora com configurações mínimas.

É crucial observar que, por padrão, qualquer requisição entre redes é bloqueada, como evidenciado na Fig. 23, que apresenta as regras da rede `DMZ1`. A mensagem do recurso alerta que todas as conexões de entrada nessa interface estão bloqueadas até a adição de regras de passagem.

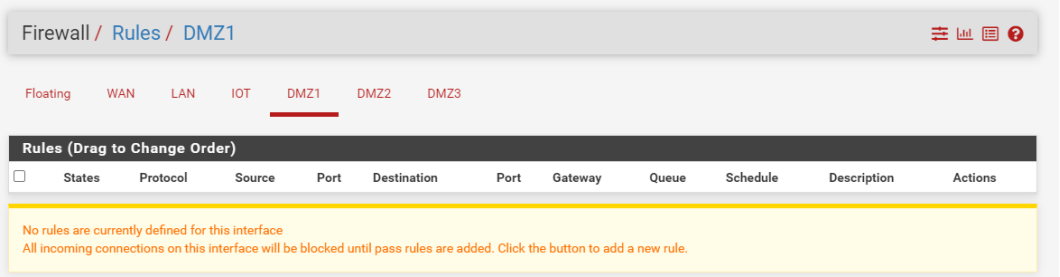


Figura 23 – Configuração inicial de rede MAIOS/*pfSense*

A Fig. 20 expõe as regras mínimas para uma implementação básica, incluindo a liberação do protocolo *Internet Control Message Protocol* (ICMP) para permitir o *ping*. Na versão final do MAIOS, apenas o servidor *Home Assistant* terá acesso externo, as regras serão configuradas com restrição total e com monitoramento de pacotes em tempo real. Em testes, a segmentação demonstrou ser totalmente eficiente.

Essa abordagem permite ao MAIOS operar com inteligência, otimizando a segurança e garantindo uma gestão eficaz das interfaces. Ao ser integrado ao *pfSense*, o *switch* cria um ambiente controlado e segmentado, promovendo a coexistência segura de diferentes serviços na rede. A implementação cuidadosa das regras, conforme descrito, assegura um ambiente robusto e protegido contra acessos indesejados.

Adicionalmente, uma alternativa para a segmentação de portas é a utilização de *Virtual Local Area Network* (VLANs). O principal propósito das VLANs é estabelecer comunicação e conexão em redes físicas por meio de domínios de *broadcast*, proporcionando uma separação lógica entre diferentes serviços. Essa capacidade de gerar redes segmentadas de maneira lógica é uma característica valiosa do MAIOS.

Nesta simulação, optou-se por uma abordagem de segmentação física, atribuindo uma porta de rede para dispositivos IoT e configurando as demais em modo *bridge*. Essa escolha reflete a natureza orientada a IoT do MAIOS e as configurações padrão do equipamento seguirão essa abordagem.

Ao adotar essa estratégia, o MAIOS proporciona uma separação eficiente entre os diferentes tipos de serviços, otimizando não apenas o desempenho, mas também reforçando as medidas de segurança. A configuração física dedicada à IoT oferece uma solução para a coexistência de dispositivos variados em uma rede, garantindo a integridade e isolamento necessários para ambientes diversificados.

5.2.3.2 Interoperabilidade

A interoperabilidade do MAIOS contará com um servidor instalado com o *Home Assistant*. Independentemente do IoT instalado, o controle final se dará por meio desse recurso.

O teste principal se dará utilizando dispositivos de marcas distintas. Em nossa simulação há dispositivos da marca *Tuya* e *Sonoff*. Ambas as marcas possuem aplicações próprias de controle e não se comunicam. A primeira utiliza a aplicação *Smart Live* e a segunda a aplicação *eWlink*. Ambas possuem uma ampla variedade de dispositivos de automação.

Os dispositivos utilizados na simulação são o *Tuya* Interruptor e o Mini R2 Sonoff, conforme a Fig. 24. Tais dispositivos possuem uma variedade de aplicação, pois conseguem transformar qualquer aparelho em inteligente, desde que, estes possuam intensidade de corrente elétrica de até 15 amperes, no caso dos da marca *Tuya*, e de até 10 amperes, no caso dos da marca *Sonoff*.

Figura 24 – Dispositivos Tuya e Sonoff

Ambos os dispositivos se conectam a redes por meio da rede WI-FI de 2.4 GHz e em nossa simulação a conexão se deu de forma hibrida. A rede simulada recebeu um roteador WI-FI externo configurado na porta orientada a IoT administrada pelo *Home Assistant*.

Conforme dito, o servidor *Home Assistant* está presente em nossa rede simulada e é acessado via rede externa pelo endereço IP `10.10.10.2`. De modo geral, a se manter essa faixa de endereço IP no produto final MAIOS, o usuário doméstico só precisaria conectar o roteador IoT na porta dedicada e este já receberia a faixa de IP por DHCP *Server* também habilitado pelo *pfSense*.

Para o caso dessas duas marcas, o *Home Assistant* possui integração nativa e, em poucos ajustes, ele incorpora os dispositivos de mareira rápida e fácil. Além disso, existe uma biblioteca de marcas passíveis de integração. Atualmente a plataforma garante suporte a integração de 2584 modelos, protocolos ou marcas, conforme Fig. 25.

De maneira automática, alguns dispositivos foram localizados, especificamente um televisor *smart* da marca *Samsung* e alguns de seus controles passaram para aplicação. É possível criar *dashboard* personalizada como a Fig. 26. A interface é intuitiva e com boa usabilidade.

