

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS

GABRIELLA BARBUTTI

ANÁLISE DE VULNERABILIDADES E AMEAÇAS EM
REDES IOT CORPORATIVAS

CAMPINAS
2023

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS
ESCOLA POLITÉCNICA
PROGRAMA DE PÓS-GRADUAÇÃO EM GESTÃO DE
REDES DE TELECOMUNICAÇÕES

GABRIELLA BARBUTTI

ANÁLISE DE VULNERABILIDADES E AMEAÇAS
EM REDES IOT CORPORATIVAS

Dissertação apresentada como exigência para obtenção do título de Mestre em Gestão de Redes de Telecomunicações ao Programa de Pós-Graduação em Gestão de Redes de Telecomunicações da Escola Politécnica. Área de Concentração: Gestão de Redes e Serviços.

Orientador (a): Profa. Dra. Lia Toledo Moreira Motta.

CAMPINAS

2023

Ficha catalográfica elaborada por Adriane Elane Borges de Carvalho CRB 8/9313
Sistema de Bibliotecas e Informação - SBI - PUC-Campinas

006.22 Barbutti, Gabriella
B241a

Análise de vulnerabilidades e ameaças em redes IoT corporativas / Gabriella Barbutti. - Campinas: PUC-Campinas, 2023.

106 f.

Orientador: Lia Toledo Moreira Mota.

Dissertação (Mestrado em Gestão de Redes de Telecomunicações) - Programa de Pós-Graduação em Gestão de Redes de Telecomunicações, Escola Politécnica, Pontifícia Universidade Católica de Campinas, Campinas, 2023.

Inclui bibliografia.

1. Internet das coisas. 2. Informática - Interfaces (Computador). 3. Comunicação e tecnologia - Inovações tecnológicas. I. Mota, Lia Toledo Moreira. II. Pontifícia Universidade Católica de Campinas. Escola Politécnica. Programa de Pós-Graduação em Gestão de Redes de Telecomunicações. III. Título.

23. ed. CDD 006.22

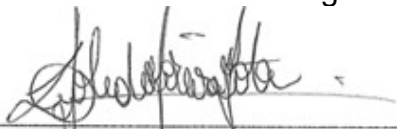
GABRIELLA BARBUTTI

**ANÁLISE DE VULNERABILIDADES E AMEAÇAS EM
REDES IOT CORPORATIVAS**

Dissertação apresentada como exigência para obtenção do título de Mestre em Gestão de Redes de Telecomunicações ao Programa de Pós-Graduação em Gestão de Redes de Telecomunicações da Escola Politécnica. Área de Concentração: Gestão de Redes e Serviços.

Orientador (a): Profa. Dra. Lia Toledo Moreira Motta.

Dissertação defendida e aprovada em 27 de junho de 2023 pela Comissão Examinadora constituída dos seguintes professores:



Profa. Dra. Lia Toledo Moreira Motta

Orientadora da Dissertação e Presidente da Comissão Examinadora

Pontifícia Universidade Católica de Campinas



Prof. Dr. Marcius Fabius Henriques de Carvalho
Pontifícia Universidade Católica de Campinas



Profa. Dra. Renata Rampim
RF Consulting

AGRADECIMENTOS

Essa conquista não seria possível sem o apoio da minha orientadora Profa. Dra. Lia Moreira Mota, sua sabedoria, paciência, maestria, foram fundamentais para o meu crescimento acadêmico e pessoal.

A PUC-Campinas pelo fornecimento da Bolsa de Estudos e todos os meios e condições que colocou a minha disposição para realização desta pesquisa de mestrado.

Ao meu marido, Ricardo Marques, sua presença, compreensão e apoio foram fundamentais para que eu me dedicasse ao mestrado e concluísse essa etapa com sucesso, me encorajando a persistir, lembrando do meu potencial e celebrando cada pequena vitória.

Aos meus pais Cristina e Orlando e meus avós Thereza e Nelson, que desde o início foram meu porto seguro, me apoiando incondicionalmente em cada etapa dessa jornada acadêmica. Todo incentivo e encorajamento me deram forças para superar os desafios, enfrentar os obstáculos e continuar persistindo nos meus sonhos.

RESUMO

A evolução dos meios de comunicação alterou o padrão de vida das pessoas, empresas podem ampliar sua cobertura, seu monitoramento e serviços com as tecnologias que a cada dia ampliam horizontes para melhoria da comunicação. Equipamentos com interfaces de rede, passam a vincular objetos físicos do dia a dia a Internet, aumentando assim a popularidade e gamificação da Internet das Coisas (IoT). O Objetivo principal por traz de todo este progresso é simplificar a vida das pessoas, empresas e evolução humana com custo acessível e poder de processamento limitado, esses dispositivos semiautônomos vem causando preocupações quanto a suas ameaças e vulnerabilidades, mediante aos órgãos de Segurança Cibernética mundial. Este trabalho tem como objetivo analisar as principais vulnerabilidades e ameaças em redes IoT corporativas e domésticas, com objetivo de classificar essas vulnerabilidades e ameaças quanto a seu impacto nas redes mencionadas. Nessa classificação, serão considerados impactos técnicos, econômicos e as especificidades das redes corporativas e domésticas. A metodologia será baseada no envio de um questionário, visando elencar, junto a um grupo de especialistas da área de Tecnologia da Informação, na região de Campinas/SP, as principais fragilidades dessas redes, especialmente nos ambientes de trabalho que efetivamente sofrem com tais ameaças, com foco nas práticas utilizadas por atacantes, que visam explorar desde a degradação dos serviços de um dispositivo até o sequestro dos dados ou acessos. A partir das informações coletadas na pesquisa, será realizada a classificação das vulnerabilidades e ameaças, utilizando o Método SAW – Método de Ponderação Aditiva Simples. Como resultados, espera-se, além da classificação das vulnerabilidades e ameaças em redes IoT corporativas e residenciais, a proposição de um modelo de segurança para essas redes, que possa colaborar para a proteção dos dispositivos e informações que compõem essas redes, tornando-as menos vulneráveis e susceptíveis a ameaças.

Palavras-chave: Internet das Coisas, Segurança da Informação, Método SAW.

ASBTRACT

The evolution of the means of communication has changed people's standard of living, companies can expand their coverage, monitoring and services with technologies that expand horizons every day to improve communication. Devices with network interfaces start to link everyday physical objects to the Internet, thus increasing the popularity and gamification of the Internet of Things (IoT). The main objective behind all this progress is to simplify the lives of people, companies and human evolution with affordable cost and limited processing power, these semi-autonomous devices have been causing concerns about their threats and vulnerabilities, through cybersecurity agencies worldwide. This work aims to analyze the main vulnerabilities and threats in corporate and domestic IoT networks, to classify these vulnerabilities and threats in terms of their impact on the networks. In this classification, technical and economic impacts and the specificities of corporate and domestic networks will be considered. The methodology will be based on sending a questionnaire, aiming to list, together with a group of specialists in Information Technology, in the region of Campinas/SP, the main weaknesses of these networks, especially in work environments that effectively suffer from such threats., focusing on the practices used by attackers, who aim to exploit everything from the degradation of a device's services to the hijacking of data or access. From the information collected in the research, the classification of vulnerabilities and threats will be carried out, using the SAW Method – Simple Additive Weighting Method. As a result, it is expected, in addition to the classification of vulnerabilities and threats in corporate and residential IoT networks, the proposition of a security model for these networks, which can collaborate to protect the devices and information that make up these networks, making them less vulnerable and susceptible to threats.

Keywords: Internet of Things, Information Security, SAW Method.

LISTA DE FIGURAS

FIGURA 1: TOTAL DE INCIDENTES REPORTADOS POR ANO, FONTE: (CERT, 2022).....	11
FIGURA 2: PRINCIPAIS PORTAS QUE SOFRERAM VARREDURAS E OUTROS ATAQUES, FONTE: (CERT, 2023).	12
FIGURA 3: ESQUEMA DA ONTOLOGIA DE SEGURANÇA DA INFORMAÇÃO.....	20
FIGURA 4: AGENTES DE AMEAÇAS E AS VULNERABILIDADES DE SEGURANÇA. FONTE: ADAPTADO DE (OWASP, 2013).	21
FIGURA 5: MATRIZ NÃO NORMALIZADA.	49
FIGURA 6: MATRIZ NORMALIZADA.	50
FIGURA 7: PRINCIPAIS PASSOS DA METODOLOGIA PROPOSTA.	52
FIGURA 8: FORMULÁRIO CONCEDIDO PARA OS ESPECIALISTAS.....	54
FIGURA 9: FLUXO PARA CAPTAÇÃO DAS RESPOSTAS DOS ESPECIALISTAS.	54
FIGURA 10: RESPOSTAS DOS ESPECIALISTAS.	56
FIGURA 11: CRITÉRIOS E ALTERNATIVAS PARA APLICAÇÃO DO MÉTODO SAW.	57
FIGURA 12: MATRIZ NORMALIZADA.	57
FIGURA 13: DETERMINAÇÃO DO RANKING DAS VULNERABILIDADES.....	58
FIGURA 14: MATRIZ DE COMPARAÇÃO CONSIDERANDO PESOS IGUAIS PARA TODOS OS CRITÉRIOS.	59
FIGURA 15: MATRIZ DE COMPARAÇÃO CONSIDERANDO PESO MAIOR PARA O CRITÉRIO FREQUÊNCIA DE OCORRÊNCIA.	59
FIGURA 16: MATRIZ DE COMPARAÇÃO CONSIDERANDO PESO MAIOR PARA O CRITÉRIO IMPACTO DE DEGRADAÇÃO DE REDE. 60	
FIGURA 17: MATRIZ DE COMPARAÇÃO CONSIDERANDO PESO MAIOR PARA O CRITÉRIO IMPACTO FINANCEIRO.	61
FIGURA 18: MATRIZ DE COMPARAÇÃO CONSIDERANDO PESO MAIOR PARA O CRITÉRIO IMPACTO DE QUEDA DE REDE.	61
FIGURA 19: MATRIZ DE COMPARAÇÃO CONSIDERANDO PESOS FORNECIDOS PELOS ESPECIALISTAS.	62
FIGURA 20: RANKING PARA O CENÁRIO 1.	63
FIGURA 21: RANKING PARA O CENÁRIO 2.	65
FIGURA 22: RANKING PARA O CENÁRIO 3.	66
FIGURA 23: RANKING PARA O CENÁRIO 4.	67
FIGURA 24: RANKING PARA O CENÁRIO 5.	69
FIGURA 25: RANKING PARA O CENÁRIO 6.	70
FIGURA 26: ÍNDICE DE CRITICIDADE DAS VULNERABILIDADES.....	72

LISTA DE TABELAS

TABELA 1: PRINCIPAIS MÉTODOS MULTICRITÉRIO.....	47
TABELA 3: ÍNDICE DE CRITICIDADE PARA AS 9 VULNERABILIDADES.....	72

SUMÁRIO

1. INTRODUÇÃO	10
1.1 Justificativa para o Desenvolvimento do Trabalho.....	12
1.2 Objetivo Geral	13
2. REDES IOT.....	15
2.1. Protocolo de Comunicação	16
2.2 Segurança da Informação	17
2.3. Segurança em Redes IoT.....	21
2.4. A Legislação com a Segurança da Informação	23
3. VULNERABILIDADES E AMEAÇAS EM UMA REDE IOT	25
3.1 Vulnerabilidades	25
3.1.1. Senhas Frágeis de Fácil Decodificação	25
3.1.2. Serviços de Interface de Redes Inseguros.....	27
3.1.3. Falta de Mecanismo de Atualização Seguro	28
3.1.4. Uso de Componentes Inseguros ou Desatualizados.....	30
3.1.5. Proteção de Privacidade Insuficiente	32
3.1.6. Transferência e Armazenamento de Dados Inseguros	33
3.1.7. Falta de Gerenciamento de Dispositivos	35
3.1.8. Configuração Padrão de Conta	37
3.1.9. Falta de <i>Hardening</i> Físico	40
3.2 Ameaças	42
3.2.1. Frequência de Ocorrência	42
3.2.2. Impacto de Degradação de Rede.....	43
3.2.3. Impacto Financeiro	43
3.2.4. Impacto de Queda de Rede	44

4. MÉTODOS MULTICRITÉRIO PARA A TOMADA DE DECISÃO.....	45
4.1 Tipos de Métodos Multicritério para Tomada de Decisão	45
4.2 Método SAW (Método de Ponderação Aditiva Simples).....	49
5. METODOLOGIA	52
5.1 Considerações Sobre a Pesquisa.....	53
5.2 Definições das Alternativas e Critérios	53
5.3 Formulário Fornecido aos Especialistas	53
5.4 Aplicação do Método SAW e Coleta de Dados.....	56
5.5 Cenários Avaliados	58
6. RESULTADOS.....	63
6.1 Resultado do Cenário 1 – Caso Base.....	63
6.2 Resultado do Cenário 2 – Frequência de Ocorrência	64
6.3 Resultado do Cenário 3 – Impacto de Degradação de Rede.....	65
6.4 Resultado do Cenário 4 – Impacto Financeiro	67
6.5 Resultado do Cenário 5 – Impacto de Queda de Rede	69
6.6 Resultados do Cenário 6 – Pesos Definidos Pelos Especialistas.....	70
7. ANÁLISE E DISCUSSÕES	71
7.1 Mitigação das Principais Vulnerabilidades.....	73
7.2 Mitigação de vulnerabilidade – Falta de mecanismo de atualização seguro 74	
7.3 Mitigação de vulnerabilidade – Proteção de privacidade insuficiente	75
7.4 Mitigação de vulnerabilidade – Senhas frágeis de fácil decodificação.....	77
8. CONCLUSÃO	79
REFERÊNCIAS.....	80
APÊNDICES.....	88

1. INTRODUÇÃO

A Internet das Coisas (Internet of Things - IoT) é uma rede de objetos interconectados, dispositivos eletrônicos, que possuem capacidade de processamento, coleta e transmissão de dados. À medida que o conceito IoT promove a integração de tecnologias e equipamentos onde cada objeto inteligente passa a ser capaz de interações uns com os outros, a sociedade passa a consumir informações sobre estes dispositivos e isso inclui desde informações médicas em dispositivos que monitoram pressão arterial, até sensores para monitoramento de acesso e temperatura (MENG, 2021).

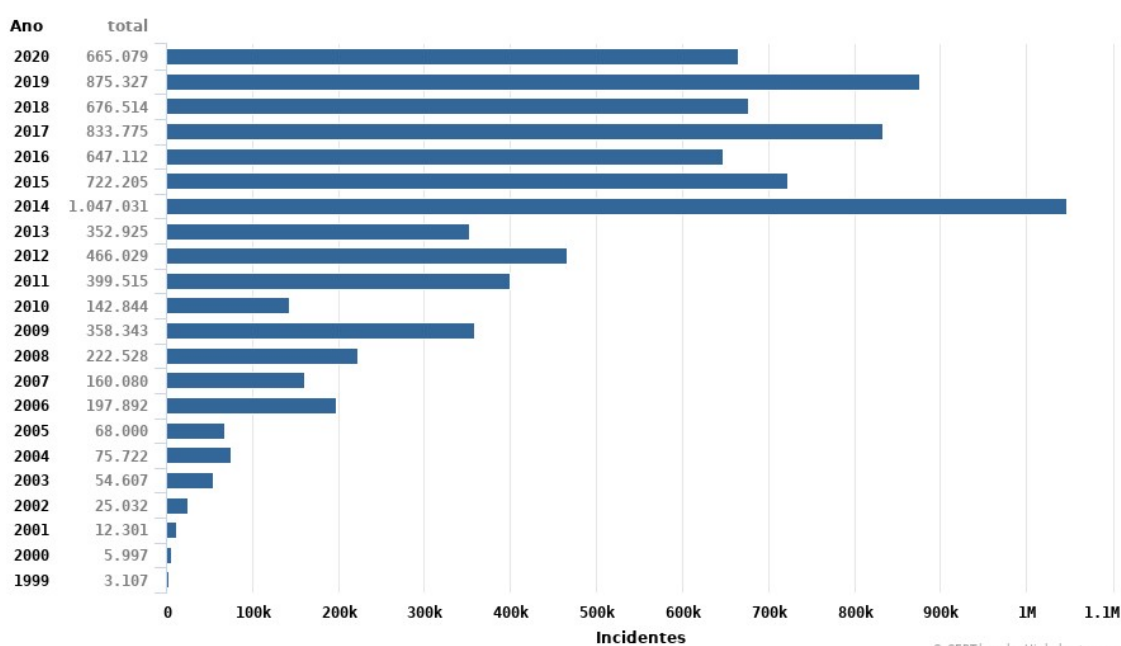
A IoT pode ajudar a trazer transformações na vida das pessoas, na forma como os dados são gerados, na facilidade do acesso e em sua disponibilidade. Por outro lado, pode ser uma porta aberta aos criminosos ou a pessoas mal-intencionadas que podem explorar erros no desenvolvimento do dispositivo, causando a perda do acesso, roubo de informações ou a sua paralização em casos extremos de atualização de firmwares. Nesse sentido, as organizações enfrentam, diariamente, novas oportunidades, variados riscos e desafios preocupantes de segurança de dados. Estas deverão saber lidar com estes problemas, para que isto não represente prejuízos financeiros e até da reputação empresarial.

Ao mesmo tempo em que a IoT proporciona benefícios valiosos nas instituições, os riscos de exposição a diversas ameaças de segurança e de privacidade aumentam bastante com o aumento da quantidade de dispositivos conectados nessas redes (MENG, 2021). Nos últimos anos, com o aumento de equipamentos IoT ligados em rede, estes se tornam expostos a várias varreduras na Internet por criminosos interessados em explorar vulnerabilidades em seu desenvolvimento. Cabe registrar que os equipamentos IoT trabalham com processadores e memória de capacidade limitada onde o objetivo destas tentativas de exploração é, exclusivamente, a obtenção dos seus dados, do controle do seu dispositivo e até para ser utilizado como fonte de chantagem e ameaças em rede (MENG, 2021).

Os telejornais têm noticiado diversos casos de vazamento de informações das empresas. Pode-se destacar, por exemplo, o caso de Edward Joseph Snowden, que atuava como administrador de sistemas da Agência de Segurança Nacional dos Estados Unidos, denominada NSA (National Security Agency), onde tomou posse de informações, utilizando credenciais que possuía por sua condição de funcionário. Posteriormente, Edward resolveu divulgar as informações e planos de ordem internacional do governo americano, incluindo, mas não se limitando a documentos, apresentações, conjuntos de e-mails trocados entre autoridades de diversos países e até informações sigilosas que culminaram no envolvimento de nomes de governantes do Brasil (GUARDIAN, 2022).

No Brasil, o CERT.br (CERT, 2022), organismo que coordena as respostas de incidentes informáticos nacionais, aponta números altos ao longo dos últimos 4 anos. Neste número, estão incluídas as tentativas de fraudes a bancos, as páginas falsas, o comércio eletrônico criminoso, as varreduras a redes e a propagação de vírus. A Figura 1 ilustra o número de incidentes desde o ano de 1999. Cabe registrar que apesar do número de 2020 ser inferior ao de 2019, as ações que foram reportadas consideram provedores de acesso, telecomunicações, grandes empresas em diversos ramos e até pessoas físicas.

Figura 1: Total de incidentes reportados por ano, Fonte: (CERT, 2022).



© CERT.br – by Highcharts.com

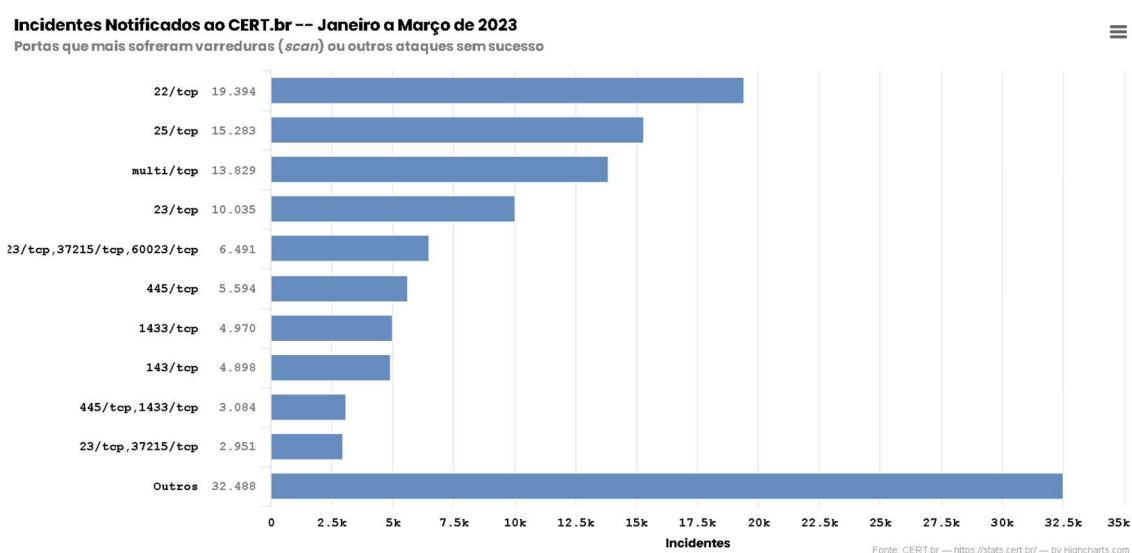
Este trabalho está inserido justamente nessa temática atual, abordando o problema da baixa qualidade da segurança nos equipamentos IoT.

1.1 Justificativa para o Desenvolvimento do Trabalho

A IoT é uma rede de dispositivos interconectados que coletam e trocam dados e apresenta riscos exclusivos de privacidade e segurança cibernética que devem ser abordados (NIST, 2019). Existe uma alta crescente de vulnerabilidades e ataques assolando muitas empresas, podendo trazer prejuízos de ordem financeira às grandes indústrias.