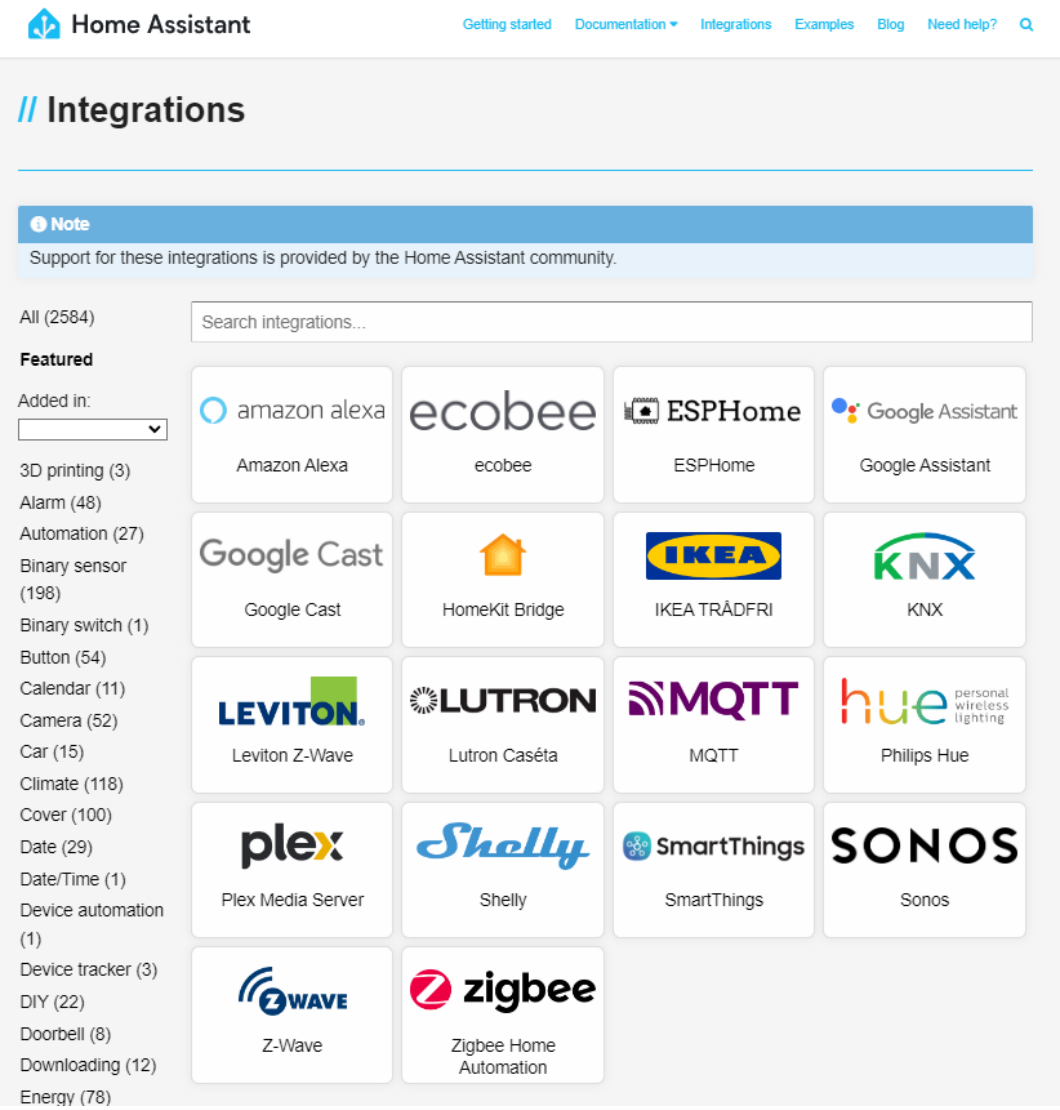


Figura 25 – Integração de dispositivos *Home Assistant*

Fonte:https://www.home-assistant.io/integrations/

Ao reconhecer dispositivos de fabricantes diferentes, foi demonstrada a capacidade que o MAIOS tem em sua configuração final. As duas marcas escolhidas para a simulação e testes possuem. como dito, integração oficial com a ferramenta e embora tenhamos utilizados apenas essas, a gama de dispositivos suportados é ampla.

Outra vantagem obtida por esse modelo é a possibilidade de acesso aos dispositivos sem a necessidade de *internet*. Grande parte dos fabricantes de IoT voltados para o bem estar possuem aplicações alcançáveis apenas pela internet.

5.2.3.3 Detecção e Prevenção de intrusão

Para esse teste foi instalado o *System for Network and Host-based Event Recognition and Analysis Technologies* (SNORT) no *pfSense* e aplicado o controle sobre a rede IoT. Importante salientar que o próprio *pfSense* possui outra ferramenta para esse fim, como

Figura 26 – Exemplo de *dashboard Home Assistant*

Fonte:https://community.home-assistant.io/t/a-different-take-on-designing-a-lovelace-ui/162594

o Suricata, e no mercado existem diversos. Todavia, este projeto utilizou o SNORT em conjunto com o *pfSense*.

5.3 Protótipo Real

Nessa seção a proposta é apresentar um caso real de configuração física para o MAIOS voltado ao experimento. Após a simulação, verificamos que o projeto é totalmente factível. Embora nos testes utilizando o Laboratório GNS3 tenhamos a mesclagem de componentes externos, formando uma rede hibrida, o teste totalmente em ambiente real traz uma visão mais profunda e garantirá que o emprego do MAIOS é possível.

5.3.1 Hardware Proposto para os testes (*Switch* MAIOS)

Para a realização de testes optamos pela utilização de um computador com configurações intermediárias, superiores às recomendadas pelos softwares utilizados. A proposta nesse momento é a implementação do modelo e sua eficácia dentro dos objetivos almejados por nosso trabalho.

Um desafio posterior seria outro caso com recursos mínimos, que impactaria nas dimensões do produto e no valor final ao consumidor, todavia, o foco será a eficiência do projeto proposto.

5.3.2 Configuração Física

Para fins de replicabilidade da instalação, apresentamos as configurações utilizadas para os testes. Embora todos os softwares utilizados não exijam tantos recursos, optamos por configurações intermediárias pela capacidade do equipamento.

Como dito, as configurações da máquina escolhida são muito superiores àquelas exigências recomendadas pelo distribuidor do *pfSense* e do *Home Assistant*, as quais recomendam configurações básicas com processador de dois núcleos, 4GB de memória RAM e 20 Gb de espaço em disco.

O computador utilizado conta com as seguintes configurações:

- **Processador**: AMD Rysen 5;
- **Memória RAM**: 16 GB;
- **HD**: 256 GB;
- **Adaptadores de rede** do tipo *Ethernet-Universal Serial Bus* (USB) *chipset* RD9700;
- **Placa de rede**: *onboard chipset* RD9900;
- Demais periféricos.

A escolha do tipo de processador e adaptadores de rede impacta nas demais configurações dos recursos empregados, ou seja, ao escolher outro processador ou placa de rede é possível que seja exigida a instalação de outros *drivers*.

5.3.3 Preparação do ambiente

No ambiente de produção há que se instalar tanto o *pfSense* como o Home Assitant, em suas versões de Sistemas Operacionais, para chegarmos em um padrão próximo de nossa pretensão. Para instalar ambos em um mesmo dispositivo, optamos por utilizar a versão também de sistema operacional da VMware em sua versão 8.0 EXSi.

A instalação não ocorreu de forma tranquila, uma vez que essa versão de sistema operacional da VMware não conta com suporte de diversos tipos de drives, e em nosso projeto necessitamos do *driver* da placa de rede com chipset RTL 8118AS (Placa on board) e com o chipset RD9900 para os adaptadores de rede utilizados.

Para contornar o problema é apresentada a solução de criação de uma imagem formato ISO da instalação do software VMware EXSI modificada com os *drivers* necessários. Salienta-se que essa solução pode ser utilizada não só para inclusão de *drivers* de rede como também para outros tipos de *drivers* necessários para a solução de quaisquer problemas.

Em primeiro momento, faz-se o *download* de todos os componentes de software necessários para a solução, quais sejam:

- ❏ Imagem da instalação do VMware EXSi (https://vmware.com);
- ❏ Instalador VMware vSphere PowerCLI (https://vmare.com);
- ❏ Script Power Shell ESXi-Customizer-PS-V2.4.3.ps1 (https://www.v-front.de);
- ❏ *Drivers* de Rede (site dos fabricantes).

De posse de todos os componentes necessários, partimos para a instalação dos recursos necessários para criação de nossa versão adaptada do VMware para atendimento aos requisitos do MAIOS.

A primeira ação é instalar o *VMware vSphere PowerCLI*, que é uma espécie de uma interface de linha de comando do *Windows PowerShell*. Assim sendo, essa aplicação utiliza como base um programa *Windows* que vem instalado por padrão, para segurança, com restrição a execução de *scripts* conforme vemos na Fig. 27.

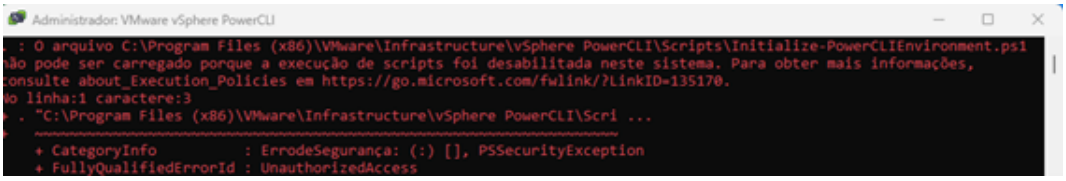


Figura 27 – Tela com informação de bloqueio de execução de *script Power Shell*

Há que se liberar a execução de *script* para continuidade da instalação, para tanto, em primeiro momento confirmamos a restrição com o comando `Get-ExecutionPolicy`, Fig. 28.

Figura 28 – Utilização do comando *Get-ExecutionPolicy Power Shell*

Ao verificar que as configurações estão restritas, executa-se o comando `Set-ExecutionPolicy`, digitando "`Unrestricted`", para desabilitar essa segurança, e confirma-se a alteração da política de segurança conforme Fig. 29.

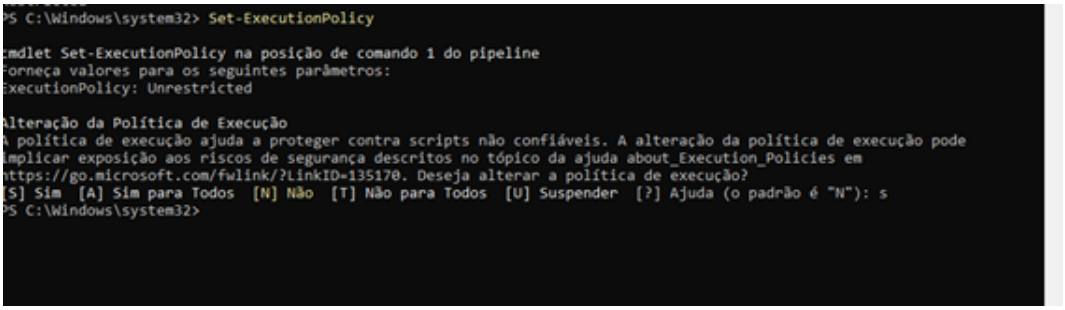


Figura 29 – Utilização do comando *Set-ExecutionPolicy Power Shell*

Após, verifica-se se realmente está sem as políticas de segurança em sua configuração de bloqueio, conforme Fig. 30.

Figura 30 – Utilização do comando *Get-ExecutionPolicy Power Shell*

Recomenda-se, que após o processo de criação da imagem personalizada retorne-se ao padrão de segurança executando o mesmo processo com a escolha da opção "`Restricted`" no lugar de "`Unrestricted`".

Após isso, o *script* `ESXi-Customizer-PS-V2.4.3.ps1`, que dará inicio à criação de uma imagem do VMware personalizada com os *drivers* necessários para reconhecimento das placas de redes, deve ser executado.

Ao executar o comando, o usuário é alertado pelo sistema de proteção sobre a execução de um *script* de terceiros. Tais execuções podem danificar o computador. Entretanto, dado que a fonte é confiável, assinala-se a opção de executar conforme Fig. 31. Neste caso executamos uma funcionalidade de ajuda presente no *script*.