Com a ajuda da Internet, organizações criminosas regionais e locais começaram a estabelecer redes criminosas que operam em todo o mundo. De acordo com CERT.br, pode-se observar na figura 2 a seguir uma considerável quantidade de incidentes que foram reportados nos últimos meses. Esse gráfico ilustra detalhadamente os principais protocolos que mais sofrem varreduras e tentativas de intrusão na atualidade. A maioria desses protocolos é TCP e trabalha em comunicação com dispositivos IoT (CERT.br, 2023).

Figura 2: Principais portas que sofreram varreduras e outros ataques, Fonte: (CERT, 2023).



Neste contexto, este trabalho trata da importância da atualização das informações na era cibernética, com foco em expor as principais ameaças e vulnerabilidades em uma rede IoT corporativa, e em paralelo, oferecer um plano de mitigação dessas principais vulnerabilidades, a fim de poder auxiliar na resolução e prevenção de incidentes de cibersegurança para as grandes indústrias brasileiras.

De forma mais específica, diante de tantas das ameaças e vulnerabilidades em uma rede IoT corporativa, torna-se evidente a necessidade da proposição e execução de ações para minimizar a possibilidade de ocorrência de ataques. Entretanto, uma vez que essas vulnerabilidades são em grande quantidade, é de importante que as organizações tenham um plano para o tratamento das mesmas, ou seja, é necessário haver uma priorização do tratamento das vulnerabilidades que mais impactam em uma rede IoT corporativa, levando-se em conta impactos técnicos e financeiros.

Dessa forma, a utilização de um Método Multicritério pode auxiliar a organização na tomada de decisão sobre quais vulnerabilidades devem ser tratadas de forma prioritária, a partir de uma classificação (ranqueamento) das mesmas, levando-se em conta diferentes critérios, tanto técnicos, quanto financeiros.

1.2 Objetivo Geral

Este trabalho tem como objetivo identificar as principais vulnerabilidades em uma rede IoT corporativa, a partir de uma classificação das mesmas realizada pela aplicação de um Método Multicritério de tomada de decisão. A partir dessa classificação, é realizada a proposição de ações para a mitigação das principais vulnerabilidades analisadas. Organização do Trabalho

Este trabalho está estruturado como se segue.

Capítulo 2 - Revisão Bibliográfica - apresenta um estudo sobre redes IoT e as possíveis implementações de segurança para essas redes, sendo expostos os principais modelos e estruturação destas redes.

Capítulo 3 – Vulnerabilidades e ameaças em uma rede IoT - : apresenta as principais vulnerabilidades e ameaças em uma rede IoT corporativa, de acordo com a literatura.

Capítulo 4 – Método de ponderação aditiva simples – trata do Método Multicritério escolhido para a classificação (ranqueamento) das vulnerabilidades.

Capítulo 5 – Metodologia – aborda a metodologia utilizada para o desenvolvimento do trabalho

Capítulo 6 – Resultados – apresenta os principais resultados obtidos neste trabalho.

Capítulo 7 – Análise e Discussões – trata das análises e discussões referentes aos resultados obtidos no capítulo anterior e apresenta uma proposta de ações para a mitigação das principais vulnerabilidades analisadas.

Capítulo 8 – Conclusão – aborda as principais conclusões deste trabalho.

2. REDES IOT

De acordo com a referência (OLSON, 2016), as redes IoT são constituídas por dispositivos que se comunicam entre si sendo que esses dispositivos podem ser os mais diversos, de uma geladeira a carros, máquinas, computadores e smartphones, e variam desde dispositivos grandes a pequenos objetos, como lâmpadas e relógios.

Cabe salientar que esses dispositivos devem estar equipados com os componentes certos para fornecer comunicação como chips, sensores, antenas, entre outros, permitindo que uma pessoa interaja com o dispositivo por meio de tecnologia em redes de comunicação como Wi-Fi, Bluetooth, Near Field Communication (NFC), etc.

Muitos setores da indústria têm trabalhado para produzir dispositivos que facilitem a tomada de decisões, amplifiquem os controles, garantam o devido sensoriamento e monitoramento de ambiente. Estes dispositivos podem variar de tamanho, capacidade, custo e até processamento (FERREIRA, 2022).

O uso destes dispositivos, amplia a execução de atividades e tarefas simples do dia a dia, como por exemplo:

- a. Monitoramento de temperatura e umidade: são utilizados em diversos cenários de automações e coletas de análise, como em aparelhos de ar-condicionado, centrais de automações empresariais, controle e funcionamento de terminados equipamentos de refrigeração, ambientes que dependam de temperatura de precisão como datacenters, dentre outros.
- b. Monitoramento de som: são utilizados na monitoração de variação de volumes e no padrão de som gerados por um equipamento em funcionamento com objetivo de detectar problemas em seu funcionamento que exijam atuação. Outro uso muito popular, são as assistentes por voz, que possuem um modelo bastante simplificado de

identificar palavras-chave e direcionar o conteúdo do comando para um sistema em nuvem.

- c. Monitoramento cardíaco: estes sensores podem ser colocados sobre a pele do usuário, com capacidade de monitorar desde frequência cardíaca até alterações de comportamento que possa ser danoso à saúde, como arritmias e alteração de temperatura corporal. Estes dispositivos com fins médicos, estão cada vez mais acessíveis financeiramente, contribuem para acompanhar evoluções e problemas que possam atenuar a situação da saúde.

As tecnologias de comunicação destes dispositivos podem envolver Wifi, Bluetooth, redes 3G, redes 4g e NFC.

Considerada como uma grande solução tecnológica para o mercado de eletroeletrônicos e smart home, as redes IoT têm sido apontadas como um dos segmentos de mercado com alto potencial para implantação destes dispositivos “independentes”. No entanto, a adoção de um dispositivo IoT por um usuário doméstico depende de seu desejo de adquiri-lo, pois existem fatores como conveniência e segurança que são identificados como as duas principais condições que influenciam nesta decisão (DONG; CHANG, 2014).

Com relação à segurança dessas redes, os principais desafios incluem privacidade, autenticação e conexão de ponta a ponta segura (PRISMS, 2014). A presença de vários padrões e protocolos atualmente usados no mercado, requer atenção para garantia da compatibilidade (ZHAO, 2010).

2.1. Protocolo de Comunicação

Uma das principais vulnerabilidades no aspecto de segurança dos protocolos IP (utilizados também nas redes IoT) é a incapacidade de autenticar uma máquina na rede. Ou seja, é tecnicamente impossível determinar, com certeza, a identidade da máquina que tenha originado um determinado pacote (POUW, 1999), e existem poucas garantias de que o conteúdo de um pacote não tenha sido alterado ou até sofrido uma violação.

No ambiente da Internet, não é incomum máquinas serem atacadas por deficiências nas implementações das camadas TCP/IP, ataques tipo “*SYN flooding*”, que se aproveitam de uma vulnerabilidade na implementação da fase *three-way handshake*. Esta vulnerabilidade é determinada quando, por exemplo, o host B recebe uma requisição SYN do host A, ele deve manter o estado desta conexão parcialmente aberta em uma fila por alguns segundos, a exploração pode ocorrer quando esta requisição é feita inúmeras vezes, sem existir tempo suficiente para resposta, ocupando rapidamente o processamento e consequentemente impedindo o aceite de novas conexões (BLANK, 2006).

Existe ainda, na pilha de protocolos a possibilidade de um atacante enviar dados com um endereço IP de origem que não é o do próprio equipamento; a camada IP não tem capacidade de autenticar os pacotes recebidos, exigindo que o equipamento de destino efetue as respostas para os endereços que não são reais, dificultando a resposta, consumindo recursos e inundando o equipamento destino com requisições que não são verdadeiras, esta técnica de exploração tem o nome de “IP Spoofing” (SHINDER, 2011). (Shinder, 2011).

Diante destes possíveis ataques, se faz necessário o entendimento e aplicação de mecanismos de segurança em redes IoT capazes de limitar o campo de exploração de um atacante.

2.2 Segurança da Informação

A definição de segurança da informação pode ser resumida como a proteção da informação a fim de preservar os três principais pilares de segurança, sendo eles: confidencialidade, integridade e disponibilidade, para que não sejam explorados por ameaças ou vulnerabilidades que possam prejudicar os negócios de uma organização (SÊMOLA, 2003).

Os objetivos e a cultura de uma organização devem considerar a segurança da informação como uma prioridade crucial para proteção do negócio. Esta proteção pode ser entendida sob três pontos de vista (SIPONEN, 2001):

- a. Técnico, com ênfase na utilização de controles tecnológicos como medida de proteção da informação;

- b. Social, com foco na motivação de pessoas e no comportamento coletivo para resolução de problemas de segurança;
- c. Sociotécnico, com a exploração das vantagens e minimização das desvantagens das duas abordagens anteriores, de forma simultânea

Dentre os fatores críticos que influenciam o sucesso da cultura de segurança da informação, a política de segurança é considerada uma das melhores práticas a serem adotadas, tanto para as organizações, como para a conscientização do usuário final (WILLIAMS, 2001).

A segurança da informação e seus problemas são abordados em várias dimensões e por meio de iniciativas, tanto na literatura quanto dentro das organizações. No que se refere à dimensão corporativa, por mais que haja o reconhecimento da necessidade de implementá-la, geralmente não há clareza sobre o que deve ser protegido e sobre como preparar esta implementação (ALMEIDA; SOUZA; CARDOSO, 2010).

Para que exista um ambiente de redes em conformidade, onde as vulnerabilidades e ameaças são tratadas com o devido acompanhamento, o gerenciamento de riscos é uma disciplina da segurança da informação que pode auxiliar a elencar os fatores determinantes para qualificar vulnerabilidades e ameaças com uma avaliação de probabilidade e impacto de ocorrências em ambientes de redes IoT.

Para contribuir na qualificação das ameaças, considerando que um dos principais objetivos envolvidos na segurança da informação é a proteção do patrimônio empresarial e até pessoal, não se limitando aos ativos, mas as informações e dados que ali trafegam, sugere-se o devido acompanhamento com (ALMEIDA; SOUZA; CARDOSO, 2010):

- a. Objetivo: auxiliar no gerenciamento desses riscos através do uso de uma representação formal de informações relacionadas, promovendo a aquisição e compartilhamento de conhecimento no domínio;
- b. Tomada de decisões: auxiliar na implementação da gestão de riscos e na tomada de decisões. Cabe salientar que a decisão nestes casos

pode ser para assumir o risco de um equipamento IoT desatualizado tecnologicamente ou até que represente uma ameaça ao funcionamento da estrutura empresarial, como por exemplo, sensores sem controles de acesso apropriados, sejam físicos e até lógicos.

- c. Lições aprendidas: auxiliar na reutilização de conhecimento e informações, planejando treinamento de colaboradores e o devido arquivamento eletrônico dos registros de ameaças e vulnerabilidades para posterior estudo e acompanhamento.

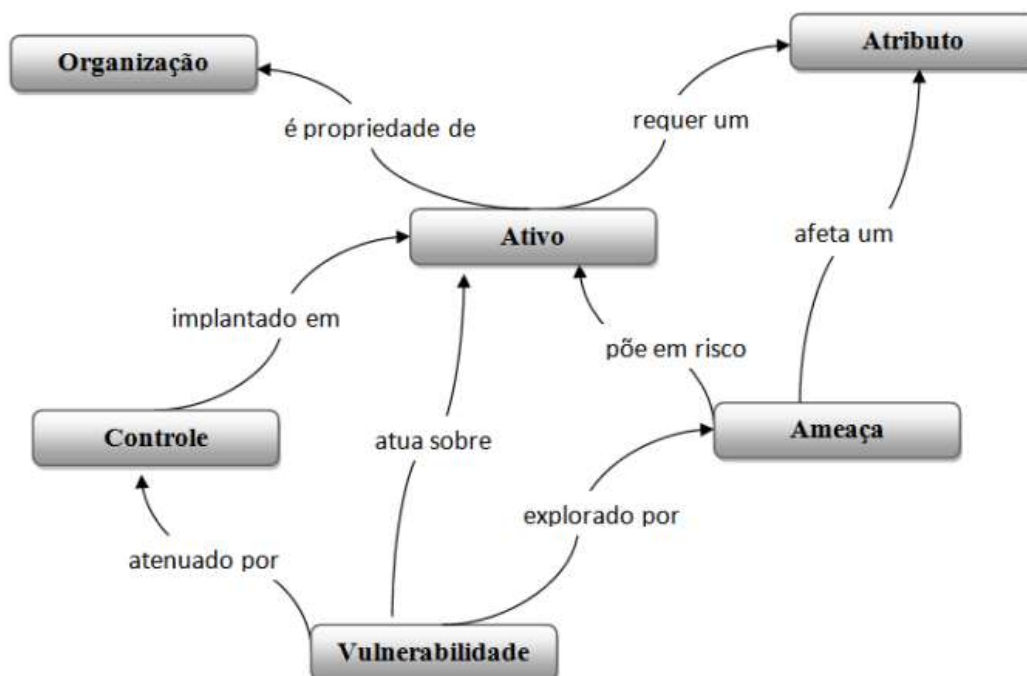
Existem estudos complementares que definem modelos para avaliar a segurança da informação com critérios e afinidades gerais (ALMEIDA; SOUZA; CARDOSO, 2010) e para esta explanação pode-se considerar:

- a. Organização: uma entidade social composta por recursos materiais e humanos que possui objetivos comuns, procedimentos sistêmicos para controlar seu desempenho e limites definidos que a separam do meio ambiente. Pode ser uma instituição pública ou privada.
- b. Atributo de segurança: propriedade atribuída a um ativo que demonstre aderência aos requisitos de segurança.
- c. Ativo: algo de propriedade da organização que é usado para atingir seus objetivos sociais, tais como: equipamentos, móveis, periféricos, dentre outros.
- d. Controle: procedimento sistêmico padrão implementado para reduzir vulnerabilidades e proteger as atividades por meio de medidas preventivas e corretivas.
- e. Ameaça: possibilidade de causar danos às atividades da organização, o que afeta atributos específicos de segurança investigando vulnerabilidades organizacionais. Pode ter origem humana ou natural e ser o resultado de um evento não intencional ou de uma ação mal-intencionada.

- f. Vulnerabilidade: situação caracterizada pela falta de medidas de proteção adequadas. Uma vulnerabilidade tem um nível de gravidade associado por exemplo, crítico, alto, moderado ou baixo), podendo ter origens administrativas, técnicas ou físicas.

A figura 3 ilustra o esquema da ontologia de segurança da informação frente aos riscos e vulnerabilidades associadas a um ativo.

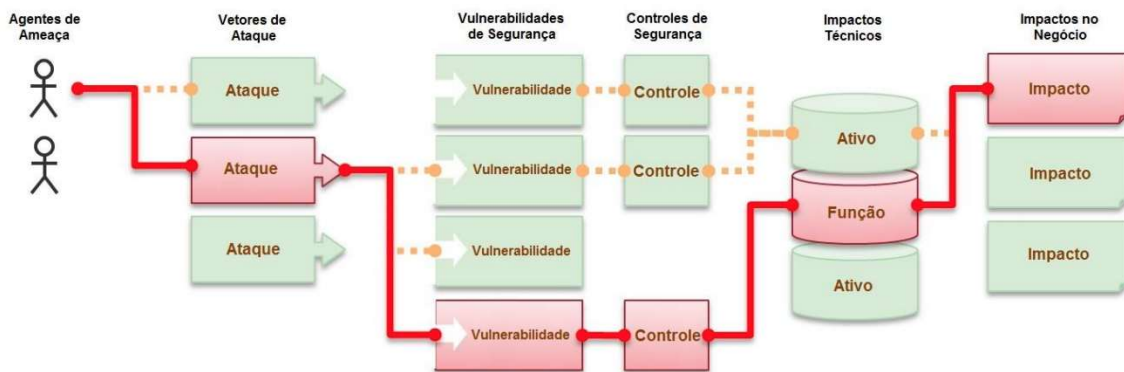
Figura 3: Esquema da ontologia de segurança da informação.



Fonte: ALMEIDA et al. (2010)

A Figura 4 apresenta os caminhos para encontrar e explorar vulnerabilidades, através de agentes que representam ameaças a um ambiente ou sistema.

Figura 4: Agentes de ameaças e as vulnerabilidades de segurança. Fonte: adaptado de (OWASP, 2013).



Para que os agentes de ameaças explorem vulnerabilidades, vetores de ataque com ferramentas sofisticadas são necessárias. O devido controle do ambiente, infraestrutura e até as funções correlatas dos dispositivos IoT utilizados, devem ser atualizados e avaliados com frequência.

2.3. Segurança em Redes IoT

A segurança das redes IoT na indústria e nas residências é de extrema importância, pois as infraestruturas estão se tornando cada vez mais conectadas e dependentes de dispositivos IoT para operar eficientemente. A falta de segurança adequada nessas redes pode resultar em sérias consequências, como a interrupção da produção, a perda de dados confidenciais e até mesmo riscos à segurança física. (CHOO, 2019).

Existem vários tipos de vulnerabilidades que podem ser exploradas em redes IoT, alguns exemplos:

- a. Falta de autenticação e autorização adequadas: Dispositivos IoT podem ser comprometidos se não houver mecanismos adequados para autenticar e autorizar o acesso a eles. Isso pode permitir que invasores acessem e controlem os dispositivos.
- b. Comunicação insegura: Se as comunicações entre os dispositivos IoT e os sistemas de gerenciamento não forem protegidas, os dados transmitidos podem ser interceptados, modificados ou falsificados.

- c. Falta de atualizações e patches de segurança: Muitos dispositivos IoT têm vida útil longa e podem não receber atualizações regulares de segurança. Isso significa que vulnerabilidades conhecidas não são corrigidas, tornando os dispositivos mais suscetíveis a ataques.
- d. Configurações padrão inseguras: Muitos dispositivos IoT são implantados com configurações padrão que podem ser facilmente exploradas. Senhas fracas ou padrões de autenticação previsíveis são exemplos comuns de configurações inseguras.
- e. Físico comprometido: Dispositivos IoT na indústria podem ser fisicamente acessíveis a invasores, permitindo que eles realizem ações maliciosas, como inserir dispositivos ou alterar conexões.

Para proteger as redes IoT na indústria, várias soluções estão sendo desenvolvidas. Alguns dos avanços mais recentes incluem:

- f. Criptografia: o uso de criptografia robusta para proteger a comunicação entre dispositivos IoT e sistemas de gerenciamento, garantindo que os dados transmitidos permaneçam seguros e confidenciais.
- g. Autenticação forte: implementar métodos de autenticação mais fortes, como autenticação de dois fatores, para garantir que apenas usuários autorizados tenham acesso aos dispositivos IoT.
- h. Atualizações regulares: garantir que os dispositivos IoT recebam atualizações regulares de segurança para corrigir vulnerabilidades conhecidas e garantir que estejam protegidos contra novas ameaças.
- i. Monitoramento contínuo: utilizar soluções de monitoramento de segurança em tempo real para identificar atividades suspeitas ou anomalias nas redes IoT e responder rapidamente a possíveis ataques.

Essas são apenas algumas das medidas de segurança que estão sendo adotadas para proteger as redes IoT na indústria.

2.4. A Legislação com a Segurança da Informação

A legislação brasileira tem evoluído para promover a segurança da informação e proteção de redes. Algumas leis importantes que apoiam as medidas de proteção de redes no Brasil são:

- a. Lei Geral de Proteção de Dados (LGPD) - A LGPD entrou em vigor em setembro de 2020 e estabelece diretrizes para o tratamento de dados pessoais por parte de empresas e organizações. Ela estabelece princípios, direitos dos titulares dos dados, obrigações para as empresas e penalidades em caso de violações de dados.
- b. Marco Civil da Internet - O Marco Civil da Internet, instituído em 2014, estabelece princípios, direitos e deveres para o uso da Internet no Brasil. Ele aborda questões relacionadas à privacidade, liberdade de expressão, neutralidade da rede e responsabilidade dos provedores de serviços.
- c. Lei de Crimes Cibernéticos (Lei 12.737/2012) - Também conhecida como "Lei Carolina Dieckmann", essa lei estabelece penalidades para crimes cometidos no ambiente digital, como invasão de dispositivos, roubo de dados, entre outros.
- d. Lei de Acesso à Informação (Lei 12.527/2011) - Essa lei regulamenta o acesso a informações públicas no Brasil, garantindo a transparência e o direito dos cidadãos de obter informações do governo. Ela também abrange a proteção de dados pessoais no contexto da administração pública.

Essas leis têm atuado nos anos atuais para promover benefícios tanto para as empresas quanto para os usuários das redes. Alguns dos benefícios incluem:

- e. Proteção da privacidade: As leis garantem a proteção dos dados pessoais, estabelecendo diretrizes claras sobre como as informações devem ser coletadas, usadas e armazenadas. Isso aumenta a

confiança dos usuários nas empresas e ajuda a evitar o uso indevido de informações sensíveis.

- f. Melhoria na segurança cibernética: Com a aplicação das leis, as empresas são incentivadas a adotar medidas de segurança mais robustas para proteger as redes e os dados. Isso ajuda a reduzir o risco de violações de segurança e ataques cibernéticos.
- g. Responsabilidade e prestação de contas: As leis estabelecem obrigações claras para as empresas em relação à proteção de dados e segurança da informação. Isso garante que as empresas sejam responsabilizadas por eventuais violações e que prestem contas sobre suas práticas de segurança.
- h. Maior transparência: As leis exigem que as empresas informem aos usuários como seus dados serão utilizados e com quem serão compartilhados. Isso proporciona maior transparência e permite que os usuários tomem decisões informadas sobre o compartilhamento de suas informações.

Além de fornecerem uma base jurídica para garantir a privacidade e a segurança dos dados coletados e processados pelos dispositivos IoT, elas incentivam a adoção de boas práticas de segurança, como o uso de criptografia, autenticação segura e atualizações regulares.

3. VULNERABILIDADES E AMEAÇAS EM UMA REDE IOT

3.1 Vulnerabilidades

De acordo com OWASP (2018), vulnerabilidades em redes IoT referem-se a fraquezas ou falhas nos mecanismos de segurança que podem ser exploradas por agentes mal-intencionados para obter acesso não autorizado, manipular dados ou interromper o funcionamento normal de dispositivos e sistemas IoT. Essas vulnerabilidades podem surgir de vários fatores e podem ser categorizadas como:

- a. Senhas frágeis de fácil decodificação.
- b. Serviços de interface de redes inseguros.
- c. Falta de mecanismo de atualização segura.
- d. Uso de componentes inseguros ou desatualizados.
- e. Proteção de privacidade insuficiente.
- f. Transferência e armazenamento de dados inseguros.
- g. Falta de gerenciamento de dispositivos
- h. Configuração padrão de contas.
- i. Falta de *hardening* físico.

3.1.1. Senhas Frágeis de Fácil Decodificação

Quando se trata de senhas e codificação para uma rede IoT, é importante priorizar a segurança. Senhas fáceis podem deixar os dispositivos IoT vulneráveis a acesso não autorizado e possíveis ataques cibernéticos (OWASP, 2018). Como exemplo, a seguir algumas considerações importantes para criar senhas fortes e implementá-las em redes IoT:

- a. Complexidade da senha - uma senha forte deve ser complexa, combinando letras maiúsculas e minúsculas, números e caracteres

especiais. Evitar usar palavras comuns, padrões previsíveis ou informações pessoais. Por exemplo, "P@ssw0rd!" é uma senha mais forte do que "password123."

- b. Comprimento - o comprimento da senha é crucial. Quanto mais longa a senha, mais difícil é decifrá-la. Utilizar um mínimo de oito caracteres, mas idealmente, usar uma senha que consiste em várias palavras ou uma combinação de palavras, números e símbolos. Por exemplo, "*CorrectHorseBatteryStaple*" é uma senha forte.
- c. Evitar senhas padrão ou comuns - muitos dispositivos IoT vêm com nomes de usuário e senhas padrão, como "admin" e "senha". É crucial alterar essas credenciais padrão para senhas exclusivas e fortes imediatamente após configurar o dispositivo. Evitar usar senhas comuns que sejam fáceis de adivinhar ou que possam ser encontradas em dicionários de senhas.
- d. Autenticação de dois fatores (2FA) - a implementação da autenticação de dois fatores adiciona uma camada extra de segurança. Ela exige que os usuários forneçam um método de verificação adicional, como impressão digital, código SMS ou aplicativo de autenticação, junto com sua senha para acessar a rede IoT.
- e. Armazenamento e criptografia de senhas - ao armazenar senhas, é essencial usar métodos de criptografia seguros. Evitar armazenar senhas em texto sem formatação ou formatos com hash fraco. Utilizar algoritmos criptográficos fortes e práticas padrão do setor para garantir a segurança do armazenamento de senhas.
- f. Atualizações regulares de senha - incentivar os usuários a alterar suas senhas periodicamente. A implementação de uma política que imponha alterações de senha a cada poucos meses ajuda a proteger contra vulnerabilidades de longo prazo. Além disso, ajuda a evitar a reutilização de senhas que podem ter sido comprometidas em outras violações de dados.

- g. Educação e conscientização do usuário - é crucial educar os usuários sobre a importância de senhas fortes e os riscos potenciais de senhas fracas. Promover as melhores práticas de senha, como não compartilhar senhas, evitar anotá-las em locais de fácil acesso e usar senhas exclusivas para cada dispositivo ou serviço.
- h. Segmentação de rede - para aumentar a segurança, considerar implementar a segmentação de rede para seus dispositivos IoT. Ao dividir a rede IoT em segmentos separados ou VLANs (Virtual Local Area Networks), pode-se isolar dispositivos e restringir o acesso não autorizado se um dispositivo estiver comprometido.
- i. Atualizações e patches regulares - manter dispositivos IoT e seus softwares associados atualizados com as últimas atualizações de firmware e patches de segurança. Os fabricantes geralmente lançam atualizações para corrigir vulnerabilidades e melhorar a segurança do dispositivo, portanto, deve-se certificar-se de que seus dispositivos estejam executando as versões mais recentes.

Seguindo essas diretrizes e incorporando práticas de senha segura em na IoT, pode-se reduzir significativamente o risco de acesso não autorizado e proteger dispositivos e dados contra possíveis ameaças.

3.1.2. Serviços de Interface de Redes Inseguros

Serviços de interface de rede inseguros em uma rede IoT referem-se a vulnerabilidades ou fraquezas nas interfaces de rede usadas por dispositivos IoT que podem ser exploradas por atores mal-intencionados para obter acesso não autorizado ou controle sobre esses dispositivos. Os serviços de interface de rede são responsáveis por facilitar a comunicação entre os dispositivos IoT e a infraestrutura de rede maior (OWASP, 2018).

Aqui estão alguns exemplos comuns de serviços de interface de rede inseguros em uma rede IoT:

- a. Credenciais fracas ou padrão: muitos dispositivos IoT vêm com nomes de usuário e senhas padrão, que geralmente são bem conhecidos e

- b. facilmente exploráveis. Se essas credenciais padrão não forem alteradas ou forem fracas, um invasor pode facilmente obter acesso ao dispositivo e potencialmente comprometer toda a rede.
- c. Falta de criptografia: a criptografia desempenha um papel vital na segurança dos dados transmitidos pelas redes. Se o serviço de interface de rede de um dispositivo IoT não utilizar protocolos de criptografia ou usar criptografia fraca, ele se tornará suscetível a espionagem e interceptação de dados. Isso pode levar ao acesso não autorizado a informações confidenciais ou à adulteração da funcionalidade do dispositivo.
- d. Serviços não autenticados: em alguns casos, os dispositivos IoT podem fornecer serviços de rede que não requerem nenhuma forma de autenticação. Isso significa que qualquer pessoa que tenha acesso à interface de rede do dispositivo pode acessá-la e controlá-la sem qualquer impedimento. É crucial implementar mecanismos de autenticação adequados para garantir que apenas indivíduos ou sistemas autorizados possam interagir com o dispositivo IoT.
- e. Protocolos vulneráveis: os dispositivos IoT geralmente dependem de vários protocolos de rede, como HTTP, MQTT ou CoAP, para se comunicar com outros dispositivos ou sistemas de *back-end*. Se esses protocolos tiverem vulnerabilidades conhecidas ou não forem implementados corretamente, os invasores podem explorá-los para comprometer o dispositivo ou obter acesso não autorizado à rede.
- f. Falta de atualizações de segurança: muitos dispositivos IoT têm recursos limitados e podem não receber atualizações de segurança regulares dos fabricantes. Isso pode deixar os serviços de interface de rede expostos a vulnerabilidades conhecidas que podem ser facilmente exploradas por invasores.

3.1.3. Falta de Mecanismo de Atualização Seguro

A falta de um mecanismo seguro de atualização em uma rede IoT, refere-se à ausência ou inadequação de um método confiável para atualizar o software ou firmware em execução nos dispositivos IoT. Isso pode levar a vulnerabilidades de segurança significativas e desafios no gerenciamento e manutenção da rede IoT (OWASP, 2018).

Vários fatores contribuem para esse problema:

- a. Dispositivos com recursos limitados: muitos dispositivos IoT têm poder de computação, memória e capacidade de armazenamento limitados. Essas restrições dificultam a implementação de recursos de segurança robustos, incluindo mecanismos de atualização seguros. Devido às limitações de hardware, os fabricantes podem priorizar a funcionalidade em detrimento da segurança, levando a processos de atualização inseguros ou à omissão total dos mecanismos de atualização.
- b. Diversidade de dispositivos e protocolos: o ecossistema IoT abrange uma ampla gama de dispositivos de vários fabricantes, cada um com seus próprios protocolos proprietários, sistemas operacionais e pilhas de software. Essa diversidade cria desafios de compatibilidade e torna desafiador estabelecer um mecanismo de atualização padronizado que funcione universalmente em todos os dispositivos. Os fabricantes podem se concentrar no desenvolvimento de recursos e funcionalidades em vez de investir recursos na criação de uma infraestrutura de atualização segura.
- c. Limitações de conectividade: muitos dispositivos IoT operam em ambientes com conectividade de rede limitada ou intermitente. Eles podem contar com protocolos sem fio de baixa potência, operar em locais remotos ou estar sujeitos a interrupções frequentes na conectividade. Essas limitações podem prejudicar a capacidade de fornecer atualizações confiáveis aos dispositivos, aumentando o risco de vulnerabilidades não corrigidas.

- d. Falta de práticas de segurança padronizadas: o setor que gerencia redes com dispositivos IoT, carece de um conjunto unificado de padrões de segurança e práticas recomendadas. Os fabricantes podem não priorizar a segurança durante as fases de projeto e desenvolvimento, resultando em medidas de segurança inadequadas, incluindo mecanismos de atualização. A ausência de práticas de segurança padronizadas dificulta a aplicação de mecanismos de atualização seguros em todo o setor.
- e. Longos ciclos de vida do dispositivo: os dispositivos IoT geralmente têm longos ciclos de vida, principalmente em implantações industriais ou de infraestrutura. Isso significa que os dispositivos podem permanecer em serviço por vários anos ou até décadas sem receber atualizações ou patches de segurança. À medida que surgem novas vulnerabilidades, os dispositivos sem suporte tornam-se cada vez mais vulneráveis a ataques, pois não há nenhum mecanismo para resolver problemas de segurança por meio de atualizações.

A falta de um mecanismo de atualização seguro em uma rede IoT cria riscos de segurança significativos. Ele deixa os dispositivos suscetíveis a *exploits* e comprometimentos, levando potencialmente a violações de dados, acesso não autorizado e formação de *botnets* para atividades maliciosas. É importante que os fabricantes de dispositivos IoT e as partes interessadas reconheçam a importância de mecanismos de atualização seguros e invistam na implementação de práticas robustas e padronizadas para garantir a segurança contínua das implantações de IoT.

3.1.4. Uso de Componentes Inseguros ou Desatualizados

O uso de componentes inseguros ou desatualizados em uma rede IoT pode levar a exploração de sérias vulnerabilidades de segurança. Os dispositivos IoT geralmente consistem em hardware, firmware e software que se comunicam entre si e com a Internet para coletar, processar e trocar dados. Se esses componentes não forem seguros ou não forem atualizados regularmente,

podem ser explorados por indivíduos mal-intencionados para obter acesso não autorizado à rede ou comprometer a integridade dos dados (OWASP, 2018).

Aqui estão algumas explicações sobre os riscos associados ao uso de componentes inseguros ou desatualizados em uma rede IoT:

- a. Vulnerabilidades conhecidas: os componentes desatualizados podem conter falhas de segurança conhecidas que foram corrigidas em versões posteriores. Isso permite que os hackers aproveitem essas vulnerabilidades conhecidas para invadir os dispositivos IoT e a rede.
- b. Falta de patches de segurança: à medida em que as ameaças evoluem, os fabricantes lançam patches e atualizações de segurança para corrigir quaisquer brechas ou falhas descobertas. No entanto, se os componentes não forem atualizados, as correções não serão aplicadas, deixando os dispositivos e a rede vulneráveis a ataques.
- c. Senhas padrão e frágeis: muitos dispositivos IoT vêm com senhas padrão configuradas que são amplamente conhecidas pelos hackers. Se essas senhas não forem alteradas, os invasores podem facilmente acessar os dispositivos e, potencialmente, comprometer toda a rede.
- d. Comunicação não criptografada: componentes desatualizados podem não suportar protocolos de criptografia robustos, o que torna a comunicação entre os dispositivos e a rede suscetível a interceptação e leitura não autorizada. Isso pode permitir que informações confidenciais sejam acessadas e comprometidas.
- e. Ausência de medidas de segurança adicionais: atualizações de segurança frequentes ajudam a melhorar as defesas contra novas ameaças e vulnerabilidades. Componentes desatualizados podem não ter as mais recentes medidas de segurança implementadas, como firewalls, sistemas de detecção de intrusões e autenticação multi fator, deixando a rede IoT mais exposta a ataques.
- f. Falta de suporte do fabricante: à medida que os dispositivos IoT envelhecem, os fabricantes podem descontinuar o suporte e as

atualizações de segurança para esses componentes. Isso significa que os dispositivos permanecerão vulneráveis, pois não receberão correções para novas ameaças que surgirem.

É essencial que os proprietários e administradores de redes IoT estejam cientes desses riscos e tomem medidas proativas para garantir que os componentes sejam seguros e estejam atualizados. Isso inclui a implementação de políticas de atualização, o monitoramento regular de patches de segurança, a alteração de senhas padrão, a criptografia de dados sensíveis e a escolha de fornecedores que ofereçam suporte de longo prazo aos seus produtos.

3.1.5. Proteção de Privacidade Insuficiente

A vulnerabilidade de proteção de privacidade insuficiente em uma rede IoT refere-se a uma falha de segurança que expõe os dados privados dos usuários a acesso não autorizado ou divulgação não autorizada. Os dispositivos IoT são dispositivos inteligentes interconectados que coletam e trocam dados pela internet e podem ser encontrados em vários ambientes, como residências, indústrias, saúde e sistemas de transporte (OWASP, 2018).

A proteção insuficiente da privacidade pode surgir devido a vários fatores em uma rede IoT, sendo eles:

- a. Criptografia de dados inadequada - os dispositivos IoT geralmente coletam informações confidenciais, como detalhes pessoais, dados de localização ou até mesmo dados relacionados à saúde. Se esses dados não forem criptografados adequadamente durante a transmissão ou armazenamento, eles podem ser interceptados ou acessados por indivíduos não autorizados ou agentes mal-intencionados.
- b. Autenticação e controle de acesso fracos - os dispositivos IoT devem empregar mecanismos de autenticação robustos para garantir que apenas usuários ou dispositivos autorizados possam acessar dados confidenciais ou controlar os dispositivos. Senhas fracas ou falta de

protocolos de autenticação adequados podem levar ao acesso não autorizado, comprometendo a privacidade.

- c. Protocolos de comunicação inseguros - os dispositivos IoT dependem de vários protocolos de comunicação para transmitir dados entre dispositivos e sistemas de *back-end*. Se esses protocolos tiverem vulnerabilidades de segurança ou não forem adequadamente protegidos, os invasores podem interceptar ou manipular os dados, comprometendo a privacidade.
- d. Atualizações de segurança insuficientes - os dispositivos IoT geralmente são executados em software ou firmware incorporado, que pode conter vulnerabilidades de segurança. Se os fabricantes de dispositivos não fornecerem atualizações ou patches de segurança regulares para lidar com essas vulnerabilidades, isso deixará os dispositivos expostos a violações de privacidade.
- e. Práticas inadequadas de manipulação de dados - os dispositivos IoT geram e processam grandes quantidades de dados e, se práticas adequadas de manipulação de dados não forem implementadas, existe o risco de acesso ou divulgação não autorizados. Isso inclui anonimização inadequada de dados, retenção de dados desnecessários ou proteção insuficiente de dados em repouso.

As consequências da vulnerabilidade de proteção de privacidade insuficiente podem ser graves. Isso pode levar a vigilância não autorizada, roubo de identidade, fraude financeira ou até danos físicos se os dispositivos IoT comprometidos controlarem sistemas críticos. Além disso, violações de privacidade podem comprometer a confiança do usuário, levando a danos à reputação de organizações que implantam redes IoT.

3.1.6. Transferência e Armazenamento de Dados Inseguros

Transferência e armazenamento inseguros de dados referem-se a uma vulnerabilidade que pode ocorrer em uma rede IoT em que dados confidenciais não são protegidos adequadamente durante a transmissão ou armazenamento.

Essa vulnerabilidade pode levar a acesso não autorizado, violação de dados e comprometimento da privacidade (OWASP, 2018).

Existem vários fatores que contribuem para essa vulnerabilidade em uma rede IoT:

- a. Criptografia fraca - se os dados transmitidos ou armazenados em uma rede IoT não forem criptografados ou forem criptografados com algoritmos fracos, eles se tornarão suscetíveis à interceptação por agentes mal-intencionados. Métodos de criptografia fracos podem ser facilmente quebrados, expondo as informações confidenciais.
- b. Falta de autenticação - sem mecanismos de autenticação adequados, indivíduos não autorizados podem obter acesso à rede IoT e interceptar ou modificar os dados em trânsito. Isso pode levar ao acesso não autorizado a informações confidenciais e até mesmo ao controle de dispositivos IoT.
- c. Segurança de armazenamento de dados inadequada - os dispositivos IoT geram e coletam grandes quantidades de dados. Se esses dados forem armazenados sem medidas de segurança adequadas, como controles de acesso fracos ou armazenamento não criptografado, eles se tornarão um alvo atraente para invasores. O acesso não autorizado aos dados armazenados pode resultar em roubo, manipulação ou adulteração de dados.
- d. Protocolos de comunicação vulneráveis - os dispositivos IoT geralmente usam vários protocolos de comunicação para transmitir dados dentro da rede. Se esses protocolos estiverem desatualizados, mal implementados ou tiverem vulnerabilidades conhecidas, os invasores podem explorá-los para interceptar ou manipular dados durante a transmissão.
- e. Falta de atualizações de firmware - os dispositivos IoT podem ter vulnerabilidades de firmware ou software que podem ser exploradas por invasores para obter acesso ou controle não autorizado. Se os

dispositivos não forem atualizados regularmente com patches e correções de segurança, eles permanecerão vulneráveis a explorações conhecidas.

As consequências da transferência e armazenamento inseguros de dados em uma rede IoT podem ser graves. Os invasores podem obter acesso a informações confidenciais do usuário, comprometer a integridade dos dados ou até mesmo assumir o controle de dispositivos IoT para fins maliciosos. Isso pode ter implicações significativas em termos de violação de privacidade, perdas financeiras, riscos de segurança e danos à reputação.

Para mitigar essas vulnerabilidades, é crucial implementar algoritmos de criptografia fortes, aplicar mecanismos de autenticação, empregar protocolos de comunicação seguros, atualizar firmware/software regularmente e garantir controles de acesso e criptografia adequados para os dados armazenados. Além disso, monitoramento contínuo, avaliações de vulnerabilidade e testes de penetração podem ajudar a identificar e resolver quaisquer pontos fracos na infraestrutura de segurança da rede IoT.

3.1.7. Falta de Gerenciamento de Dispositivos

A falta de gerenciamento de dispositivos em uma rede IoT refere-se a uma falha de segurança que pode ocorrer ao gerenciar dispositivos temporariamente desconectados ou offline. Essa vulnerabilidade pode ser explorada por agentes mal-intencionados para obter acesso não autorizado a dispositivos ou à própria rede.

Quando um dispositivo IoT está temporariamente desconectado ou offline, como quando está desligado, em manutenção ou com uma interrupção de rede, ele pode ser configurado para estabelecer uma conexão com um servidor de gerenciamento após a reconexão. Esse mecanismo permite que o gerenciamento remoto, atualizações ou alterações de configuração sejam aplicadas ao dispositivo assim que ele voltar a ficar online.

No entanto, se o processo de gerenciamento de dispositivos ausentes não estiver devidamente protegido, ele pode se tornar um possível ponto de entrada

para invasores. Aqui estão alguns problemas comuns que podem levar a vulnerabilidades:

- a. Autenticação fraca - se o mecanismo de autenticação usado durante a reconexão do dispositivo for fraco ou facilmente contornado, um invasor poderá se passar pelo dispositivo e obter acesso não autorizado.
- b. Falta de criptografia - se a comunicação entre o dispositivo e o servidor de gerenciamento não for criptografada corretamente, os dados confidenciais trocados durante o processo de reconexão podem ser interceptados e manipulados por invasores.
- c. Processo de atualização/configuração inseguro - se os arquivos de atualização ou configuração enviados ao dispositivo durante a reconexão não forem devidamente verificados ou autenticados, os invasores podem injetar código malicioso ou adulterar as configurações, comprometendo a segurança ou a integridade do dispositivo.
- d. Falta de controles de acesso - se os controles de acesso adequados não estiverem em vigor durante o processo de gerenciamento de dispositivos ausentes, os invasores podem explorar essa fraqueza para obter controle não autorizado sobre o dispositivo ou a rede.

Para mitigar as vulnerabilidades de falta de gerenciamento de dispositivos, é importante seguir as práticas recomendadas de segurança pelo CERT.br (CERT.br, 2023):

- e. Autenticação forte - implementar mecanismos de autenticação forte, como autenticação de dois fatores ou autenticação baseada em certificado, para garantir que apenas dispositivos autorizados possam se reconectar à rede.
- f. Comunicação Segura - usar protocolos de criptografia, como TLS (Transport Layer Security), para proteger a comunicação entre o

dispositivo e o servidor de gerenciamento, garantindo a confidencialidade e integridade dos dados trocados.

- g. Processo seguro de atualização/configuração - aplicar assinaturas digitais ou verificação de soma de verificação para validar a autenticidade e a integridade dos arquivos de atualização e configuração antes de aplicá-los ao dispositivo. Empregar mecanismos de atualização seguros que impeçam modificações não autorizadas.
- h. Controles de acesso - implementar controles de acesso e mecanismos de autorização para limitar as ações que podem ser executadas durante o processo de gerenciamento de dispositivos ausentes. Conceder privilégios apenas a administradores ou dispositivos autorizados.
- i. Monitoramento e Detecção de Intrusão - monitorar continuamente a rede em busca de atividades incomuns ou não autorizadas durante o processo de reconexão do dispositivo. Empregar sistemas de detecção de intrusão para detectar e responder a ataques potenciais.

Ao abordar essas medidas de segurança, as organizações podem minimizar os riscos associados às vulnerabilidades do Device Away Management e melhorar a segurança geral de suas redes IoT.