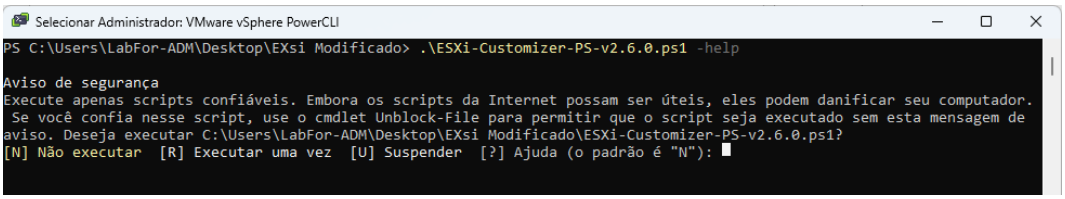


Figura 31 – Execução do *script* - *ESXi-Customizer-PS-V2.4.3.ps1*

Após execução será apresentada uma tela com todos os parâmetros utilizados, conforme mostra a Fig. 32, incluindo parâmetros adicionais.

O comando `ESXi-Customizer-PS-v2.6.0.ps1 -v60 -vft -load sata-xahci,net55-r8168` criará dentro da pasta onde o *script* é executado uma versão personalizada da instalação do VMware EXSi, conforme mostra a Fig. 31.

O passo seguinte é a instalação da VMware, que ocorre com o auxilio de um USB com funções de boot, ou seja, com instalador que se inicializa ao ligar a máquina. O ambiente VMware, após a instalação, é acessado via *Hypertext Transfer Protocol* (HTTP) e nesse momento criamos duas máquinas virtuais. A primeira com o *pfSense* e a segunda com o *Home Assitant*. A configuração dessas máquinas virtuais seguem o mesmo padrão das máquinas instaladas em nossa simulação na seção 5.1.1. A tela inicial do VMware é representada pela Fig. 33.

A diferença principal entre os ambientes simulado e real, no que tange as configurações, é a presença física das placas de rede, conforme mostra a Fig. 34, que permitirão as conexões pertinentes.

```
Administrador: VMware vSphere PowerCLI
                              [-ozip] [-pkgDir <dir>] [-outDir <dir>] [-vft] [-dpt depot1[,...]]
                              [-load vib1[,...]] [-remove vib1[,...]] [-log <file>] [-ipname <name>]
                              [-ipdesc <desc>] [-ipvendor <vendor>] [-nsc] [-test]

Optional parameters:
   -help              : display this help
   -izip <bundle>     : use the VMware Offline bundle <bundle> as input instead of the Online depot
   -update            : only with -izip, updates a local bundle with an ESXi patch from the VMware Online depot,
                        combine this with the matching ESXi version selection switch
   -pkgDir <dir>      : local directory of Offline bundles and/or VIB files to add (if any, no default)
   -ozip              : output an Offline bundle instead of an installation ISO
   -outDir <dir>      : directory to store the customized ISO or Offline bundle (the default is the
                        script directory. If specified the log file will also be moved here.)
   -vft               : connect the V-Front Online depot
   -dpt depot1[,...]  : connect additional Online depots by URL or local Offline bundles by file name
   -load vib1[,...]   : load additional packages from connected depots or Offline bundles
   -remove vib1[,...] : remove named VIB packages from the custom Imageprofile
   -sip               : select an Imageprofile from the current list
                        (default = auto-select latest available standard profile)
   -v67 | -v65 | -v60 |
   -v55 | -v51 | -v50 : Use only ESXi 6.7/6.5/6.0/5.5/5.1/5.0 Imageprofiles as input, ignore other versions
   -nsc               : use -NoSignatureCheck with export
   -log <file>        : Use custom log file <file>
   -ipname <name>
   -ipdesc <desc>
   -ipvendor <vendor> : provide a name, description and/or vendor for the customized
                        Imageprofile (the default is derived from the cloned input Imageprofile)
   -test              : skip package download and image build (for testing)
```

Figura 32 – Parâmetros opcionais do script - ESXi-Customizer-PS-V2.4.3.ps1

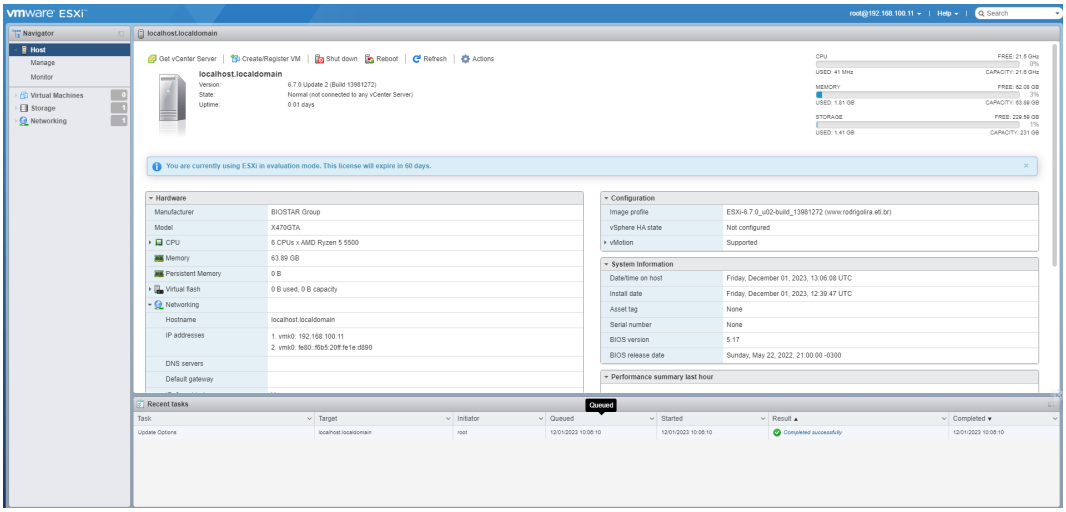


Figura 33 – Tela inicial da instalação VMware EXSi

5.3.4 Testes de Funcionalidade

A exemplo da versão simulada, o sistema real se comportou conforme o esperado. As configurações do *pfSense* e do *Home Assistant* ocorreram de maneira mais fácil e sem nenhum um tipo de adaptação. Tal facilidade se relaciona ao fato das placas de redes serem reais, pois em ambiente virtual as configurações fogem um pouco da normalidade ainda que não tenha grandes complicações.