3.1.8. Configuração Padrão de Conta

O termo "vulnerabilidade de configuração de conta padrão" refere-se a uma falha de segurança que surge quando os dispositivos IoT são implantados com credenciais de login padrão ou mecanismos de autenticação fracos. Essa vulnerabilidade pode expor a rede IoT a acesso não autorizado, comprometer a segurança do dispositivo e potencialmente levar a várias atividades maliciosas (OWASP, 2018)

As vulnerabilidades de configuração de conta padrão prevalecem em dispositivos IoT porque os fabricantes geralmente definem nomes de usuário e senhas padrão para simplificar a instalação e configuração do dispositivo. No

entanto, essa conveniência pode representar um risco de segurança significativo se essas credenciais padrão não forem alteradas pelo proprietário do dispositivo durante a configuração inicial. Essa vulnerabilidade pode ser explorada como se segue:

- a. Credenciais padrão - os invasores podem verificar a Internet em busca de dispositivos IoT usando credenciais de login padrão. Uma vez identificados, eles podem obter acesso não autorizado a esses dispositivos simplesmente usando os nomes de usuário e senhas padrão.
- b. Força bruta de credenciais - nos casos em que as credenciais padrão foram alteradas, mas senhas fracas ou fáceis de adivinhar são usadas, os invasores podem empregar técnicas de força bruta para adivinhar sistematicamente as credenciais corretas e obter acesso não autorizado.
- c. Coleta de credenciais - os invasores podem extrair credenciais padrão de imagens de firmware comprometidas ou publicamente disponíveis ou documentação de dispositivos, permitindo que eles explorem dispositivos que ainda possuem as configurações padrão em vigor.

Depois que um invasor obtém acesso a um dispositivo IoT na rede, ele pode explorá-lo das seguintes maneiras:

- d. Controle não autorizado - os invasores podem manipular as configurações do dispositivo, modificar seu comportamento ou usá-lo como um ponto de articulação para lançar ataques contra outros dispositivos ou a rede mais ampla.
- e. Roubo de dados - dependendo dos recursos do dispositivo, os invasores podem acessar e extrair dados confidenciais, comprometendo a privacidade do usuário ou violando a segurança organizacional.
- f. Recrutamento de *botnet* - dispositivos IoT comprometidos podem ser recrutados para *botnets*, grandes redes de dispositivos comprometidos

controlados por uma única entidade. *Botnets* podem ser explorados para várias atividades maliciosas, como lançar ataques DDoS ou distribuir malware.

Para mitigar a vulnerabilidade de configuração de conta padrão em uma rede IoT, várias práticas recomendadas devem ser seguidas:

- g. Alterar credenciais padrão - sempre altere nomes de usuário e senhas padrão durante a configuração inicial dos dispositivos IoT. Usar senhas fortes e exclusivas que sejam difíceis de adivinhar.
- h. Autenticação segura - implementar mecanismos de autenticação robustos, como autenticação de dois fatores (2FA) ou autenticação multifator (MFA), para adicionar uma camada extra de segurança.
- i. Atualizações regulares de firmware - manter os dispositivos IoT atualizados com o firmware mais recente fornecido pelo fabricante, pois as atualizações geralmente incluem patches e melhorias de segurança.
- j. Segmentação de rede - isolar os dispositivos IoT de sistemas e dados críticos implementando a segmentação de rede. Dessa forma, mesmo que um dispositivo IoT seja comprometido, o impacto potencial na rede geral é limitado.
- k. Inventário e monitoramento de dispositivos - manter um inventário atualizado de todos os dispositivos IoT na rede e monitore regularmente seu comportamento em busca de sinais de acesso não autorizado ou atividade suspeita.
- l. Auditorias de segurança - conduzir auditorias de segurança periódicas de dispositivos IoT para identificar vulnerabilidades e garantir que as medidas de segurança adequadas estejam em vigor.

Ao seguir essas práticas, o risco associado às vulnerabilidades de configuração de conta padrão pode ser significativamente reduzido, aumentando

a segurança da rede IoT e protegendo contra possíveis acessos e explorações não autorizados.

3.1.9. Falta de *Hardening* Físico

O termo "falta de *hardening* físico" refere-se a uma vulnerabilidade em uma rede IoT, onde as medidas de segurança física para os dispositivos são insuficientes ou inexistentes, deixando-os suscetíveis a ataques físicos ou adulterações. Essa vulnerabilidade surge devido a uma falha na implementação de salvaguardas adequadas para proteger a integridade física dos dispositivos IoT (OWASP, 2018).

De acordo com o NIST (2023), aqui estão alguns dos principais aspectos dessa vulnerabilidade:

- a. Acesso não autorizado - sem medidas de proteção física, os dispositivos IoT podem ser facilmente acessados por indivíduos não autorizados. Isso pode incluir invasores obtendo acesso físico direto aos dispositivos ou adulterando-os em trânsito ou durante a instalação.
- b. Adulteração de dispositivos - os invasores podem modificar ou adulterar os dispositivos IoT se faltarem medidas de segurança física. Isso pode envolver a alteração do hardware, firmware ou definições de configuração do dispositivo, podendo levar ao controle ou manipulação não autorizada da funcionalidade do dispositivo.
- c. Manipulação de sensores - em alguns casos, os dispositivos IoT são equipados com sensores para monitorar parâmetros físicos, como temperatura, umidade ou movimento. Sem proteção física adequada, os invasores podem interferir nesses sensores, levando a leituras imprecisas ou dados falsos. Isso pode ter implicações significativas em cenários em que decisões críticas são tomadas com base nos dados coletados por esses sensores.
- d. Ataques físicos - os dispositivos IoT que são facilmente acessíveis e não protegidos fisicamente podem ser fisicamente danificados ou destruídos. Os invasores podem prejudicar ou desativar

intencionalmente os dispositivos, causando interrupção da funcionalidade pretendida ou tornando-os completamente inoperáveis.

- e. Remoção não autorizada de dispositivos - a falta de proteção física também pode resultar na remoção não autorizada de dispositivos IoT de seus locais designados. Isso pode levar à perda de dados, interrupção de serviços ou possível uso indevido dos dispositivos por indivíduos não autorizados.

Para mitigar a vulnerabilidade de falta de proteção física em uma rede IoT, o NIST também apresenta as seguintes medidas que devem ser consideradas:

- f. Ambiente físico seguro - certificar-se de que os dispositivos IoT estejam localizados em áreas seguras onde o acesso físico é restrito ou monitorado. Isso pode envolver a colocação de dispositivos em armários trancados ou salas com acesso limitado.
- g. Embalagem inviolável - implementar embalagens invioláveis para dispositivos IoT durante o envio e a instalação. Isso ajuda a detectar se um dispositivo foi adulterado antes ou durante a implantação.
- h. Bloqueios e barreiras físicas - utilizar bloqueios físicos, lacres de segurança ou barreiras para impedir o acesso não autorizado a dispositivos IoT. Isso inclui a proteção de pontos de acesso, como portas, conectores ou gabinetes de dispositivos.
- i. Autenticação e criptografia de dispositivos - implementar mecanismos de autenticação e protocolos de criptografia fortes para proteger contra controle ou manipulação não autorizada dos dispositivos IoT, mesmo se o acesso físico for obtido.
- j. Monitoramento e Alarme - Implantar sistemas de monitoramento de segurança que podem detectar adulteração física ou acesso não autorizado a dispositivos IoT. Isso permite uma resposta oportuna e ações de mitigação.

- k. Auditoria e manutenção regulares - Realizar auditorias regulares e verificações de manutenção para identificar e corrigir quaisquer deficiências físicas de segurança na rede IoT. Isso inclui verificar a integridade das conexões físicas, inspecionar os compartimentos do dispositivo e atualizar as práticas de segurança.

Ao implementar essas medidas, a falta de vulnerabilidade de proteção física pode ser mitigada, reduzindo o risco de ataques físicos, acesso não autorizado e adulteração em uma rede IoT.

3.2 Ameaças

De acordo com CERT.br (2023) as ameaças em uma rede IoT, referem-se a riscos potenciais que podem comprometer a segurança, a privacidade e a funcionalidade dos dispositivos IoT, bem como a infraestrutura geral da rede. Essas ameaças podem surgir de várias fontes e podem ter efeitos prejudiciais no ecossistema IoT. A seguir estão detalhas as principais ameaças em uma rede IoT de acordo com a OWASP (2018).

3.2.1. Frequência de Ocorrência

A frequência de ocorrência em uma rede IoT refere-se à taxa ou frequência com que incidentes de segurança ocorrem nessa rede. Como a IoT envolve a interconexão de dispositivos físicos por meio da Internet, esses dispositivos podem estar sujeitos a várias ameaças de segurança. Esta ameaça em uma rede IoT, também pode ser determinada pelo número de incidentes de segurança que ocorrem em um determinado período. Esses incidentes podem incluir ataques cibernéticos, exploração de vulnerabilidades, invasões de privacidade, roubo de dados, interrupções de serviço e outros tipos de atividades maliciosas (OWASP, 2018).

A frequência de ocorrência pode variar dependendo de vários fatores, como o número de dispositivos conectados à rede IoT, a natureza dos dispositivos e suas vulnerabilidades, a segurança implementada na rede e a sofisticação dos ataques direcionados à IoT. Uma alta frequência de incidentes na rede pode indicar que ela é alvo de ataques frequentes ou que existem falhas

significativas na segurança. Isso pode resultar em interrupções operacionais, perda de dados, comprometimento da privacidade dos usuários e outros impactos negativos (CERT.br, 2023).

3.2.2. Impacto de Degradação de Rede

Esta ameaça refere-se a qualquer evento ou ação que possa comprometer a funcionalidade, disponibilidade ou desempenho de uma rede IoT, podendo ter efeitos prejudiciais nos dispositivos conectados, bem como nos sistemas e aplicativos que dependem desses dispositivos (OWASP, 2018).

Uma rede IoT é composta por dispositivos interconectados que coletam, trocam e compartilham dados entre si e com outros sistemas. Esses dispositivos podem incluir sensores, medidores inteligentes, câmeras, dispositivos vestíveis e outros objetos conectados. A degradação da rede IoT ocorre quando há uma diminuição na capacidade da rede em fornecer serviços e comunicação confiáveis entre esses dispositivos (CERT.br, 2023).

3.2.3. Impacto Financeiro

As violações de segurança e os ataques cibernéticos podem causar impactos financeiros significativos para as empresas, incluindo custos de reparo sistêmico, perda de dados, multas regulatórias, danos à reputação e possíveis ações judiciais (Kaspersky, 2021).

As interrupções operacionais também podem causar grande impacto financeiro dentro de uma organização, resultando em perda de produtividade, custos de reparo e penalidade contratuais. A duração das indisponibilidades varia amplamente dependendo do incidente específico e da eficácia das medidas de recuperação (IBM, 2019).

Por fim, à medida que as redes IoT crescem em escala, podem surgir desafios financeiros relacionados à expansão da infraestrutura, aquisição de tecnologia atualizada, treinamento de pessoas e um bom gerenciamento dos dados (MCKINSAY, 2019).

3.2.4. Impacto de Queda de Rede

A queda de rede IoT pode ter vários impactos significativos para as empresas. Alguns dos principais impactos incluem na interrupção nas operações, onde pode afetar a capacidade de controlar e monitorar os dispositivos conectados, dependendo da gravidade da interrupção, as operações podem ser paralisadas de forma parcial ou totalmente (CHOUDHARY, 2016).

Muitas empresas dependem da IoT para fornecer serviços inovadores aos clientes, como cidades inteligentes, saúde conectada e monitoramento remoto. Uma queda na rede IoT pode resultar na interrupção desses serviços, causando insatisfação dos clientes e perda de informações (KHAN, 2013).

Por fim, as empresas que dependem da IoT podem enfrentar prejuízos financeiros diretos e indiretos devido a quedas de rede. Isso inclui custos de reparo e manutenção de dispositivos, perda de produtividade, perda de clientes e danos à reputação da marca (FUQAHA, 2016).

Diante das ameaças e vulnerabilidades em uma rede IoT corporativa, torna-se evidente a necessidade da proposição e execução de ações para evitar que as mesmas tragam consequências significativas no que tange à segurança da informação dessas redes. Entretanto, uma vez que essas vulnerabilidades são em grande quantidade, é de fundamental importância que as organizações tenham um plano para o tratamento das mesmas, ou seja, é necessário haver uma priorização do tratamento das vulnerabilidades que mais impactam em uma rede IoT corporativa, levando-se em conta impactos técnicos e financeiros.

Nesse contexto, a utilização de um Método Multicritério pode auxiliar a organização na tomada de decisão sobre quais vulnerabilidades devem ser tratadas de forma prioritária, a partir de uma classificação (ranqueamento) das mesmas, levando-se em conta diferentes critérios, tanto técnicos, quanto financeiros.

4. MÉTODOS MULTICRITÉRIO PARA A TOMADA DE DECISÃO

Este Capítulo apresenta o Método Multicritério utilizado para a classificação (ranqueamento) das vulnerabilidades em uma rede IoT

4.1 Tipos de Métodos Multicritério para Tomada de Decisão

A tomada de decisão multicritério é uma abordagem sistemática usada para avaliar e tomar decisões quando há vários critérios ou objetivos conflitantes a serem considerados. Ela ajuda os tomadores de decisão a analisar problemas complexos, considerando vários fatores simultaneamente, permitindo um processo de tomada de decisão mais abrangente (Hermann, 2007).

Uma ampla gama de fatores deve ser levada em consideração para iniciar um processo de tomada de decisão. Por exemplo: dados científicos, questões éticas e morais e políticas de interesses das partes interessadas. A análise de decisão de multicritério (MCDA, do inglês Multi-Criteria Decision Analysis), é um método que pode combinar esses fatores e auxiliar na tomada de decisão final (CEGAN, 2017). Na década de 1960, foram desenvolvidas diversas técnicas de MCDA, para auxiliar na tomada de decisão por critérios pré-estabelecidos (MENDONZA; MARTINZ, 2006).

A teoria e a metodologia por trás da MCDA estão focadas na resolução de problemas complexos encontrados nos negócios, Engenharia e outras esferas do desenvolvimento humano. Padrões ou metas lucrativos e competitivos, incluindo, eficácia, desempenho, custo, confiabilidade, risco, produtividade e acessibilidade, definem bem este método (ACHILLAS, 2013).

Desde a sua concepção, a MCDA evoluiu tanto em termos de abordagens complexas quanto de métodos simples, mas todos apresentam as seguintes características (THEODOROU; FLORIDES; TASSOU, 2010):

- a. As soluções podem ser avaliadas e classificadas de acordo com a preferência;
- b. Critérios baseados na natureza do problema;

- c. Matriz de valores específicos para cada critério;
- d. Pesos para cada critério;
- e. Avaliação de cada solução alternativa em relação a alternativas.

Uma compreensão muito ampla dos problemas é fornecida pelas abordagens de MCDA. Os tomadores de decisão que estão familiarizados com o assunto se envolvem mais, fazem promessas menos comprometedoras, mais convincentes e mais simples de serem alcançadas (THEODOROU; FLORIDES; TASSOU, 2010).

Existem vários objetivos e critérios frequentemente conflitantes para cada problema. Cada critério tem um peso diferente. A MCDA pode ser visto como uma técnica de avaliação de cenários reais que ocorreram em contextos específicos, usando uma variedade de critérios qualitativos e quantitativos para selecionar o melhor curso de ação, decisão, estratégia ou política de uma variedade de possibilidades acessíveis (THEODOROU; FLORIDES; TASSOU, 2010).

De acordo com Hajkowicz e Collins (2007), as técnicas de MCDA podem ser classificadas da seguinte forma:

- a. **Multi-Attribute Value Theory:** são métodos que podem definir uma expressão para a influência do tomador de decisão usando funções utilidade / valor. Com base nisso, cada critério é convertido em uma escala sem dimensão comum (LINKOV, 2004). Os métodos mais conhecidos são os *Multi-Attribute Utility Theory (MAUT)* e o *Multi-Attribute Value Theory (MAVT)*, que são considerados métodos compensatórios. Significa que mesmo que seu critério seja de menor peso, o mesmo pode ser compensado pelo critério de maior peso. Embora MAUT e MAVT tenham bases bem descritas e similares, a escolha dos critérios o torna um método bem desafiador (SCHUWIRTH; REICHERT; LIENERT, 2012).
- b. **Pairwise comparisons:** este método envolve uma escala pré-determinada, a comparação de pares de critérios indica o quanto um

é mais significativo em comparação ao outro. Quando é impossível estabelecer funções de utilidade, as comparações pareadas são muito úteis; caso contrário, o método MAUT é recomendado (ISHIZAKA; NEMERY, 2013). O MAUT inclui técnicas comuns, como o AHP (*Analytical Hierarchy Process*), ANP (*Analytical Network Process*) e MAC-BETH (*Measuring Attractiveness by a Categorical Based Evaluation Technique*). O AHP é considerado um método MCDM bastante utilizado devido à sua facilidade de uso e adaptabilidade. No entanto, existe uma limitação ao lidar com a interdependência entre os critérios, uma vez que assume que eles são independentes (LI, F.; LI, Y., 2011).

- c. **Outranking approaches:** neste método, define-se que uma alternativa possui maior dominância sobre a outra (KANGAS, LESKINEN, PYKALAINEN, 2001). Esta categoria inclui os seguintes métodos *ELECTRE (Elimination and Choice Expressing Reality)*, *PROMETHEE (The Preference Ranking Organization Method for Enrichment of Evaluations)* e o *SAW (Simple Additive Weighting Method)*. A sua maior vantagem é que evitam a compensação dos pesos entre os critérios e seus processos de normalização (ISHIZAKA; NEMERY, 2013). Esses métodos são recomendados quando as métricas dos critérios não são facilmente definidas (LINKOV, 2004).

Muitos métodos multicritério são citados por diversos autores. A Tabela 1 apresenta os principais Métodos Multicritério descritos na literatura.

Tabela 1: Principais Métodos Multicritério

Acrônimo	Método	Primeira referência
SAW	Ponderação aditiva simples (Simple Additive Weighting)	(HWANG, 1981)
ARAS	Avaliação da relação aditiva (Additive Ration Assessment)	(KERŠULIENE; ZAVADSKAS; TURSKIS, 2010)
SWARA	Análise passo a passo da relação de avaliação de peso (Step-wise Weight Assessment Ration Analysis)	(KERŠULIENE; ZAVADSKAS; TURSKIS, 2010)
TOPSIS	Técnica para ordem de preferência por semelhança com a solução ideal (Technique for Order of Preference by Similarity to Ideal Solution)	(HWANG, 1981)

ELECTRE	Eliminação e escolha que expressam a realidade (Elimination et Choix Traduisant la Réalité, Elimination and Choice Expressing REality)	(BENAYOUN; B. ROY; SUSSMAN., 1966)
LINMAP	Técnica de programação linear para análise multidimensional e preferência (Linear Programming Technique for Multidimensional Analysis and Preference)	(SRINIVASAN; SHOCKER, 1973)
AHP	Analytic Hierarchy Process	(WIND; SAATY, 1980)
ANP	Analytic Network Process	(SAATY, 2001)
PROMETHEE	Método de organização de classificação de preferências para enriquecimento de avaliações (The Preference Ranking Organization Method for Enrichment of Evaluations)	(BRANS; VINCKE, 1985)
MOORA	Otimização multi-objetivo com base na análise Ration (Multi-Objective Optimization on the basis of Ration Analysis)	(BRAUERS, WILLEM KAREL M; ZAVADSKAS, 2010)
MULTIMOORA	Formulário multiplicativo com otimização multiobjetivo com base na análise Ration (Multiplicative form with Multi-Objective Optimization on the basis of Ration Analysis)	(BRAUERS, WILLEM KAREL M; ZAVADSKAS, 2010)
DEA	Data Envelopment Analysis	(AHN; CHARNES; COOPER, 1987)
VIKOR	Solução de otimização e compromisso multicritério (Visekriterijumska optimizacija i Kompromisno Resenje, Multicriteria Optimization and Compromise Solution)	(OPRICOVIC, 2002)
COPRaS	Avaliação Proporcional Complexa (Complex Proportional Assessment)	(ZAVADSKAS, E.K.; KAKLAUSKAS; SARKA, 1994)
Acrônimo	Método	Primeira referência
EVAMIX	Avaliação de dados mistos (Evaluation of Mixed Data)	(VOOGD, 1983)
DEMATEL	Laboratório de avaliação e julgamento (Decision-Making trial and Evaluation Laboratory)	(GABUS; FONTELA, 1973)
WASPAS	Avaliação de produto de soma agregada ponderada (Weighted Aggregated Sum Product Assessment)	(ZAVADSKAS, EDMUNDAS KAZIMIERAS et al., 2012)
WSM	Método da soma ponderada (Weighted Sum Method)	(FISHBURN, 1967)
WPM	Método do Produto Ponderado (Weighted Product Method)	(WANG, MINGXI et al., 2010)*
CP	Compromise Programming	(SRINIVASAN; SHOCKER, 1973)
MAUT	Teoria do utilitário de atributos múltiplos (MultiAttribute Utility Theory)	(KEENEY; RAIFFA, 1976)
CBR	Raciocínio baseado em Casos (Case Based Reasoning)	(SCHENK; JAMES R. PINKERT., 1977)

GA	Algoritmo genético (Genetic Algorithm)	(GOLDBERG; HOLLAND, 1988)
SMART	Técnica simples de classificação de múltiplos atributos (Simple Multi-Attribute Rating Technique)	(KEENEY; RAIFFA, 1976)
MAVT	Teoria do valor de atributos múltiplos (MultiAttribute Value Theory)	(HOSTMANN et al., 2005)
REMBRANDT	Ratio Estimation in Magnitudes or Decibels to Rate Alternatives which are Non-Dominated	(LOOTSMA, 1993)
NAIADE	Nova abordagem para avaliação imprecisa e ambientes de decisão (Novel Approach to Imprecise Assessment and Decision Environments)	(MUNDA, 1995)

4.2 Método SAW (Método de Ponderação Aditiva Simples)

Para este trabalho, será adotado o Método de Tomada de Decisão SAW (Método de Ponderação Aditiva Simples, do inglês Simple Additive Weighting Method), que tem por objetivo apresentar formas de soluções para o problema atual e apoiar no processo decisório a fim de recomendar as principais ações que devem ser tomadas diante do cenário apresentado.

A figura 5 exibe a base da aplicação da proposta, a matriz m por n , não normalizada, os critérios (C_i) são representados pelas ameaças expostas pela OWASP - *Open Web Application Security Project* (Fundação de código aberto para segurança de aplicativos), enquanto as Alternativas (A_j) são representadas pelas principais vulnerabilidades também apresentadas pela comunidade OWASP.

Para cada critério (C_i) relacionado com cada alternativa (A_j) tem-se o valor numérico (v_{ij}) correspondente, onde m são as 4 ameaças em estudo e n são as 9 vulnerabilidades apresentadas.

Figura 5: Matriz não normalizada.

		n columnas \xrightarrow{j}				
			A1	A2	...	A _j
i ↓ m linhas	C1		v11	v12		v1j
	C2		v21	v22		v2j
	⋮		⋮	⋮		⋮
	⋮		⋮	⋮		⋮
	C _i		v _{i1}	v _{i2}		v _{ij}

Para a formação da matriz normalizada, apresentada a seguir na figura 6, realizou-se um estudo preliminar de cada coluna resultante da matriz. Nessa etapa, deve-se atentar a grandeza do valor do elemento (v_{ij}) tido como importante, sendo observado o maior valor (ω) do elemento da coluna, para caso diretamente proporcional, ou observado o menor valor (α) do elemento da coluna, para caso inversamente proporcional.

Figura 6: Matriz Normalizada.

		n colunas \xrightarrow{j}			
		A1	A2	...	Aj
m linhas \downarrow	C1	r11	r12		r1j
	C2	r21	r22		r2j
	⋮	⋮	⋮		⋮
	Ci	ri1	ri2		rij

Caso o valor do elemento (v_{ij}) favorável seja um valor elevado, então usa-se o cálculo para normalização (r_{ij}) de forma a maximizar o valor do atributo positivo, caso contrário, se o valor do elemento (v_{ij}) em análise favorável seja um valor baixo, próximo a zero, então usa-se o cálculo para normalização (r_{ij}) de forma a minimizar o valor do atributo negativo. Os elementos da matriz normalizada (r_{ij}) estão relacionados para análise representados pela Equação 1, a seguir:

$$r_{ij} = \begin{cases} \text{atributo positivo : } \frac{v_{ij}}{\omega} \\ \text{atributo negativo: } \frac{\alpha}{v_{ij}} \end{cases} \quad (\text{Eq. 1})$$

Por fim, a partir da criação da matriz normalizada de decisão Multicritério SAW, se obtém o resultado (S_i) pela somatória dos valores dos critérios normalizados, para cada alternativa (A_i). Cada valor numérico normalizado (r_{ij}) relacionado ao critério (C_i) é multiplicado por um peso, representado pela Equação 2:

$$S_i = \sum_{j=1}^m W_j * r_{ji} \quad (\text{Eq. 2})$$

Onde:

S_i = resultado da i -ésima alternativa, para $i = 1, 2, \dots, m$

m = número total de critérios

W_j = peso atribuído ao j -ésimo critério, para $j = 1, 2, \dots, n$

r_{ij} = valor normalizado da i -ésima alternativa pelo j -ésimo critério

5. METODOLOGIA

A metodologia utilizada neste trabalho foi estudada para atuar em seis grandes passos, orientadas no diagrama de fluxo abaixo e detalhada a seguir.

Figura 7: Principais passos da metodologia proposta.



- a. Passo 1: Levantamento Bibliográfico dos principais desafios relacionados aos aspectos de segurança em redes IoT e seus requisitos de implantação.
- b. Passo 2: Revisão Bibliográfica das melhores práticas de segurança de redes de maneira geral e levantamento das principais vulnerabilidades e ameaças em redes IoT.
- c. Passo 3: Definição das principais vulnerabilidades (alternativas do Método SAW) e critérios que mais impactam essas vulnerabilidades em uma rede IoT corporativa.
- d. Passo 4: Elencar, junto a um grupo de especialistas da área de Tecnologia da Informação, a influência (impacto) dos critérios definidos no Passo 3 nas principais vulnerabilidades (também definidas no passo anterior), por meio da submissão de um questionário para esses especialistas, encontrado no Apêndice A deste documento. As respostas a esse questionário são utilizadas para o ranqueamento das principais vulnerabilidades em uma Rede IoT corporativa, conforme detalhado posteriormente neste trabalho.
- e. Passo 5: Aplicação de método multicritério para classificação (ranqueamento/classificação) das vulnerabilidades e ameaças em redes IoT.

- f. Passo 6: Com base na classificação obtida no Passo 5, proposição de ações de segurança, com intuito de colaborar para a proteção dos dispositivos, dados e informações que compõem essas redes, tornando-as menos vulneráveis e susceptíveis a ameaças.

5.1 Considerações Sobre a Pesquisa

A realização desta pesquisa deve apoiar a identificação de pontos fracos, avaliar riscos, garantia da conformidade, aumentar a segurança e permitir melhorias contínuas em uma rede IoT. Ao lidar proativamente com as vulnerabilidades, as organizações podem fortalecer a postura de segurança de suas redes e mitigar possíveis riscos e ameaças.

5.2 Definições das Alternativas e Critérios

As alternativas utilizadas no Método SAW, consideradas neste trabalho, correspondem às principais vulnerabilidades que uma rede IoT corporativa está sujeita, de acordo com a referência (OWASP, 2017). Embora a tecnologia IoT ofereça inúmeros benefícios, como maior eficiência, automação e conveniência, ela também apresenta vários riscos que podem ser explorados por criminosos do meio digital.

Já para a definição dos critérios para aplicação do Método SAW foram baseadas nos impactos que as vulnerabilidades definidas no item anterior causam nesses critérios. Ou seja, foram escolhidos critérios, de acordo com a referência (OWASP, 2017) que possuem correlação, em maior ou menor grau, com as vulnerabilidades definidas.

5.3 Formulário Fornecido aos Especialistas

De forma específica, conforme mencionado no capítulo de Metodologia, no Passo 4 consiste em uma pesquisa de campo, utilizando como método o levantamento de dados relacionados à segurança da informação em redes IoT. A ferramenta utilizada para captação das colaborações ou respostas dos especialistas corresponde ao aplicativo Microsoft Forms, um formulário online, disponibilizado por meio da plataforma e ferramental da empresa Microsoft. A Figura 8 ilustra como o formulário foi disponibilizado para esses especialistas, é

importante salientar que a aplicação desse questionário foi autorizada pelo Comitê de Ética em Pesquisa da Pontifícia Universidade Católica de Campinas.

Figura 8: Formulário Concedido para os Especialistas.

Análise de Vulnerabilidades e Ameaças em Redes IoT

Esta pesquisa tem como objetivo analisar as principais vulnerabilidades e ameaças exploradas por criminosos cibernéticos em redes IoT corporativas e domésticas, com foco em classificar essas vulnerabilidades e ameaças quanto a seu impacto nas redes mencionadas. Nessa classificação, serão considerados impactos técnicos, econômicos e as especificidades de uma rede IoT.

A metodologia será baseada na resposta deste questionário, visando elencar, junto a um grupo de especialistas da área de Tecnologia e Segurança da Informação, as principais fragilidades de uma rede composta por ativos de tecnologia, especialmente nos ambientes de trabalho que efetivamente sofrem com tais ameaças, com foco nas práticas utilizadas por atacantes, que visam explorar desde a degradação dos serviços de um dispositivo até o sequestro dos dados ou acessos.

Aluna do curso de Mestrado em Engenharia Elétrica Gabriella Barbuti.

* Required

Antes de responder a pesquisa é necessário responder os campos a seguir: [?]

1. Favor informar sua Nacionalidade: * [?]

Brasileira

Outra

2. Atualmente você trabalha na área de Tecnologia e Segurança da Informação? * [?]

Sim, atuo na área.

Não, mas já atuei.

Next

This content is created by the owner of the form. The data you submit will be sent to the form owner. Microsoft is not responsible for the privacy or security practices of its customers, including those of this form owner. Never give out your password.

Análise de Vulnerabilidades e Ameaças em Redes IoT

* Required

Questionário [?]

3. Atribua a correlação entre o critério **Frequência de Ocorrência** e cada uma das vulnerabilidades (**senhas frágeis de fácil decodificação, serviços e interfaces de rede inseguros, etc**) de acordo com a gradação a seguir.

Deve-se escolher um grau de correlação onde:

1 - Representa **Não há Correlação**
 3 - Representa **Correlação Baixa**
 5 - Representa **Correlação Mediana**
 7 - Representa **Correlação Alta**
 9 - Representa **Correlação Extrema**

	1	3	5	7	9
Senhas frágeis de fácil decodificação	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Serviços e interfaces de rede inseguros	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falta de mecanismo de atualização segura	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Uso de componentes inseguros ou desatualizados	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Proteção de privacidade insuficiente	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Transferência e armazenamento de dados inseguros	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Para ilustrar o fluxo da pesquisa, a Figura 9 apresenta os 4 passos necessários para conclusão da captação dos dados.

Figura 9: Fluxo para captação das respostas dos especialistas.



Ao todo, 33 especialistas responderam ao questionário e suas respostas estão apresentadas no Apêndice 1 deste trabalho.

Foram disponibilizadas 5 questões, para cada especialista responder de acordo com seu conhecimento e experiência na área. As perguntas realizadas

possuem o mesmo grau de interpretação, onde somente os critérios de avaliação se alteram. A seguir as questões que foram concedidas aos especialistas:

Questão 1: Atribua a correlação entre o critério **Frequência de Ocorrência** e cada uma das vulnerabilidades (senhas frágeis de fácil decodificação, serviços e interfaces de rede inseguros etc.) de acordo com a gradação a seguir.

Questão 2: Atribua a correlação entre o **critério Impacto de Degradação de Rede** e cada uma das vulnerabilidades (senhas frágeis de fácil decodificação, serviços e interfaces de rede inseguros etc.) de acordo com a gradação a seguir.

Questão 3: Atribua a correlação entre o critério **Impacto Financeiro** e cada uma das vulnerabilidades (senhas frágeis de fácil decodificação, serviços e interfaces de rede inseguros etc.) de acordo com a gradação a seguir.

Questão 4: Atribua a correlação entre o critério **Impacto de Queda de Rede** e cada uma das vulnerabilidades (senhas frágeis de fácil decodificação, serviços e interfaces de rede inseguros etc.) de acordo com a gradação a seguir.

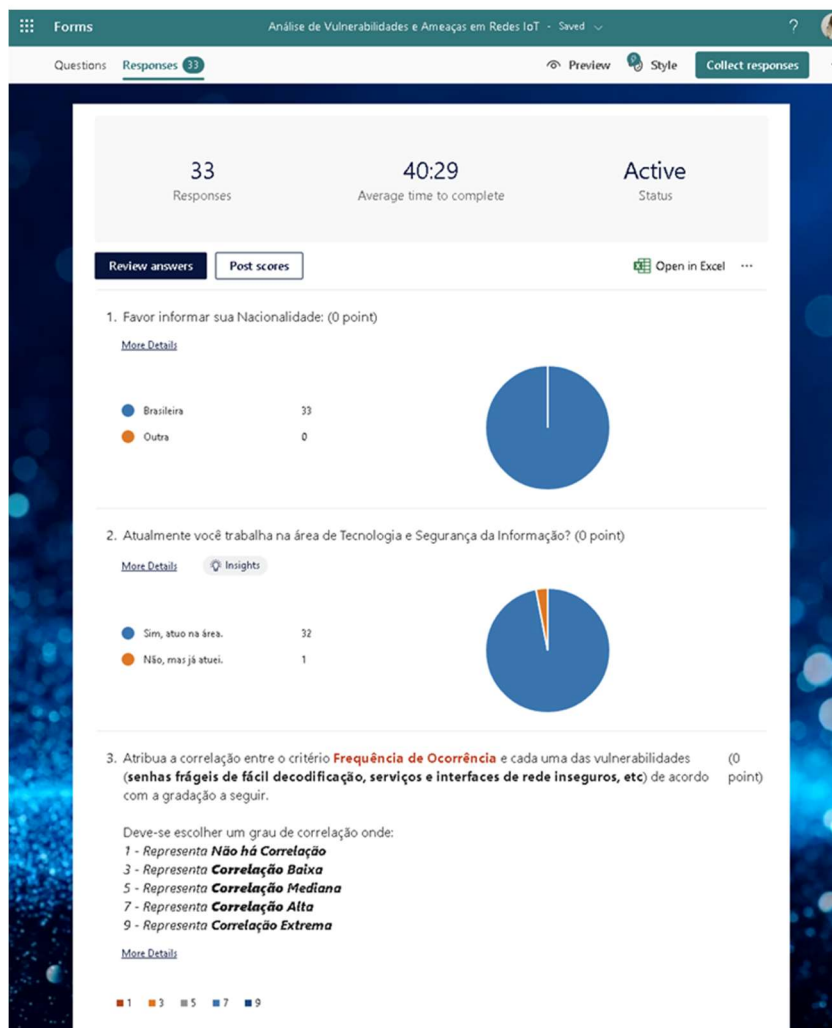
Questão 5: Que outros impactos você considera que sejam incluídos para a classificação das ameaças e vulnerabilidades em uma rede IoT?

Para todas as questões (com exceção da Questão 5), os especialistas deveriam optar por uma dentre as seguintes respostas:

- 1 - Representa que Não há Correlação
- 3 - Representa Correlação Baixa
- 5 - Representa Correlação Mediana
- 7 - Representa Correlação Alta
- 9 - Representa Correlação Extrema

A Figura 10 apresenta a síntese de algumas respostas efetuadas pelos especialistas, para ilustrar o formato dos bastidores da recepção dos dados.

Figura 10: Respostas dos Especialistas.



5.4 Aplicação do Método SAW e Coleta de Dados

Para aplicação do Método SAW, foram definidos 4 critérios com seus respectivos pesos e 9 alternativas, a partir da referência (OWASP, 2013). Os pesos atribuídos a cada um dos critérios foram variados, gerando 6 diferentes cenários estudados.

A Figura 11 ilustra a matriz de comparação por pares onde pode-se observar os critérios (nas linhas) e as alternativas, ou vulnerabilidades, (nas colunas). Cada elemento dessa tabela corresponde ao valor da correlação entre a alternativa (coluna) e o critério (linha), que foi definido a partir de uma média coletada das respostas dos especialistas ao questionário citado anteriormente.

Figura 11: Critérios e alternativas para aplicação do método SAW.

	Alternativas								
	Senhas frágeis de fácil decodificação	Serviços e interfaces de rede inseguros	Falta de mecanismo de atualização segura	Uso de componentes inseguros ou desatualizados	Proteção de privacidade insuficiente	Transferência e armazenamento de dados inseguros	Falta de gerenciamento de dispositivos	Configurações padrão de contas	Falta de Hardening Físico
Frequência de ocorrência	0,20	0,40	0,10	0,10	0,20	0,20	0,30	0,35	0,15
Impacto de degradação de rede	0,40	0,30	0,30	0,40	0,30	0,35	0,10	0,35	0,40
Impacto financeiro	0,40	0,10	0,30	0,30	0,20	0,10	0,20	0,10	0,30
Impacto de queda de rede	0,20	0,20	0,30	0,20	0,30	0,35	0,40	0,20	0,15

A matriz ilustrada na Figura 11 foi, então, normalizada para aplicação do método SAW. A normalização da matriz é realizada dividindo-se cada elemento de cada coluna pelo valor máximo da mesma coluna. A linha em verde que aparece na figura 12, representa a soma dos elementos de cada coluna da matriz normalizada.

Figura 12: Matriz normalizada.

	Senhas frágeis de fácil decodificação	Serviços e interfaces de rede inseguros	Falta de mecanismo de atualização	Uso de componentes inseguros ou	Proteção de privacidade insuficiente	Transferência e armazenamento	Falta de gerenciamento de dispositivos	Configurações padrão de contas	Falta de Hardening Físico
Frequência de ocorrência	0,500	1,000	0,333	0,250	0,667	0,571	0,750	1,000	0,375
Impacto de degradação de rede	1,000	0,750	1,000	1,000	1,000	1,000	0,250	1,000	1,000
Impacto financeiro	1,000	0,250	1,000	0,750	0,667	0,286	0,500	0,286	0,750
Impacto de queda de rede	0,500	0,500	1,000	0,500	1,000	1,000	1,000	0,571	0,375
SOMA	3,000	2,500	3,333	2,500	3,333	2,857	2,500	2,857	2,500

Dando sequência a aplicação do Método SAW, foi determinado um ranking, para classificar as vulnerabilidades, de acordo com a equação:

$$Score\ i = w1 * x1i + w2 * x2i + \dots + wn * xni$$

Onde w é o peso de cada critério, x é o valor normalizado de cada critério para a alternativa i e n é o número de critérios. A alternativa com maior pontuação (Score) é a alternativa que aparece em primeiro lugar no ranking, conforme ilustrado na figura 13.

Figura 13: Determinação do Ranking das vulnerabilidades

	Senhas frágeis de fácil decodificação	Serviços e interfaces de rede	Falta de mecanismo de atualização	Uso de componentes inseguros ou desatualizados	Proteção de privacidade insuficiente	Transferência e armazenamen	Falta de gerenciamento de	Configurações padrão de contas	Falta de Hardening Físico
Frequência de ocorrência	0,125	0,250	0,083	0,063	0,167	0,143	0,188	0,250	0,094
Impacto de degradação de rede	0,250	0,188	0,250	0,250	0,250	0,250	0,063	0,250	0,250
Impacto financeiro	0,250	0,063	0,250	0,188	0,167	0,071	0,125	0,071	0,188
Impacto de queda de rede	0,125	0,125	0,250	0,125	0,250	0,250	0,250	0,143	0,094
SOMA	0,750	0,625	0,833	0,625	0,833	0,714	0,625	0,714	0,625
RANKING	Senhas frágeis de fácil decodificação	Serviços e interfaces de rede inseguros	Falta de mecanismo de atualização segura	Uso de componentes inseguros ou desatualizados	Proteção de privacidade insuficiente	Transferência e armazenamento de dados inseguros	Falta de gerenciamento de dispositivos	Configurações padrão de contas	Falta de Hardening Físico
	3	6	1	6	1	4	6	5	6

5.5 Cenários Avaliados

Foram avaliados 6 cenários com objetivo de qualificar de acordo com a experiência dos especialistas e serão apresentados em formato de matrizes segregadas para tomada de decisão e são elas:

- Caso 1 - Base
- Caso 2 - Frequência de ocorrência
- Caso 3 - Impacto de degradação de rede
- Caso 4 - Impacto financeiro
- Caso 5 – Impacto de queda de rede
- Caso 6 – Pesos fornecidos pelos especialistas

Cenário 1 – Caso Base

Neste Cenário, a figura 14 representa uma tabela onde a primeira coluna representa os critérios e a primeira linha representa as alternativas. Considerando que todos os 4 critérios avaliados possuem o mesmo peso (0,25), visando a determinação de um ranking das vulnerabilidades em que todos os critérios possuem a mesma importância.

Figura 14: Matriz de comparação considerando pesos iguais para todos os critérios.

	Senhas frágeis de fácil decodificação	Serviços e interfaces de rede	Falta de mecanismo de atualização	Uso de componentes inseguros ou desatualizados	Proteção de privacidade insuficiente	Transferência e armazenamento	Falta de gerenciamento de dispositivos	Configurações padrão de contas	Falta de Hardening Físico
Frequência de ocorrência	0,125	0,250	0,083	0,063	0,167	0,143	0,188	0,250	0,094
Impacto de degradação de rede	0,250	0,188	0,250	0,250	0,250	0,250	0,063	0,250	0,250
Impacto financeiro	0,250	0,063	0,250	0,188	0,167	0,071	0,125	0,071	0,188
Impacto de queda de rede	0,125	0,125	0,250	0,125	0,250	0,250	0,250	0,143	0,094
SOMA	0,750	0,625	0,833	0,625	0,833	0,714	0,625	0,714	0,625

Cenário 2 – Frequência de Ocorrência:

Neste cenário, considerou-se que o critério representado fosse “Frequência de ocorrência”, representado pelo círculo em vermelho na figura 15. O peso definido para este critério foi de 0,4 e todos os demais critérios peso 0,2, visando a determinação de um ranking das vulnerabilidades em que a Frequência de ocorrência possui maior importância do que os demais critérios.

Figura 15: Matriz de comparação considerando peso maior para o critério Frequência de Ocorrência.

	Senhas frágeis de fácil decodificação	Serviços e interfaces de rede inseguros	Falta de mecanismo de atualização segura	Uso de componentes inseguros ou desatualizados	Proteção de privacidade insuficiente	Transferência e armazenamento de dados inseguros	Falta de gerenciamento de dispositivos	Configurações padrão de contas	Falta de Hardening Físico
Frequência de ocorrência	0,200	0,400	0,133	0,100	0,267	0,229	0,300	0,400	0,150
Impacto de degradação de rede	0,200	0,150	0,200	0,200	0,200	0,200	0,050	0,200	0,200
Impacto financeiro	0,200	0,050	0,200	0,150	0,133	0,057	0,100	0,057	0,150
Impacto de queda de rede	0,100	0,100	0,200	0,100	0,200	0,200	0,200	0,114	0,075
SOMA	0,700	0,700	0,733	0,550	0,800	0,686	0,650	0,771	0,575

Cenário 3 - Impacto de degradação de rede

Neste cenário, considerou-se que o critério representado fosse “Impacto de degradação de rede”, representado pelo círculo em vermelho na figura 16. O peso definido para este critério foi de 0,4 e todos os demais critérios peso 0,2, visando a determinação de um ranking das vulnerabilidades em que a Frequência de ocorrência possui maior importância do que os demais critérios.

Figura 16: Matriz de comparação considerando peso maior para o critério Impacto de degradação de rede.