O *pfSense* é um software consolidado no mercado, presente em grandes empresas, e a forma de emprego no MAIOS segue a mesma linha daquela utilizada em ambientes corporativos, qual seja, um servidor com máquina virtual integrada e o *pfSense* fazendo todo o controle.

A segmentação de rede física, notadamente implementadas pelos adaptadores de redes configurados em interfaces diferentes no *pfSense*, se mostrou satisfatória. Dessa forma

Figura 34 – Adaptadores RJ45-USB

temos a certeza do desacoplamento, o que em simulação pode não ser bem compreendido. Cada dispositivo conectado na interface a que pertence assume as configurações impostas por servidor DHCP específico.

A interface responsável pela especificidade propiciada pela ideia do MAIOS corresponde ao objetivo principal de segurança em IoT. De maneira nativa, é a única interface que contará com total controle de pacotes e monitoramento de intrusão com o suporte do *plugin* SNORT presente em nossa instalação. A interoperabilidade é fornecida na rede graças ao servidor *Home Assistant*. Como podemos observar no estudo, a existência de arquiteturas com padrões heterogêneos e aplicações com fornecedores de nuvem específicos criam uma fragmentação que limita as soluções de IoT. Em nossa abordagem conseguimos identificar dispositivos de marcas distintas, sendo dos fabricantes *Sonoff* e *Tuya*.

Para a implantação do SNORT, empregado para IDS e IPS, utilizamos as regras advindas das comunidades, entretanto, foi possível verificar a possibilidade de criação de regras próprias e o consumo de regras de terceiros. Nesse sentido, no futuro podemos implementar novas condicionantes que visariam a melhora nesses quesitos.

5.4 Resiliência a Ataques

A principal ferramenta utilizada foi uma versão modificada do Linux voltada para testes de invasão e penetração (pentest) entre outras. Para tanto, instalamos uma máquina virtual com o Kali Linux que atende aos propósitos deste tópico.

Importante destacar que os testes ocorreram em ambiente controlado, ou seja, tanto em laboratório (hibrido) quanto em configuração real, que em ambos os casos estavam apartados de qualquer rede em produção.

Dentre funcionalidades do Kali Linux exploramos a *Network Mapper* (Nmap), como funcionalidade de escaneamento da rede, identificando todos os dispositivos presentes na

rede com seus respectivos endereços IPs. O Nmap listou apenas os dispositivos conectados na rede, onde o servidor Kali foi instalado. Durante esse teste, o SNORT precisou ser desativado, pois estava bloqueando a ação do teste. Tal recurso é adotado tanto para testes de penetração como por criminosos em busca de brechas de segurança, deste modo, o SNORT ao identificar sua ação bloqueava o computador de origem em nossa configuração.

Com esse resultado, verificamos a efetividade da segmentação de portas, um de nossos objetivos principais e de igual forma a potencialidade da ferramenta em prevenir essa busca de brechas em nossa rede, como portas abertas, por exemplo.

Para testar a interoperabilidade do sistema, instalamos dispositivos de fabricantes distintos, o que foi possível com o servidor *Home Assistant*. Não foi possível perceber diferenças entre a o servidor instalado em nossa simulação e o ambiente real.

Ao transpor as simulações para o ambiente real do protótipo, replicamos os mesmos cenários, para verificar se o MAIOS mantinha sua eficácia na detecção e resposta. Essa transição para um ambiente físico proporcionou uma compreensão mais holística da resiliência do sistema, considerando variáveis do mundo real.

5.5 Resultados Parciais

A análise comparativa entre os resultados da simulação e os obtidos no protótipo revelou, conforme esperado, grandes semelhanças. Tal fato se deve a dinâmica do laboratório criado no GNS3, onde se buscou, a máxima compatibilidade com o mundo real. Pela melhor capacidade de processamento e memória, além de serviços dedicados, o ambiente real se mostrou mais rápido.

Com base nos testes de resiliência e nos resultados comparativos, a solução MAIOS demonstrou eficiência na segregação da rede e na defesa de ataques presentes na *Snort gplv2 community rules*.

A conclusão parcial é que o MAIOS se mostrou promissor e conseguirá cumprir seus objetivos. As regras da comunidade no que tange ao uso do SNORT não são suficientes para uma heterogeneidade de dispositivos, entretanto a possibilidade de criar novas regras personalizadas e atualizar a lista de maneira rápida é um diferencial atraente e indispensável.

Capítulo 6

Conclusão

Este capítulo apresenta as conclusões a respeito deste trabalho de pesquisa. A seção 6.1 mostra as principais contribuições. Na seção 6.2 são apresentadas algumas possibilidades de trabalhos futuros, que poderão ser desenvolvidos em continuidade desta pesquisa. E, por fim, a seção 6.3 lista a contribuição bibliográfica fruto deste trabalho de pesquisa até o momento.

6.1 Principais Contribuições

Considerando a crescente preocupação com a segurança de IoT em ambientes domésticos e corporativos, esta pesquisa buscou oferecer uma solução funcional para essa questão. Ao longo deste estudo, foram delineados objetivos específicos, desde a pesquisa bibliográfica, para entender o estado da arte do tema, até o desenvolvimento de um modelo conceitual e funcional do projeto, a análise da viabilidade e a avaliação dos resultados.

As contribuições deste trabalho para a comunidade e o desenvolvimento da tecnologia são podem ser significativas, uma vez que este projeto deixa um legado plenamente aplicável. Primeiramente, a pesquisa bibliográfica realizada representou uma revisão abrangente do conhecimento existente sobre segurança de dispositivos de IoT, fornecendo um panorama do estado atual da tecnologia e das práticas recomendadas. Além disso, o desenvolvimento de um modelo conceitual e funcional oferece uma contribuição prática para a implementação de soluções de segurança mais eficazes para a integração de dispositivos pessoais à infraestrutura de rede corporativa.

As soluções apresentadas estão presentes no mercado, principalmente no que tange ao uso empresarial. O uso de *firewall* robusto e segmentação de rede já são premissas em segurança de rede ou cibersegurança, entretanto, em ambiente doméstico isso não é pensado, seja pela impressão de não relevância do ponto de conexão ou pelos custos elevados em executar tais medidas de segurança. Junta-se a isso, a crescente busca por comodidades alcançáveis por IoT e falta de soluções voltadas para o propósito da segurança dessa nova malha na rede, neste caso, até em ambiente corporativo.