	Senhas frágeis de fácil decodificação	Serviços e interfaces de rede inseguros	Falta de mecanismo de atualização segura	Uso de componentes inseguros ou desatualizados	Proteção de privacidade insuficiente	Transferência e armazenamento de dados inseguros	Falta de gerenciamento de dispositivos	Configurações padrão de contas	Falta de Hardening Físico
Frequência de ocorrência	0,100	0,200	0,067	0,050	0,133	0,114	0,150	0,200	0,375
Impacto de degradação de rede	0,400	0,300	0,400	0,400	0,400	0,400	0,100	0,400	0,400
Impacto financeiro	0,200	0,050	0,200	0,150	0,133	0,057	0,100	0,057	0,150
Impacto de queda de rede	0,100	0,100	0,200	0,100	0,200	0,200	0,200	0,114	0,075
SOMA	0,800	0,650	0,867	0,700	0,867	0,771	0,550	0,771	1,000

Cenário 4 - Impacto financeiro

Neste cenário, considerou-se que o critério representado fosse “Impacto financeiro”, representado pelo círculo em vermelho na figura 17. O peso definido para este critério foi de 0,4 e todos os demais critérios peso 0,2, visando a determinação de um ranking das vulnerabilidades em que a Frequência de ocorrência possui maior importância do que os demais critérios.

Figura 17: Matriz de comparação considerando peso maior para o critério Impacto Financeiro.

	Senhas frágeis de fácil decodificação	Serviços e interfaces de rede inseguros	Falta de mecanismo de atualização segura	Uso de componentes inseguros ou desatualizados	Proteção de privacidade insuficiente	Transferência e armazenamento de dados inseguros	Falta de gerenciamento de dispositivos	Configurações padrão de contas	Falta de Hardening Físico
Frequência de ocorrência	0,100	0,200	0,067	0,050	0,133	0,114	0,150	0,200	0,075
Impacto de degradação de rede	0,200	0,150	0,200	0,200	0,200	0,200	0,050	0,200	0,200
Impacto financeiro	0,400	0,100	0,400	0,300	0,267	0,114	0,200	0,114	0,300
Impacto de queda de rede	0,100	0,100	0,200	0,100	0,200	0,200	0,200	0,114	0,075
SOMA	0,800	0,550	0,867	0,650	0,800	0,629	0,600	0,629	0,650

Cenário 5 - Impacto de Queda de Rede

Neste cenário, considerou-se que o critério representado fosse “Impacto de queda de rede”, representado pelo círculo em vermelho na figura 18. O peso definido para este critério foi de 0,4 e todos os demais critérios peso 0,2, visando a determinação de um ranking das vulnerabilidades em que a Frequência de ocorrência possui maior importância do que os demais critérios.

Figura 18: Matriz de comparação considerando peso maior para o critério Impacto de queda de rede.

	Senhas frágeis de fácil decodificação	Serviços e interfaces de rede inseguros	Falta de mecanismo de atualização segura	Uso de componentes inseguros ou desatualizados	Proteção de privacidade insuficiente	Transferência e armazenamento de dados inseguros	Falta de gerenciamento de dispositivos	Configurações padrão de contas	Falta de Hardening Físico
Frequência de ocorrência	0,100	0,200	0,067	0,050	0,133	0,114	0,150	0,200	0,075
Impacto de degradação de rede	0,200	0,150	0,200	0,200	0,200	0,200	0,050	0,200	0,200
Impacto financeiro	0,200	0,050	0,200	0,150	0,133	0,057	0,100	0,057	0,150
Impacto de queda de rede	0,200	0,200	0,400	0,200	0,400	0,400	0,400	0,229	0,150
SOMA	0,700	0,600	0,867	0,600	0,867	0,771	0,700	0,686	0,575

Cenário 6 – Pesos fornecidos pelos especialistas

Neste cenário, a figura 19 ilustra os pesos fornecidos pelos especialistas, considerando o resultado extraído do formulário. Para obter este resultado, foi calculado a quantidade de vezes que uma vulnerabilidade apareceu nas 3 (três) primeiras colocações considerando os 4 (quatro) critérios: Frequência de ocorrência, Impacto de degradação de rede, Impacto Financeiro e Impacto de queda de rede.

Figura 19: Matriz de comparação considerando pesos fornecidos pelos especialistas.

	Senhas frágeis de fácil decodificação	Serviços e interfaces de rede inseguros	Falta de mecanismo de atualização segura	Uso de componentes inseguros ou desatualizados	Proteção de privacidade insuficiente	Transferência e armazenamento de dados inseguros	Falta de gerenciamento de dispositivos	Configurações padrão de contas	Falta de Hardening Físico
Frequência de ocorrência	0,500	1,000	0,333	0,250	0,667	0,571	0,750	1,000	0,375
Impacto de degradação de rede	1,000	0,750	1,000	1,000	1,000	1,000	0,250	1,000	1,000
Impacto financeiro	1,000	0,250	1,000	0,750	0,667	0,286	0,500	0,286	0,750
Impacto de queda de rede	0,500	0,500	1,000	0,500	1,000	1,000	1,000	0,571	0,375
SOMA	3,000	2,500	3,333	2,500	3,333	2,857	2,500	2,857	2,500

6. RESULTADOS

6.1 Resultado do Cenário 1 – Caso Base

É possível observar na figura 20 a vulnerabilidade de maior relevância para este Cenário (Caso Base) é a “Proteção de privacidade insuficiente”, que se refere à inadequação das medidas tomadas para proteger as informações pessoais que são coletadas e processadas pelos dispositivos conectados.

Figura 20: Ranking para o Cenário 1.



Os dispositivos IoT coletam uma grande quantidade de dados sobre os usuários, incluindo sua localização, comportamento, preferências e estado de saúde, entre outros. Esses dados são transmitidos pela Internet e provedores de serviços, fabricantes e anunciantes.

Um dos principais desafios com a privacidade da IoT é que muitos dispositivos carecem de recursos de segurança adequados, tornando-os vulneráveis a hackers e acesso não autorizado. Isso significa que os agentes

mal-intencionados podem interceptar e explorar dados confidenciais do usuário, como informações financeiras, registros médicos e até imagens de vigilância. Além disso, os dispositivos IoT geralmente coletam dados sem o conhecimento ou consentimento dos usuários, criando um risco significativo de uso indevido destes dados.

Outra questão é a falta de políticas e regulamentos de privacidade padronizados para dispositivos IoT. Com tantos dispositivos e fabricantes diferentes, não existe uma estrutura unificada para proteger a privacidade do usuário em todo seu ecossistema. Isso pode criar confusão para os usuários, que podem não saber quais dados estão sendo coletados ou como estão sendo usados.

6.2 Resultado do Cenário 2 – Frequência de Ocorrência

Neste Cenário, o critério “Frequência de Ocorrência” foi ponderado com um peso maior que os demais critérios. Dessa maneira, a figura 21 exhibe que o resultado obtido atesta que quando se considera o critério “Frequência de Ocorrência” como sendo o mais importante, a vulnerabilidade mais relevante é a “Proteção de Privacidade Insuficiente”, indicando, portanto, que essa é a vulnerabilidade mais frequente em uma rede IoT corporativa. Esse resultado foi o mesmo que o obtido para o Cenário 1.

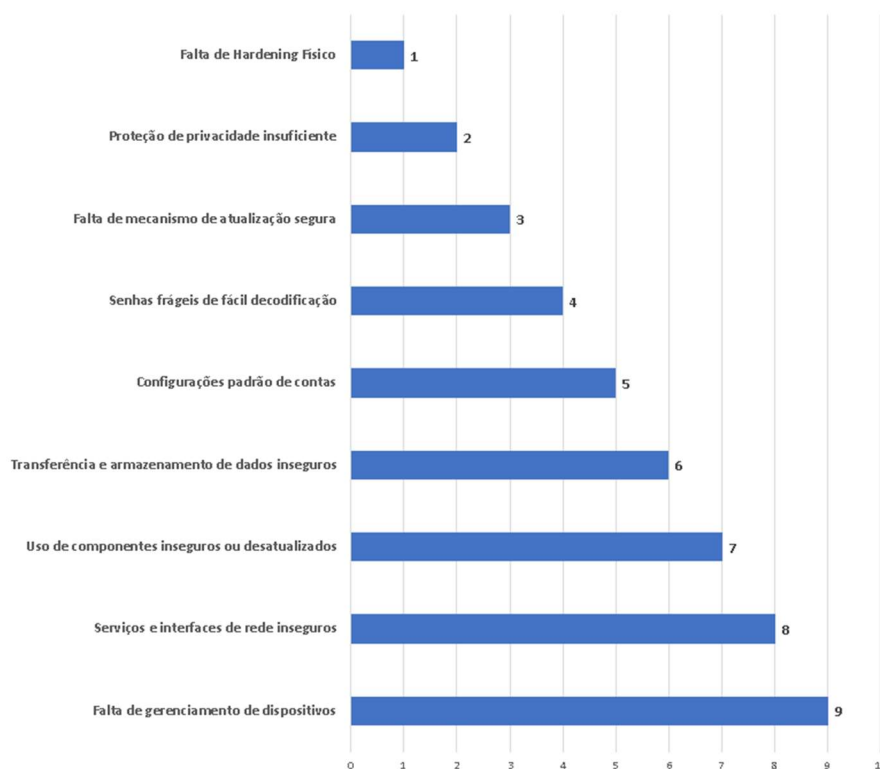
Figura 21: Ranking para o Cenário 2.



6.3 Resultado do Cenário 3 – Impacto de Degradação de Rede

Já para este cenário, o critério “Impacto de Degradação de Rede” foi ponderado com um peso maior que os demais critérios. Dessa maneira, podemos observar na figura 22 que o resultado obtido atesta que quando se considera o critério “Impacto de Degradação de Rede” como sendo o mais importante, a vulnerabilidade mais relevante é a “Falta de *Hardening* Físico”, indicando, portanto, que a “Falta de *Hardening* Físico” é a vulnerabilidade que mais afeta o “Impacto de Degradação de Rede”.

Figura 22: Ranking para o Cenário 3.



O “Impacto de Degradação de Rede”, está relacionado com queda na qualidade do acesso, latência e indisponibilidade parcial de um ambiente de rede empresarial. Os resultados apontam que esse impacto está fortemente relacionado à “Falta de *Hardening* Físico”, termo que, geralmente, se refere a uma situação em que o sistema não foi projetado ou construído com proteções físicas adequadas para resistir a certos tipos de ameaças.

Por exemplo, no contexto da segurança cibernética, a falta de proteção física pode se referir a uma falha em proteger o acesso físico a sistemas e infraestrutura críticas. Isso pode incluir, não usar bloqueios fortes e controles de acessos, não monitorar o acesso físico a data centers, salas de servidores ou não implementar controles ambientais para proteger o hardware de temperaturas extremas, umidade ou outras tensões físicas.

No geral, a falta de proteção física pode deixar sistemas e infraestruturas vulneráveis a danos e interrupções. É importante considerar a proteção física como parte de uma estratégia abrangente de gerenciamento de riscos para qualquer sistema ou infraestrutura crítica.

6.4 Resultado do Cenário 4 – Impacto Financeiro

Neste Cenário, o critério “Impacto Financeiro” foi ponderado com um peso maior que os demais critérios. Dessa maneira, o resultado obtido exibido na figura 23, atesta que quando se considera o critério “Impacto Financeiro” como sendo o mais importante, a vulnerabilidade mais relevante é a “Falta de Mecanismos de Atualização Seguro”, indicando, portanto, que a “Falta de Mecanismos de Atualização Seguro” é a vulnerabilidade que mais afeta o “Impacto Financeiro”.

Figura 23: Ranking para o Cenário 4.



A vulnerabilidade “Falta de Mecanismos de Atualização Seguro” está intimamente ligada a uma situação em que um sistema de software ou dispositivo não possui uma maneira confiável e segura de atualizar seu software ou firmware. Isso pode ser um problema sério porque as atualizações geralmente contêm patches de segurança importantes que abordam vulnerabilidades que

foram descobertas no sistema. Sem um mecanismo de atualização seguro, os invasores podem explorar essas vulnerabilidades e comprometer o sistema.

Em alguns casos, a Falta de Mecanismos de Atualização Seguro pode ocorrer devido às limitações técnicas ou falhas de design no sistema. Por exemplo, alguns sistemas mais antigos podem não ter sido projetados com atualizações de segurança em mente ou podem não ter os componentes de hardware ou software necessários para dar suporte a atualizações seguras.

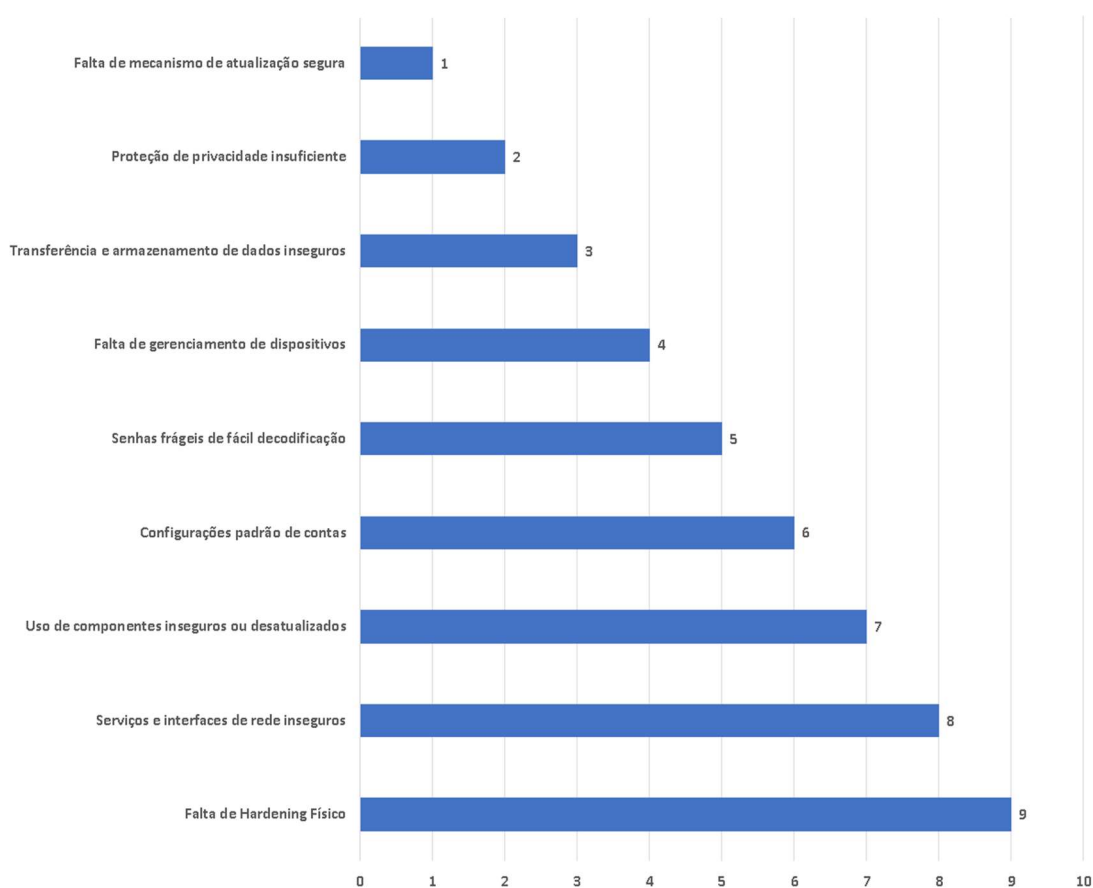
Em outros casos, a Falta de Mecanismos de Atualização Seguro pode ser devida a negligência ou descuido do fabricante ou desenvolvedor. Por exemplo, uma empresa pode deixar de fornecer atualizações regulares de segurança para um produto ou pode não priorizar a segurança no processo de desenvolvimento do produto.

Independentemente da causa, a falta de um mecanismo seguro de atualização pode deixar sistemas e dispositivos vulneráveis a ataques, e é importante que os usuários estejam cientes desse risco e tomem as devidas precauções para se proteger. Isso pode incluir verificar e instalar regularmente atualizações de software, usar medidas de segurança adicionais, como firewalls ou software de antivírus, e ser cautelosos ao abrir anexos de e-mail ou clicar em links de fontes desconhecidas.

6.5 Resultado do Cenário 5 – Impacto de Queda de Rede

Neste Cenário, o critério “Impacto de Queda de Rede” foi ponderado com um peso maior que os demais critérios. Dessa maneira, o resultado obtido atesta que quando se considera o critério “Impacto de Queda de Rede” como sendo o mais importante, a vulnerabilidade mais relevante é a “Falta de Mecanismo de Atualização Seguro”, indicando, portanto, que a “Falta de Mecanismo de Atualização Seguro” é a vulnerabilidade que mais afeta o “Impacto de Queda de Rede”. Esse resultado foi o mesmo que o obtido para o Cenário 4.

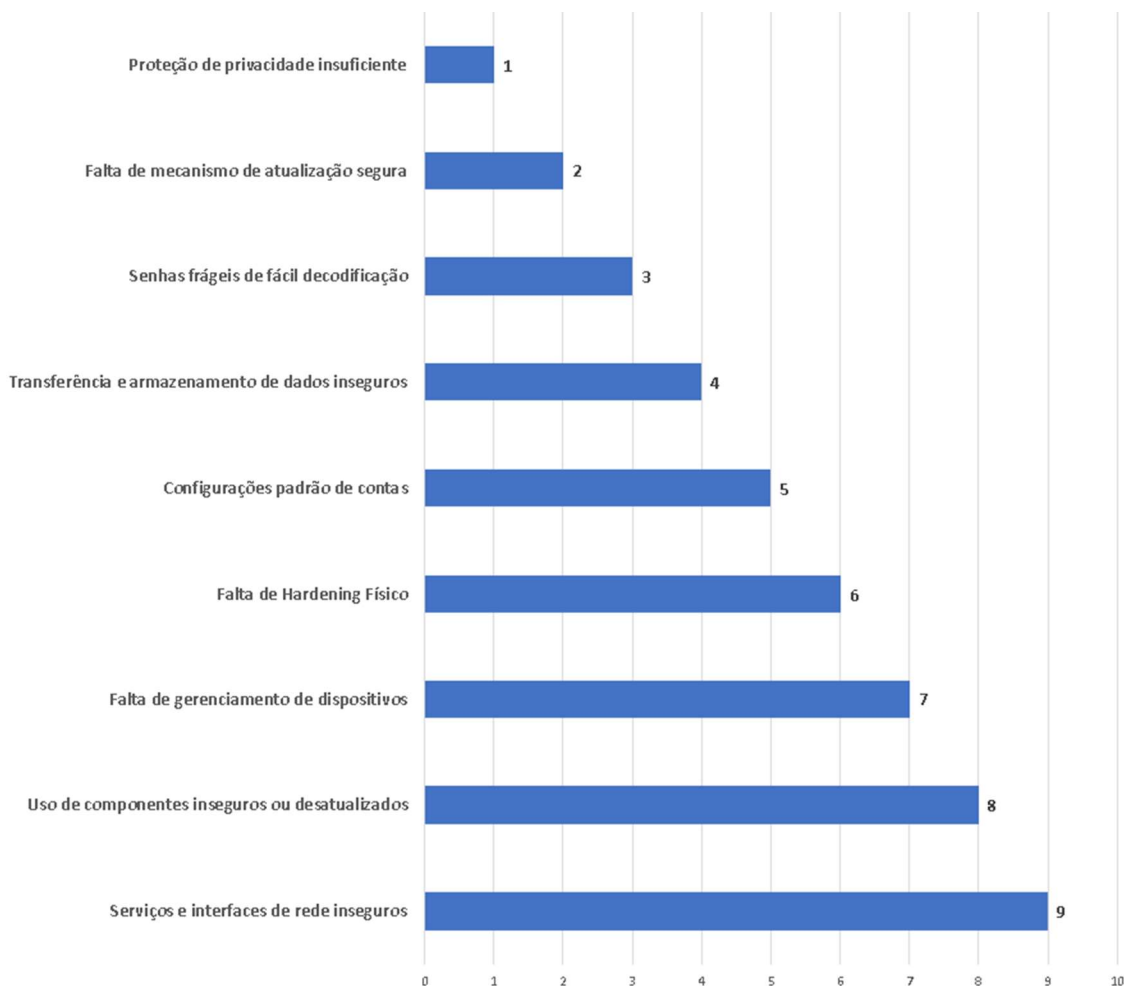
Figura 24: Ranking para o Cenário 5.



6.6 Resultados do Cenário 6 – Pesos Definidos Pelos Especialistas

Para este cenário, os pesos dos critérios foram estabelecidos pelos especialistas, com o intuito de se determinar qual vulnerabilidade é de maior relevância, considerando a experiência desses profissionais. Nesse Cenário, a vulnerabilidade mais relevante é a “Proteção de Privacidade Insuficiente”, indicando, portanto, que essa é a vulnerabilidade mais significativa, quando se considera a experiência dos especialistas. Esse resultado foi o mesmo que o obtido para os Cenários 1 e 2.

Figura 25: Ranking para o Cenário 6.



7. ANÁLISE E DISCUSSÕES

Para analisar, de forma numérica, a criticidade de cada vulnerabilidade, ou seja, a relevância de cada vulnerabilidade em uma rede IoT corporativa, foi criado um índice denominado de Índice de Criticidade (IC). Esse índice é calculado pela Equação (2).

$$IC^i = \frac{n}{nc} \quad \text{Eq. (2)}$$

Onde "n" corresponde ao número de vezes que a vulnerabilidade "i" aparece nas 3 primeiras colocações do ranking e "nc" é o número de cenário analisados (nc = 6 neste trabalho).

- Para a Vulnerabilidade 1 – Senhas frágeis de fácil decodificação:

$$IC^1 = \frac{3}{6} = 0,5$$

- Para a Vulnerabilidade 2 – Serviços de interfaces de rede inseguros:

$$IC^2 = \frac{0}{6} = 0$$

- Para a Vulnerabilidade 3 – Falta de mecanismo de atualização seguro:

$$IC^3 = \frac{5}{6} = 0,83$$

- Para a Vulnerabilidade 4 – Uso de componentes inseguros ou desatualizados:

$$IC^4 = \frac{0}{6} = 0$$

- Para a Vulnerabilidade 5 – Proteção de privacidade insuficiente:

$$IC^5 = \frac{5}{6} = 0,83$$

- Para a Vulnerabilidade 6 – Transferência e armazenamento de dados inseguros:

$$IC^6 = \frac{2}{6} = 0,33$$

- Para a Vulnerabilidade 7 – Falta de gerenciamento de dispositivos:

$$IC^7 = \frac{0}{6} = 0$$

- Para a Vulnerabilidade 8 – Configuração padrão de contas:

$$IC^8 = \frac{1}{6} = 0,17$$

- Para a Vulnerabilidade 9 – Falta de *Hardening* Físico:

$$IC^9 = \frac{2}{6} = 0,33$$

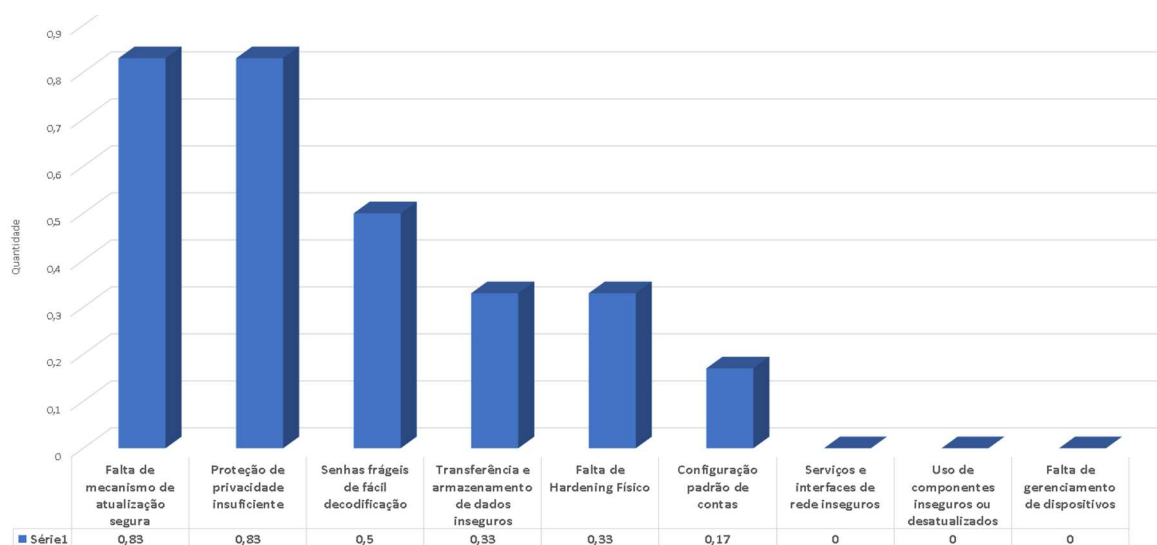
A Tabela 03 sintetiza esses resultados.

Tabela 2: Índice de Criticidade para as 9 Vulnerabilidades

Vulnerabilidade	IC
Senhas frágeis de fácil decodificação	0,5
Serviços de interfaces de rede inseguros	0
Falta de mecanismo de atualização seguro	0,83
Uso de componentes inseguros ou desatualizados	0
Proteção de privacidade insuficiente	0,83
Transferência e armazenamento de dados inseguros	0,33
Falta de gerenciamento de dispositivos	0
Configuração padrão de contas	0,17
Falta de <i>Hardening</i> Físico	0,33

A figura 26 ilustra, de forma gráfica o Índice de Criticidade para cada uma das vulnerabilidades.

Figura 26: Índice de Criticidade das vulnerabilidades.



A partir dos resultados obtidos, pode-se afirmar que as 3 vulnerabilidades de maior relevância em uma rede IoT corporativa são: Falta de um mecanismo de atualização segura, Proteção de privacidade insuficiente e Senhas frágeis de fácil decodificação.

Em primeiro lugar, as vulnerabilidades em dispositivos IoT podem permitir que invasores obtenham acesso não autorizado e roubem dados ou assumam o controle dos dispositivos. Essas vulnerabilidades podem surgir devido a falhas de projeto, erros de codificação ou mecanismos de autenticação frágil.

Em segundo lugar, a falta de um mecanismo de atualização seguro pode deixar os dispositivos IoT vulneráveis a ameaças de segurança conhecidas, tornando-os alvos fáceis para invasores. Sem atualizações e patches regulares, as vulnerabilidades não podem ser resolvidas, deixando os dispositivos e suas redes associadas expostos a ameaças cibernéticas.

Em terceiro lugar, a proteção por senha refere-se à prática de proteger o acesso a um sistema, dispositivo ou conta exigindo que os usuários insiram uma senha. No entanto, se as senhas forem fracas ou mal implementadas, elas podem se tornar frágeis e fáceis de decodificar, comprometendo a segurança.

Em quarto lugar, proteção por senha refere-se à prática de proteger o acesso a um sistema, dispositivo ou conta exigindo que os usuários insiram uma senha. No entanto, se as senhas forem fracas ou mal implementadas, elas podem se tornar frágeis e fáceis de decodificar, comprometendo a segurança.

7.1 Mitigação das Principais Vulnerabilidades

Um dos principais motivos para mitigar vulnerabilidades em uma rede IoT é prevenir ataques cibernéticos que possam comprometer a privacidade, segurança e funcionalidade dos dispositivos e da rede como um todo. Criminosos podem explorar vulnerabilidades em dispositivos IoT para obter acesso não autorizado, roubar informações confidenciais, lançar ataques e até mesmo causar danos físicos.

Mitigar vulnerabilidades em uma rede IoT envolve identificar e abordar pontos fracos nos dispositivos, na infraestrutura de rede e nos protocolos de

comunicação usados. Isso pode incluir a implementação de recursos de segurança, como criptografia, autenticação, controle de acesso e detecção de intrusão, bem como atualização e correção regulares dos dispositivos e do software de rede.

Ao atenuar as vulnerabilidades em uma rede IoT, organizações e indivíduos podem garantir que seus dispositivos e dados estejam protegidos contra ameaças cibernéticas e que possam continuar a se beneficiar da conveniência e eficiência da tecnologia IoT com tranquilidade. Por esse motivo, será esclarecido a seguir como mitigar as 3 (três) principais vulnerabilidades determinadas a partir da metodologia proposta neste trabalho, apontando para a falta de mecanismos de atualização segura, proteção de privacidade insuficiente e uso de senhas frágeis de fácil decodificação.

7.2 Mitigação de vulnerabilidade – Falta de mecanismo de atualização seguro

A falta de um mecanismo de atualização segura em uma rede IoT pode deixar os dispositivos vulneráveis a ameaças e explorações de segurança, tornando importante mitigar esse problema. Aqui estão algumas etapas que se pode seguir para mitigar esse problema:

- a. Use um processo de inicialização seguro - verifique se os dispositivos em sua rede possuem um processo de inicialização segura, onde verifica-se a integridade do firmware antes de ser carregado. Isso pode ajudar a impedir que invasores adulterem o firmware durante o processo de inicialização.
- b. Implemente a assinatura e a verificação do firmware - a assinatura e a verificação do firmware podem ajudar a garantir que apenas as atualizações autorizadas sejam aplicadas aos dispositivos IoT. Ao assinar digitalmente as atualizações de firmware e verificá-las antes da instalação, pode-se impedir que atualizações não autorizadas ou maliciosas sejam aplicadas.

- c. Use protocolos de comunicação seguros - use protocolos de comunicação seguros, como TLS ou SSL, para garantir que as atualizações de firmware sejam transmitidas com segurança entre dispositivos e servidores. Isso pode ajudar a impedir que invasores interceptem ou modifiquem atualizações de firmware em trânsito.
- d. Implementar atestado de dispositivo - o atestado de dispositivo pode ajudar a garantir que apenas dispositivos autorizados possam receber atualizações de firmware. Isso pode ser obtido a partir da implementação de mecanismos de identidade e autenticação de dispositivos, como certificados de dispositivos ou autenticação biométrica.
- e. Considere medidas de segurança física - considere a implementação de medidas de segurança física, como lacres invioláveis, para impedir que invasores obtenham acesso físico aos dispositivos e instalem atualizações de firmware maliciosas.
- f. Atualize regularmente os dispositivos - atualize regularmente o firmware dos dispositivos em sua rede para garantir que eles estejam bem protegidos contra vulnerabilidades e explorações conhecidas. Isso também pode ajudar a garantir que os dispositivos estejam sempre executando o firmware mais recente e seguro.

Ao implementar essas medidas, pode-se ajudar a mitigar a falta de um mecanismo de atualização segura em sua rede IoT, reduzindo o risco de ameaças e explorações de segurança.

7.3 Mitigação de vulnerabilidade – Proteção de privacidade insuficiente

A proteção de privacidade insuficiente em uma rede IoT pode ter sérias consequências, incluindo acesso não autorizado a dados confidenciais, roubo de identidade e outros tipos de ataques cibernéticos. Mitigar esses riscos requer uma abordagem multicamadas que lide com as vulnerabilidades subjacentes na infraestrutura de rede, criptografia de dados e mecanismos de controle de

acesso. Aqui estão algumas etapas que podem ser tomadas para mitigar a proteção de privacidade insuficiente em uma rede IoT:

- a. Use criptografia forte - a criptografia de dados é fundamental para proteger a privacidade dos dados em uma rede IoT. Algoritmos de criptografia fortes, como AES (*Advanced Encryption Standard*) e RSA (*Rivest–Shamir–Adleman*) devem ser usados para proteger os dados em trânsito e em repouso. Além disso, os dados devem ser criptografados de ponta a ponta, para que não possam ser acessados por usuários não autorizados.
- b. Implemente controles de acesso - os controles de acesso são essenciais para impedir o acesso não autorizado a dados confidenciais. Os controles de acesso devem ser implementados em vários níveis, inclusive no nível do dispositivo, no nível da rede e no nível do aplicativo. Isso pode envolver o uso de senhas fortes, autenticação de dois fatores e outras medidas de segurança para garantir que apenas usuários autorizados possam acessar a rede e seus recursos.
- c. Atualize regularmente o software e o firmware - os dispositivos IoT geralmente são vulneráveis a vulnerabilidades de segurança devido a software ou firmware desatualizado. Para atenuar esse risco, é importante atualizar regularmente o software e o firmware para a versão mais recente, que geralmente inclui patches de segurança e correções de bugs.
- d. Realize auditorias de segurança regulares - as Auditorias de segurança regulares podem ajudar a identificar possíveis vulnerabilidades e riscos na rede. Isso pode envolver testar a rede em busca de vulnerabilidades, revisar logs de acesso e realizar testes de penetração para identificar pontos fracos na infraestrutura de rede.
- e. Conscientizar os usuários - por fim, conscientizar os usuários sobre os riscos dos dispositivos IoT e como proteger sua privacidade pode ser uma maneira eficaz de mitigar os riscos. Isso pode envolver o

fornecimento de treinamento sobre como usar os dispositivos com segurança, evitando o compartilhamento de informações confidenciais e evitando clicar em links suspeitos ou abrir anexos de fontes desconhecidas.

Ao seguir essas etapas, é possível mitigar os riscos associados à proteção de privacidade insuficiente em uma rede IoT. No entanto, é importante ressaltar que os riscos de segurança estão em constante evolução, por isso deve-se permanecer vigilante e atualizado com as práticas recomendadas de segurança mais recentes.

7.4 Mitigação de vulnerabilidade – Senhas frágeis de fácil decodificação

As senhas frágeis são um grande problema de segurança em muitas redes IoT, pois tornam essas redes vulneráveis a ataques de hackers. Felizmente, existem algumas medidas que podem ser tomadas para mitigar esse problema, como segue.

- a. Implementar senhas fortes - uma das melhores formas de mitigar senhas frágeis é implementar senhas fortes, que são difíceis de decifrar. Isso inclui o uso de senhas longas, que contêm uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais. Além disso, é importante evitar o uso de senhas óbvias, como datas de nascimento, nomes de familiares, ou palavras comuns.
- b. Usar autenticação multifator - a autenticação multifator adiciona uma camada extra de segurança à rede IoT, exigindo que o usuário forneça mais de uma forma de autenticação para acessar o dispositivo. Isso pode incluir, por exemplo, uma senha e um código enviado por mensagem de texto para o celular do usuário.
- c. Atualizar regularmente as senhas - é importante lembrar que as senhas podem se tornar frágeis com o tempo, especialmente se forem usadas por muito tempo. Por isso, é recomendável que os usuários

atualizem regularmente suas senhas e evitem reutilizar senhas antigas.

- d. Implementar medidas de segurança adicionais – além das estratégias acima citadas anteriormente, há outras medidas de segurança que podem ser implementadas para mitigar senhas frágeis, como a criptografia de dados e a utilização de firewalls e sistemas de detecção de intrusão.
- e. Educar os usuários – a educação dos usuários também é fundamental para a segurança da rede IoT. É importante que os usuários entendam a importância de senhas fortes e seguras, e sejam incentivados a adotar práticas seguras de autenticação.

8. CONCLUSÃO

A IoT (Internet das Coisas) refere-se à rede de dispositivos eletrônicos conectados à internet, capazes de coletar e compartilhar dados. Embora a IoT ofereça muitas vantagens, ela também pode apresentar vulnerabilidades críticas que podem ser exploradas por criminosos e outros indivíduos mal-intencionados.

Uma das principais vulnerabilidades da IoT é a falta de segurança nos dispositivos. Muitos dispositivos IoT são projetados com pouca ou nenhuma segurança embutida, o que os torna vulneráveis a ataques. Além disso, a IoT pode ser comprometida por meio de ataques de *phishing*, engenharia social e outros métodos de engenharia reversa.

Outra vulnerabilidade é a falta de proteção adequada dos dados coletados pelos dispositivos IoT. Isso pode incluir informações confidenciais, como dados de saúde, finanças e localização. Se esses dados caírem nas mãos erradas, podem ser usados para fins maliciosos, como extorsão ou roubo de identidade.

Por fim, a IoT também é vulnerável a ataques de negação de serviço (DDoS), que podem causar interrupções em serviços essenciais, como serviços de saúde e financeiros.

Para mitigar essas vulnerabilidades, é necessário um esforço conjunto entre fabricantes de dispositivos, provedores de serviços e usuários finais. Isso pode incluir a adoção de melhores práticas de segurança, como criptografia de dados, autenticação de usuários e gerenciamento adequado de senhas. Além disso, os usuários devem ser conscientizados sobre os riscos de segurança associados à IoT e instruídos sobre como proteger seus dispositivos e dados.

Como sugestão para trabalhos futuros, sugere-se desenvolver uma metodologia semelhante voltada para rede IoT domésticas em ambientes com grande concentração de moradores, com objetivo de proteger as pessoas físicas contra ameaças ou exposição de dados.

REFERÊNCIAS

ACHILLAS, Charisios et al. The use of multi-criteria decision analysis to tackle waste management problems: A literature review. *Waste Management and Research*, v. 31, n. 2, p. 115–129, 2013.

AHN, T; CHARNES, A; COOPER, W. Using Data Envelopment Analysis to Measure the Efficiency of Not-For-Profit Organization a Critical Evaluation-Comment. Center for Cybernetic Studies, 1987.

AL-ANBARI, Mohammad A.; THAMEER, Mohanad Y.; AL-ANSARI, Nadhir. Landfill site selection by weighted overlay technique: Case study of Al-Kufa, Iraq. *Sustainability (Switzerland)*, v. 10, n. 4, p. 1–11, 2018.

AL-FUQAHA. A."Internet of Things: A Comprehensive Review on Enabling Technologies, Architectures, and Challenges" (2016).

ALMEIDA, M. B. Uma abordagem integrada sobre ontologias: Ciência da Informação, Ciência da Computação e Filosofia. *Perspectivas em Ciência da Informação*, v. 19, n. 3, p. 242-258, 2014.

ALMEIDA, M.; SOUZA, R.; CARDOSO, K. Uma proposta de ontologia de domínio para segurança da informação em organizações. *Informação e Sociedade*, [s. l.], v. 20, n. 1, p. 155-168, 2010.

AL-YAHYAI, S. Wind farmland suitability indexing using multi-criteria analysis. *Renewable Energy*, v. 44, p. 80–87, 2012.

BENAYOUN, R.; B. ROY; SUSSMAN., B. ELECTRE: Une méthode pour guider le choix en présence de points de vue multiples. SEMA-METRA International, 1966.

BLANK, ANDREY, G. TCP/IP Foundations, 2006. ISBN 9780782151138.

BRANS, J P; VINCKE, Ph. A Preference Ranking Organisation Method. Management Science, n. May 2019, 1985.

BRAUERS, W; Karel, M; ZAVADSKAS, E. Project management by multimooora as an instrument for transition economies. Technological and Economic Development of Economy, v. 8619, 2010.

BRITO, A. Direito Penal Informático. [s.l: s.n.]. v. 9788502209411.

CEGAN, JEFFREY C. et al. Trends and applications of multi-criteria decision analysis in environmental sciences: literature review. Environment Systems and Decisions, v. 37, n. 2, p. 123–133, 2017.

CHOO, E. U.; WEDLEY, W. C. A common framework for deriving preference values from pairwise comparison matrices. Computers & Operations Research , 2014 International Conference on, 2004.

CHOO, K. K. R. The Internet of Things: An Overview of Security Challenges and Solutions. Journal of Information Privacy and Security, 15(2), 2019.

CHOUDHARY, P. Internet of Things: Impact on Supply Chain Management" (2016).

DONG, Y; CHANG, W. Influence of characteristics of the Internet of Things on consumer purchase intention: Social Behavior and Personality: an international journal, 2014.

FERREIRA, F; MANZAN, R, DURAES, W. Arquitetura de Soluções IoT; Alura Books, 2022, ISBN 9786555670530.

FISHBURN, PETER C. Methods of Estimating Additive Utilities. Management Science, n. October 2015, 1967.

GABUS, A; FONTELA, E. Perceptions of the world problematique: Communication procedure, communicating with those bearing collective responsibility. p. 11–18, 1973.

GOLDBERG, D. E.; HOLLAND, J. H. Genetic Algorithms and Machine Learning. Machine Learning, p. 95–99, 1988.

GUARDIAN, T. “Edward Snowden”. Acessado em 06 de Junho 2022, <http://www.theguardian.com/us-news/edward-snowden>, 2022.

HAIKOWICZ, S; COLLINS, K. A Review of Multiple Criteria Analysis for Water Resource Planning and Management. Water Resour Manage, p. 1553–1566, 2007.

HELMANN, K. & MARÇAL, R. Método multicritério de apoio à decisão na gestão da Manutenção: aplicação do método electre I na seleção de equipamentos críticos para processo Revista Gestão Industrial, ISSN 1808-0448 / v. 03, n. 01: p. 123-133, 2007.

HOSTMANN, Markus et al. Multi-Attribute Value Theory as a Framework for Conflict Resolution in River Rehabilitation. Journal of multi-criteria Decision Analysis, v. 102, n. 2005, p. 91–102, 2005.

HWANG, C. L. Methods Multiple Attribute Decision Making. [S.l.: s.n.], 1981.

IBM. (2018). Cost of a Data Breach Study. Retrieved from <https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/>.

ISHIZAKA, A.; NEMERY, P. Multi-criteria decision analysis: methods and software. Wiley: Chichester, 2013.

KANGAS, J. MCDM Methods in Strategic Planning of Forestry on State-Owned Lands in Finland: Applications and Experiences. *Journal of Multi-criteria Decision Analysis*, v. 10, p. 257–271, 2001.

KASPERSKY. (2021). The cost of IT security incidents in 2020. Retrieved from <https://media.kaspersky.com/en/business-security/cost-of-security-incidents-2020.pdf>.

KEENEY, R. L.; RAIFFA, H. *Decision with multiple objectives: preferences and value tradeoffs*. New York: John Wiley & Sons, 1976.

KERŠULIENE, Violeta; ZAVADSKAS, Edmundas Kazimieras; TURSKIS, Zenonas. Selection of rational dispute resolution method by applying new step-wise weight assessment ratio analysis (Swara). *Journal of Business Economics and Management*, v. 11, n. 2, p. 243– 258, 2010.

KHAN, R. "Internet of Things: Architectures, Protocols, and Applications" (2013).

LINKOV, A. Multi-criteria Decision Analysis: A Framework for Structuring Remedial Decisions at Contaminated Sites. *Comparative Risk Assessment and Environmental Decision Making*, p. 15–54, 2004.

LOOTSMA, F. A. Scale Sensitivity in the Multiplicative AHP and SMART. *Journal of MultiCriteria Decision Analysis*, v. 2, n. February 1992, p. 87–110, 1993.

MCKINSEY, Global Institute. (2019). The Internet of Things: Mapping the Value Beyond the Hype. Retrieved from <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-mapping-the-value-beyond-the-hype>

MENG, W; WENJUAN, J. Enhancing the Security Of blockchain-based software defined networking through trust-based traffic fusion and filtration, [s. l.], p. 1-70, 2021.

MUNDA, G. Multicriteria Evaluation in a Fuzzy Environment. [S.l.]: Physica-Verlag Heidelberg, 1995.

NIST, “National Vulnerability database.” [Online]. Available: <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>.

NIST; BOECKL K. Considerações para Gerenciar Riscos de Privacidade e Segurança Cibernética na Internet das Coisas (IoT). Departamento de Comércio dos EUA, NISTIR. 8228, 2019.

OLSON, N. The Internet of Things. *New Media & Society*. 18(4), 680–682, [s. l.], 2016.

OPRICOVIC, S. Expert Systems with Applications Fuzzy Vikor with an application to water resources planning. *Expert Systems With Applications*, v. 38, n. 10, p. 12983–12990, 2011.

OWASP top 10 vulnerabilidades. [Online]. Available: https://www.owasp.org/images/thumb/7/79/OWASP_2018.

OWASP, “OWASP Internet of Things Project.” [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Medical_Devices.

OWASP, “Top IoT Vulnerabilities,” OWASP, 2016. [Online]. Available: https://www.owasp.org/index.php/Top_IoT_Vulnerabilities.