No que tange a interoperabilidade, outro objetivo almejado, pode-se observar pelos experimentos que se trata de algo plenamente capaz. O *Home Assistant* já é integrável a um ampla gama de dispositivos e essa lista é crescente à medida que novos vão surgindo e funcionou bem em nosso modelo.

O estudo buscou demonstrar a possibilidade de proteção desse grupo vulnerável de dispositivos, que em premissa, não conseguem se proteger sozinhos, visto suas configurações limitadas e seus objetivos. A contribuição desse trabalho é justamente o entendimento de que é possível a proteção da rede, principalmente dessa parte vulnerável, sem o emprego de grandes recursos e com o mínimo de conhecimento. A abordagem pretendida, que se mostrou viável, é um ecossistema *plug and player*, ou seja, não necessita de conhecimentos técnicos avançados para sua implementação e faz uso de soluções confiáveis.

Os resultados alcançados neste estudo têm o potencial de impactar positivamente a comunidade, especialmente no que diz respeito à adoção de medidas proativas para garantir a segurança da informação em um cenário de crescente conectividade. A simulação da ideia MAIOS já evidenciou a potencialidade do sistema e a transposição para o ambiente real só atestou o que conseguimos ver. A pesquisa fornece *insights* valiosos que podem orientar práticas de segurança mais robustas e eficientes.

Algumas limitações que acreditamos ser contornáveis no futuro, fizeram com que evoluíssemos no trabalho ao romper desafios que se mostraram complicados. Em primeiro momento a abordagem hibrida com IoT na simulação não dispunha de acervo de pesquisa, ou seja, o desenvolvimento teve de ser realizado com base em conhecimento próprio e percepções em abordagens utilizadas para outras finalidades.

A transposição do ambiente virtual para o real, com os recursos utilizados, não foram as melhores escolhas, mas, a certeza de que era necessário contribuiu para o aprendizado de outras soluções, como a inclusão de *drivers* em instalações via imagens de sistemas baseados em Linux. O virtualizador empregado, por escolha da fabricante, não adotava nativamente os drives das placas de rede que utilizávamos.

Um dos propósitos do MAIOS em sua camada *Controller* é prover o sistema com atualizações que possam ser retroalimentadas com base em informações dos sistemas instalados. Seja na atualização das regras para o sistema de detecção e prevenção a intrusão ou na atualização das assinaturas dos IoT de novos protocolos ou fabricantes. No presente trabalho não focamos nessas atualizações, mas com o entendimento que é plenamente possível. No modo atual, isso é delegado aos componentes de software utilizados.

Com nossa proposta buscamos oferecer uma experiência integrada e acessível, onde o usuário não precisa compreender detalhes técnicos complexos para manter sua rede segura. Essa abordagem visa democratizar o acesso a soluções de segurança cibernética robustas, tanto em ambientes domésticos quanto corporativos.

Em resumo, a presente dissertação contribui para o avanço da segurança da IoT,

oferecendo um modelo e *insights* relevantes que podem formar decisões e práticas tanto no ambiente corporativo quanto doméstico. Espera-se que este trabalho não apenas reflita o esforço dedicado, mas também represente uma contribuição significativa para o campo de conhecimento, alinhado com a citação inspiradora de Alan Turing: "Eu acredito que às vezes são as pessoas que ninguém espera nada que fazem as coisas que ninguém consegue imaginar". Parafraseando Turing, com base no entendimento advindo deste trabalho, acredito que às vezes soluções simples podem trazer grandes resultados.

6.2 Trabalhos Futuros

Como trabalho futuro, pode-se visionar a integração de todos os recursos do MAIOS em um único sistema operacional focado na orientação de rede em IoT. Todos os recursos empregados são advindos de versões modificadas do sistema operacional LINUX, logo, prover o mundo com o sistema operacional MAIOS, um *branch* baseado em LINUX, que contará com segmentação de rede, proteção e prevenção a ataques e contará com uma camada controle baseada no aprendizado de máquina com compartilhamento do conhecimento.

Em conjunto ao trabalho a ser desenvolvido, planejamos o recorte de temas específicos para confecção de artigos relevantes na gama de assuntos tratados nesse trabalho, com potencial de fornecer novas perspectivas no cenário tecnológico mundial.

6.3 Contribuições em Produção Bibliográfica

O presente trabalho deu origem a um artigo submetido a *Industrial Electronics Society* (IEEE) na *33rd IEEE International Symposium on Industrial Electronic*s (ISIE): **MAIOS: *A Multi Accountability IoT Oriented Switch***, a ser realizado no período de 18 a 21 de junho na cidade de Ulsan na Coréia do Sul. O referido simpósio tem foco em tecnologias de ponta para indústrias, aplicações de eletrônica, controles, comunicações, instrumentação e inteligência computacional. Conforme o site do evento, o ISIE tem como foco as tecnologias de ponta para indústrias, como eletrônica, controle, comunicações, instrumentação e inteligência artificial. Em 06 de maio de 2024 o artigo submetido recebeu notificação de aceitação. É importante salientar que o evento possui extrato A3 na avaliação da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes).

Referências

AELA. Trabalho remoto: Quais as perspectivas durante e pós-pandemia? 2021. Disponível em: <https://aelaschool.com/pt/carreira/trabalho-remoto-quais-as-perspectivas-durante-e-pos-pandemia>. Acesso em: 28.9.2023.

AFONSO Ícaro. **A arquitetura da Internet das Coisas**. 2020. Disponível em: <https://www.zup.com.br/blog/a-arquitetura-da-internet-das-coisas>. Acesso em: 20 mai 2021.

ANDRADE, V. de. A evolução da tecnologia: da descoberta do fogo à inteligência artificial. 2019. Disponível em: <https://www.tecnoveste.com.br/a-evolucao-da-tecnologia-da-descoberta-do-fogo-a-inteligencia-artificial/>. Acesso em: 14.9.2023.

ANIL, K. Open source implementation of internet of things as a network of intranet of things. p. 215–218, 2016. https://doi.org/10.1109/INCITE.2016.7857619.

BATISTA, S. S. dos S.; FREIRE, E. Sociedade e tecnologia na era digital. In: _____. **Sociedade e Tecnologia na Era Digital**. São Paulo: Editora Saraiva, 2014. p. 37. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788536522531>. Acesso em: 17.9.2023.

BOLZANI, C. A. M. **Residências Inteligentes**. São Paulo: Livraria da Física, 2004.

BRASIL. Constituição da república federativa do brasil de 1988. 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 28.9.2023.

BRORING et al. Habilitando ecossistemas de iot por meio da interoperabilidade da plataforma. **IEEE Acess**, v. 34, n. 1, p. 54–61, 2017.

CAMILO, K. Democratização do acesso à tecnologia. 2019. Disponível em: <https://irisbh.com.br/democratizacao-do-acesso-a-tecnologia/>. Acesso em: 9.9.2023.

CASADO, M. et al. Ethane: taking control of the enterprise. **ACM SIGCOMM Computer Communication Review**, ACM New York, NY, USA, v. 37, n. 4, p. 1–12, 2007. https://doi.org/10.1145/1282427.1282382.

CASTELLS, M. **A Sociedade em Rede**. 6. ed. [S.l.]: Zahar, 1999. v. 1.

CNI. Indústria 4.0: Entenda seus conceitos e fundamentos. 2020. Disponível em: <https://www.portaldaindustria.com.br/industria-de-a-z/industria-4-0/#tecnologias>. Acesso em: 9.9.2023.

COSTA, P. P. da. **Teoria de Grafos e suas Aplicações**. 69 f. Tese (Mestrado em Matemática Universitária) — Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas, Rio Claro, 2011.

DALLAQUA, C. Origem da teoria dos grafos – as 7 pontes de konigsberg. **Universo Racionalista**, 2016. Disponível em: <https://universoracionalista.org/origem-da-teoria-dos-grafos-as-7-pontes-de-konigsberg/>. Acesso em: 15.9.2023.

DINI, P. et al. Privacy-preserving defense: Intrusion detection in iot using federated learning. In: **Proceedings of the IEEE MELECON 2024 Conference**. [S.l.: s.n.], 2024. Forthcoming.

ECKER, A. Sem leitos de uti, nove pacientes com covid-19 perderam a vida nas últimas semanas na serra. 2021. Disponível em: <https://gauchazh.clicrbs.com.br/pioneiro/geral/noticia/2021/03/sem-leitos-de-uti-nove-pacientes-com-covid-19-perderam-a-vida-nas-ultimas-semanas-na-serra-ckm56eq8l html>. Acesso em: 22.9.2023.

ECOA. O que significa "democratização"? 2019. Disponível em: <https://www.uol.com.br/ecoa/listas/o-que-e-democratizacao.htm>. Acesso em: 14.9.2023.

FERREIRA, L. E.; CALIXTO, V. L. Desigualdade educacional no brasil é agravada pela pandemia. 2021. Disponível em: <https://sites.ufop.br/lamparina/blog/desigualdade-educacional-no-brasil-%C3%A9-agravada-pela-pandemia>. Acesso em: 28.9.2023.

GERBELLI, L. G.; MELO, L. Consumo de novas tecnologias ajuda a manter inflação baixa. 2020. Disponível em: <https://g1.globo.com/economia/noticia/2020/02/13/consumo-de-novas-tecnologias-ajuda-a-manter-inflacao-baixa.ghtml>. Acesso em: 22.9.2023.

GODOI, M. G. D.; AND, L. S. de A. A internet das coisas: evolução, impactos e benefícios. 2018. Disponível em: <https://revista.fatectq.edu.br/interfacetecnologica/article/download/538/363>. Acesso em: 28.9.2023.

GOULARTE, A. O novo perfil de aluno: quem são os nativos digitais? 2022. Disponível em: <https://blog.flexge.com/nativos-digitais-novo-perfil-alunos/#:~:text=Nativo%20digital%20foi%20o%20nome,contato%20direto%20com%20a%20tecnologia.> Acesso em: 10.9.2023.

GUDE, N. et al. Nox: towards an operating system for networks. **ACM SIGCOMM Computer Communication Review**, ACM New York, NY, USA, v. 38, n. 3, p. 105–110, 2008. https://doi.org/10.1145/1384609.1384625.

GUEDES, D. et al. Redes definidas por software: uma abordagem sistemica para ^ o desenvolvimento das pesquisas em redes de computadores. 2012. Disponível em: <https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/minicurso-sdn.pdf>. Acesso em: 19.9.2023.

HODGES, C. et al. The difference between emergency remote teaching and online learning. 2020. Disponível em: <https://er.educause.edu/articles/2020/3/the-difference-between-emergency-remote-teaching-and-online-learning#fn3>. Acesso em: 28.9.2023.

IBGE. Informações atualizadas sobre tecnologias da informação e comunicação. 2021. Disponível em: <https://educa.ibge.gov.br/jovens/materias-especiais/21581-informacoes-atualizadas-sobre-tecnologias-da-informacao-e-comunicacao.html>. Acesso em: 10.9.2023.

INDELMAR. O que é mqtt? 2017. Disponível em: <https://www.indelmar.com/?p=1140>. Acesso em: 10.9.2023.

IT, S. Internet das coisas: entenda o que é e veja exemplos de suas aplicações. 2017. Disponível em: <https://medium.com/system-it-solutions/internet-das-coisas-o-que-e-exemplos-b82855d1a969>. Acesso em: 10.9.2023.

KENSKI, V. M. **Tecnologias e ensino presencial e a distância**. 9rd. ed. Campinas-SP: Papirus, 2012.

KUMAR, P.; TRIPATHI, R.; GUPTA, G. P. P2idf: A privacy-preserving based intrusion detection framework for software-defined internet of things-fog (sdiot-fog). In: **Adjunct Proceedings of the 2021 International Conference on Distributed Computing and Networking**. [S.l.: s.n.], 2021. p. 37–42. https://doi.org/10.1145/3427477.3429989.

LEVINE, J. R.; YOUNG, M. L. Evolution of software-defined networkin. 2011. Disponível em: <https://www.vmware.com/learn/49566_REG.html?touch=1&src=WWW_us_ELQ_CVQ8TU2rKyGwXFRqDn9l&int_cid=7012H000001oi80>. Acesso em: 28.9.2023.

LEVY, P. **A Inteligência Coletiva: por uma Antropologia do Ciberespaço**. 3rd. ed. São Paulo: Edições Loyola, 2000.

LIMA, C. Elementos da comunicação. **Educa + Brasil**, 2019. Disponível em: <https://www.educamaisbrasil.com.br/enem/lingua-portuguesa/elementos-da-comunicacao>. Acesso em: 15.9.2023.

MACEDO, F. L. **Arquitetura da Informação: aspectos espistemológicos, científicos e práticos.** Dissertação (Dissertação de Mestrado) — Universidade de Brasília, 2005.

MATZA, M.; YONG, N. Chefe do fbi diz que vírus da covid 'provavelmente' escapou de laboratório chinês. 2023. Disponível em: <https://g1.globo.com/saude/noticia/2023/03/01/chefe-do-fbi-diz-que-virus-da-covid-provavelmente-escapou-de-laboratorio-chines.ghtml>. Acesso em: 22.9.2023.

MELO, P. H. A. D. de. **FamilyGuard: Uma Arquitetura de Segurança para Detecção de Anomalias em Redes Domésticas**. Tese (Doutorado) — Universidade Federal de Uberlândia (UFU), 2023. Tese de Doutorado.

MOLINOS, D. N. **NEA: Arquitetura de Elemento de Rede SDN com Suporte a MAC Definido pela Aplicação**. Tese (Doutorado) — Universidade Federal de Uberlândia (UFU), 2024. Tese de Doutorado.

MOTA, M. M. P. E. da; SILVA, C. L. M. da. Ensino remoto na pandemia. In: _____. Curitiba-PR: Appris, 2023. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 28.9.2023.

MOUSTAFA, N.; SLAY, J. Unsw-nb15: A comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). In: **2015 Military Communications and Information Systems Conference (MilCIS)**. [S.l.: s.n.], 2015. p. 1–6. https://doi.org/10.1109/MilCIS.2015.7348942.

NITAHARA, A. Estudo mostra que pandemia intensificou uso das tecnologias digitais. 2021. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2021-11/estudo-mostra-que-pandemia-intensificou-uso-das-tecnologias-digitais>. Acesso em: 28.9.2023.

OLIVEIRA, R. D. **Um novo método de acesso ao meio baseado em Workspaces para suporte a arquiteturas de Internet do Futuro implementado em FPGA**. 149 f. Tese (Doutorado em Ciência da Computação) — Universidade Federal de Minas Gerais, Uberlândia-MG, 2019.

ONU. Declaração universal dos direitos humanos. 1948. Disponível em: <https://www.unicef.org>. Acesso em: 28.9.2023.

OPAS. Coronavirus. 2019. Disponível em: <https://www.paho.org/pt/topicos/coronavirus?adgroupsurvey={adgroupsurvey}&gclid=CjwKCAjwseSoBhBXEiwA9iZtxoFG9v9baW1KJS_qebgttQuUN6iRJ0pZ_iNq6OumGpF2GpM9oiUk3RoCvNwQAvD_B>. Acesso em: 22.9.2023.

RIBEIRO, U. Firewall pfsense: o que é, vantagens e como instalar o software. 2022. Disponível em: <https://www.certificacaolinux.com.br/firewall-pfsense/>. Acesso em: 28.9.2023.

RONAN, C. A. **História Ilustrada da Ciência - Volume 1**. [S.l.]: Zahar, 1987.

SACCOL, A. I. da C. Z.; SCHLEMMER, E.; BARBOSA, J. M-learning e u-learning: novas perspectivas da aprendizagem móvel e ubíqua. In: _____. 1rd. ed. São Paulo-SP: Pearson, 2021. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 01.10.2023.

SACOMANO, J. et al. **Indústria 4.0: conceitos e fundamentos**. Blucher, 2018. ISBN 9788521213703. Disponível em: <https://books.google.com.br/books?id=1EwLvgEACAAJ>.

SANTOS, B. P. et al. Mobile matrix: Routing under mobility in iot, iomt, and social iot. 2018. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S1570870518302415>. Acesso em: 28.9.2023.

SCHWAB, K. **A Quarta Revolução Industrial**. [S.l.]: Edipro, 2016.

SENA, G. C. C. **MONITORAMENTO DE VARIANTES DO SARS-COV-2 E DA MANIFESTAÇÃO CLÍNICA DA COVID-19 EM BETIM – MINAS GERAIS**. 73 f. Tese (Mestrado em Genética) — Universidade Federal de Minas Gerais, Belo Horizonte-MG, 2023.

SHAFIQUE, K. et al. Internet of things (iot) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5g-iot scenarios. **IEEE Access**, v. 8, p. 23022–23040, 2020. https://doi.org/10.1109/ACCESS.2020.2970118.

SILVA, E. B. et al. Automação e sociedade: quarta revolução industrial, um olhar para o brasil. In: _____. **Histórias da informática na América Latina**. 1rd. ed. Rio de Janeiro: Brasport, 2018. p. 8. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 17.9.2023.

SINHA, S. Estado da iot 2023: Número de dispositivos iot conectados crescendo 162023. Disponível em: <https://iot-analytics.com/number-connected-iot-devices/>. Acesso em: 28.9.2023.

TANENBAUM, A.; FEAMSTER, N.; WETHERALL, D. Redes de computadores. In: _____. 6rd. ed. São Paulo-SP: Grupo A, 2021. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 01.10.2023.

VILACA, M. L. C.; ARAUJO, E. V. F. de. **Tecnologia, Sociedade e Educação na Era Digital**. Duque de Caxias-RJ: UNIGRANDERIO, 2016.

YANGYANG, G. O que é openflow? 2021. Disponível em: <https://info.support.huawei.com/info-finder/encyclopedia/en/OpenFlow.html>. Acesso em: 25.9.2023.