PAN, J; MCELHANNON, J. Future edge cloud and edge computing for Internet of Things applications. 5(1), 439–449, IEEE Internet of Things Journal, 2017.

PETERSON, LARRY, L, BRUCE, S. Computer Networks. Morgan Kaufman; Publishers 2011. ISBN 9780123850591

POUW, DUARTE, K. Segurança na arquitetura TCP/IP de firewalls e canais seguros, 1999.

SAATY, THOMAS L. Decision Making With the Analytic Network Process (ANP) And Its “Super-decisions” Software The National Missile Defense (NMD). Proceedings – 6th ISAHP 2001, p. 365–382, 2001.

SAVVAS, T; FLORIDES, G; TASSOU, S. The use of multiple criteria decision making methodologies for the promotion of RES through funding schemes in Cyprus, A review. Energy Policy, v. 38, n. 12, p. 7783–7792, 2010.

SCHENK, K, L; PINKERT, J. An algorithm for servicing multi-relational queries. Proceedings of the 1977 ACM SIGMOD international conference on Management of data, p. 10–20, 1977.

SCHUWIRTH, N; REICHERT, P; LIENERT, J. Methodological aspects of multi-criteria decision analysis for policy support: A case study on pharmaceutical removal from hospital wastewater. European Journal of Operational Research, v. 220, n. 2, p. 472–483, 2012.

SÊMOLA, M. Gestão da Segurança da Informação: uma visão executiva. Rio de Janeiro: Campus, 2003.

Shinder, Thomas W. The Best Damn Firewall Book Period, Second Edition, 2011, ISBN 9780080556871.

SHINDER, THOMAS, W. The Best Damn Firewall Book Period, Second Edition, 2011, ISBN 9780080556871.

SIPONEN, M. T. A paradigmatic analysis of conventional approaches for developing and managing secure IS. In: International Conference on Information Security, 16., 2001, MA, USA. Proceedings of... Trusted information: The new decade challenge. MA: Kluwer Academic Publishers Norwell, 2001. p. 437-452.

SRINIVASAN, V.; SHOCKER, ALLAN D. Linear programming techniques for multidimensional analysis of preferences. PSYCHOMETRIKA, n. 3, 1973.

TANEMBAUM; ANDREW S. Computer Networks: Prentice Hall. 2002. ISBN 9780130661029.

THEODOROU, S; FLORIDES, G; TASSOU, S. The use of multiple criteria decision making methodologies for the promotion of RES through funding schemes in Cyprus, A review. Energy Policy, v. 38, n. 12, p. 7783–7792, 2010.

VOOGD, H. Multicriteria Evaluation with Mixed Qualitative and Quantitative Data. International Institute for Applied Systems Analysis, 1983.

WANG, M. A Weighted product Method for Bidding Strategies in Multi-attribute Auctions. J Syst Sci Complex, n. 200159, p. 194–208, 2010.

WILLIAMS, P. Information security governance. Information Security Technical Report, v. 6, n. 3, p. 60-70, 2001.

ZHAO, X. The strategy of smart home control system design based on wireless network. In Computer Engineering and Technology (ICCET), 2010 2nd International Conference on, v. 4, n. V4-37, 2010.

APÊNDICES

a. Primeiro formulário disponibilizado aos especialistas:

Análise de Vulnerabilidades e Ameaças em Redes IoT

Esta pesquisa tem como objetivo analisar as principais vulnerabilidades e ameaças exploradas por criminosos cibernéticos em redes IoT corporativas e domésticas, com foco em classificar essas vulnerabilidades e ameaças quanto a seu impacto nas redes mencionadas. Nessa classificação, serão considerados impactos técnicos, econômicos e as especificidades de uma rede IoT.

A metodologia será baseada na resposta deste questionário, visando elencar, junto a um grupo de especialistas da área de Tecnologia e Segurança da Informação, as principais fragilidades de uma rede composta por ativos de tecnologia, especialmente nos ambientes de trabalho que efetivamente sofrem com tais ameaças, com foco nas práticas utilizadas por atacantes, que visam explorar desde a degradação dos serviços de um dispositivo até o sequestro dos dados ou acessos.

Aluna do curso de Mestrado em Engenharia Elétrica Gabriella Barbutti.

Section 1

...

Antes de responder a pesquisa é necessário responder os campos a seguir:

1. Favor informar sua Nacionalidade: *

Brasileira

Outra

2. Atualmente você trabalha na área de Tecnologia e Segurança da Informação? *

Sim, atuo na área.

Não, mas já atuei.

Questionário

3. Atribua a correlação entre o critério **Frequência de Ocorrência** e cada uma das vulnerabilidades (**senhas frágeis de fácil decodificação, serviços e interfaces de rede inseguros, etc**) de acordo com a gradação a seguir.

Deve-se escolher um grau de correlação onde:

- 1 - Representa **Não há Correlação**
- 3 - Representa **Correlação Baixa**
- 5 - Representa **Correlação Médiana**
- 7 - Representa **Correlação Alta**
- 9 - Representa **Correlação Extrema ***

	1	3	5	7	9
Senhas frágeis de fácil decodificação	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Serviços e interfaces de rede inseguros	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falta de mecanismo de atualização segura	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Uso de componentes inseguros ou desatualizados	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Proteção de privacidade insuficiente	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Transferência e armazenamento de dados inseguros	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falta de gerenciamento de dispositivos	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Configurações padrão de contas	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falta de Hardening Físico	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

4. Atribua a correlação entre o critério **Impacto de Degradação de Rede** e cada uma das vulnerabilidades (**senhas frágeis de fácil decodificação, serviços e interfaces de rede inseguros, etc**) de acordo com a gradação a seguir.

Deve-se escolher um grau de correlação onde:

1 - Representa **Não há Correlação**

3 - Representa **Correlação Baixa**

5 - Representa **Correlação Mediana**

7 - Representa **Correlação Alta**

9 - Representa **Correlação Extrema ***

	1	3	5	7	9
Senhas frágeis de fácil decodificação	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Serviços e interfaces de rede inseguros	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falta de mecanismo de atualização segura	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Uso de componentes inseguros ou desatualizados	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Proteção de privacidade insuficiente	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Transferência e armazenamento de dados inseguros	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falta de gerenciamento de dispositivos	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Configurações padrão de contas	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falta de Hardening Físico	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5. Atribua a correlação entre o critério **Impacto Financeiro** e cada uma das vulnerabilidades (senhas frágeis de fácil decodificação, serviços e interfaces de rede inseguros, etc) de acordo com a gradação a seguir.

Deve-se escolher um grau de correlação onde:

- 1 - Representa **Não há Correlação**
- 3 - Representa **Correlação Baixa**
- 5 - Representa **Correlação Médiana**
- 7 - Representa **Correlação Alta**
- 9 - Representa **Correlação Extrema ***

	1	3	5	7	9
Senhas frágeis de fácil decodificação	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Serviços e interfaces de rede inseguros	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falta de mecanismo de atualização segura	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Uso de componentes inseguros ou desatualizados	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Proteção de privacidade insuficiente	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Transferência e armazenamento de dados inseguros	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falta de gerenciamento de dispositivos	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Configurações padrão de contas	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falta de Hardening Físico	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

6. Atribua a correlação entre o critério **Impacto de Queda de Rede** e cada uma das vulnerabilidades (**senhas frágeis de fácil decodificação, serviços e interfaces de rede inseguros, etc**) de acordo com a gradação a seguir.

Deve-se escolher um grau de correlação onde:

- 1 - Representa **Não há Correlação**
- 3 - Representa **Correlação Baixa**
- 5 - Representa **Correlação Médiana**
- 7 - Representa **Correlação Alta**
- 9 - Representa **Correlação Extrema ***

	1	3	5	7	9
Senhas frágeis de fácil decodificação	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Serviços e interfaces de rede inseguros	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falta de mecanismo de atualização segura	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Uso de componentes inseguros ou desatualizados	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Proteção de privacidade insuficiente	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Transferência e armazenamento de dados inseguros	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falta de gerenciamento de dispositivos	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Configurações padrão de contas	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falta de Hardening Físico	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

7. Atribua a correlação entre o critério **Impacto de Quantidade de Usuários Afetados pela Indisponibilidade da Rede** e cada uma das vulnerabilidades (**senhas frágeis de fácil decodificação, serviços e interfaces de rede inseguros, etc**) de acordo com a gradação a seguir.

Deve-se escolher um grau de correlação onde:

- 1 - Representa **Não há Correlação**
- 3 - Representa **Correlação Baixa**
- 5 - Representa **Correlação Médiana**
- 7 - Representa **Correlação Alta**
- 9 - Representa **Correlação Extrema ***

	1	3	5	7	9
Senhas frágeis de fácil decodificação	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Serviços e interfaces de rede inseguros	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falta de mecanismo de atualização segura	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Uso de componentes inseguros ou desatualizados	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Proteção de privacidade insuficiente	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Transferência e armazenamento de dados inseguros	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falta de gerenciamento de dispositivos	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Configurações padrão de contas	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falta de Hardening Físico	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

8. Que outros impactos você considera que sejam incluídos para a classificação das ameaças e vulnerabilidades em uma rede IoT?

Enter your answer

+ Add new

b. Respostas coletadas do primeiro formulário:

Análise de Vulnerabilidades e Ameaças em Redes IoT

33

Responses

40:29

Average time to complete

Active

Status

Review answers

Post scores

Open in Excel ...

1. Favor informar sua Nacionalidade: (0 point)

[More Details](#)

● Brasileira	33
● Outra	0



2. Atualmente você trabalha na área de Tecnologia e Segurança da Informação? (0 point)

[More Details](#)

[Insights](#)

● Sim, atuo na área.	32
● Não, mas já atuei.	1



3. Atribua a correlação entre o critério **Frequência de Ocorrência** e cada uma das vulnerabilidades (**senhas frágeis de fácil decodificação, serviços e interfaces de rede inseguros, etc**) de acordo com a gradação a seguir. (0 point)

Deve-se escolher um grau de correlação onde:

- 1 - Representa **Não há Correlação**
- 3 - Representa **Correlação Baixa**
- 5 - Representa **Correlação Mediana**
- 7 - Representa **Correlação Alta**
- 9 - Representa **Correlação Extrema**

[More Details](#)

■ 1 ■ 3 ■ 5 ■ 7 ■ 9

Senhas frágeis de fácil decodificação

Serviços e interfaces de rede inseguros

Falta de mecanismo de atualização segura

Uso de componentes inseguros ou desatualizados

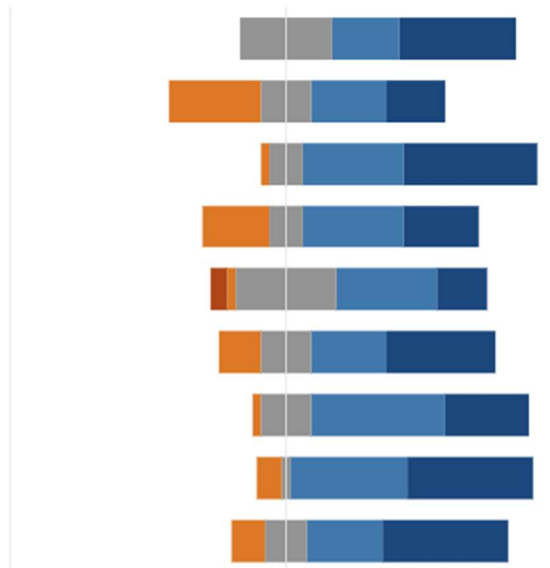
Proteção de privacidade insuficiente

Transferência e armazenamento de dados inseguros

Falta de gerenciamento de dispositivos

Configurações padrão de contas

Falta de Hardening Físico



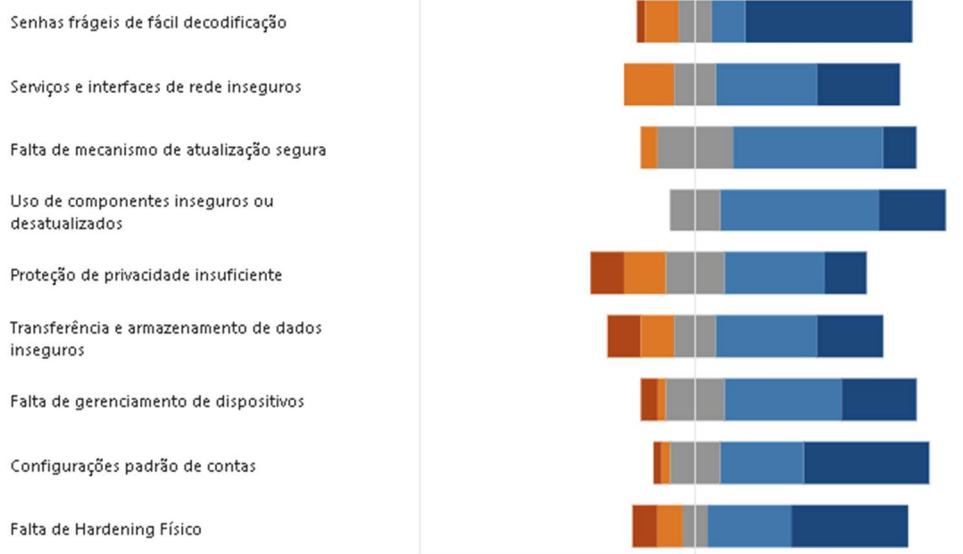
4. Atribua a correlação entre o critério **Impacto de Degradação de Rede** e cada uma das vulnerabilidades (**senhas frágeis de fácil decodificação, serviços e interfaces de rede inseguros, etc**) de acordo com a gradação a seguir. (0 point)

Deve-se escolher um grau de correlação onde:

- 1 - Representa **Não há Correlação**
- 3 - Representa **Correlação Baixa**
- 5 - Representa **Correlação Mediana**
- 7 - Representa **Correlação Alta**
- 9 - Representa **Correlação Extrema**

[More Details](#)

■ 1 ■ 3 ■ 5 ■ 7 ■ 9



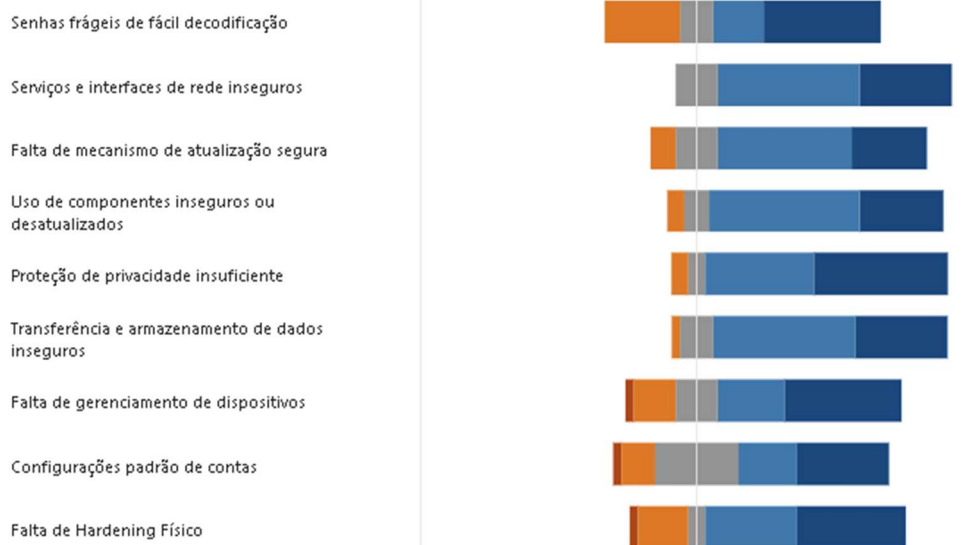
5. Atribua a correlação entre o critério **Impacto Financeiro** e cada uma das vulnerabilidades (**senhas frágeis de fácil decodificação, serviços e interfaces de rede inseguros, etc**) de acordo com a gradação a seguir. (0 point)

Deve-se escolher um grau de correlação onde:

- 1 - Representa **Não há Correlação**
- 3 - Representa **Correlação Baixa**
- 5 - Representa **Correlação Mediana**
- 7 - Representa **Correlação Alta**
- 9 - Representa **Correlação Extrema**

[More Details](#)

■ 1 ■ 3 ■ 5 ■ 7 ■ 9



6. Atribua a correlação entre o critério **Impacto de Queda de Rede** e cada uma das vulnerabilidades (**senhas frágeis de fácil decodificação, serviços e interfaces de rede inseguros, etc**) de acordo com a gradação a seguir. (0 point)

Deve-se escolher um grau de correlação onde:

- 1 - Representa **Não há Correlação**
- 3 - Representa **Correlação Baixa**
- 5 - Representa **Correlação Mediana**
- 7 - Representa **Correlação Alta**
- 9 - Representa **Correlação Extrema**

[More Details](#)

■ 1 ■ 3 ■ 5 ■ 7 ■ 9

Senhas frágeis de fácil decodificação

Serviços e interfaces de rede inseguros

Falta de mecanismo de atualização segura

Uso de componentes inseguros ou desatualizados

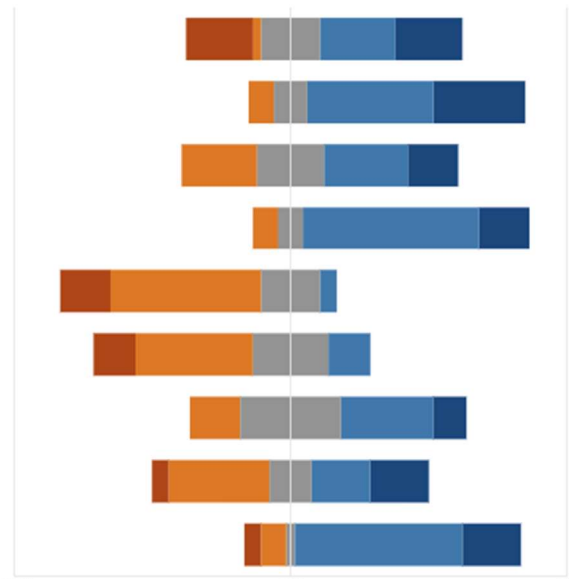
Proteção de privacidade insuficiente

Transferência e armazenamento de dados inseguros

Falta de gerenciamento de dispositivos

Configurações padrão de contas

Falta de Hardening Físico



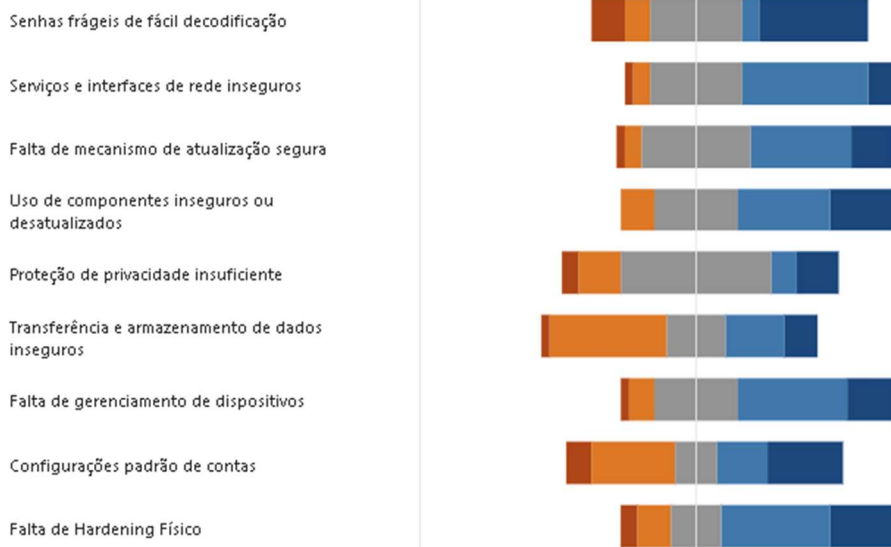
7. Atribua a correlação entre o critério **Impacto de Quantidade de Usuários Afetados pela Indisponibilidade da Rede** e cada uma das vulnerabilidades (**senhas frágeis de fácil decodificação, serviços e interfaces de rede inseguros, etc**) de acordo com a graduação a seguir. (0 point)

Deve-se escolher um grau de correlação onde:

- 1 - Representa **Não há Correlação**
- 3 - Representa **Correlação Baixa**
- 5 - Representa **Correlação Mediana**
- 7 - Representa **Correlação Alta**
- 9 - Representa **Correlação Extrema**

[More Details](#)

■ 1 ■ 3 ■ 5 ■ 7 ■ 9



8. Que outros impactos você considera que sejam incluídos para a classificação das ameaças e vulnerabilidades em uma rede IoT? (0 point)

[More Details](#)

[Insights](#)

10

Responses

Latest Responses

4 respondents (40%) answered **segurança** for this question.



8. Que outros impactos você considera que sejam incluídos para a classificação das ameaças e vulnerabilidades em uma rede IoT?

10 Responses

ID ↑	Name	Responses
1	anonymous	Impacto no vazamento de credenciais fazendo uma referência ao pilar de SI confidencialidade. Impacto de uma interceptação de pacotes e alterações dos dados fazendo uma referência ao pilar de SI Integridade.
2	anonymous	Isolamento entre a rede de dispositivos IoT e a que contém usuários
3	anonymous	Altamente vulnerável muito a zero day possui vários vetores de ataque, ausência de security by design. Escolha de hardware baseado somente no preço. Grande possibilidade de haver Backdoor de hardware, uma vez que, a maioria dos componentes são da China ou Taiwan. Os fabricantes de lot não preocupam em atualizar o software, uma vez que isso não é o core business da empresa e não gera valor tangível para empresa, adicionalmente, as constantes atualização de hardware e ou software são vistas como custo. Adicionalmente, o público alvo do lot são pessoas leigas em privacidade e segurança da informação.
4	anonymous	Impacto na Privacidade e Coleta de Dados da Rede.
5	anonymous	Pagamento ou não de sequestro de dados. Ausência de um seguro para mitigar as perdas envolvendo a subtração de dados empresariais.
6	anonymous	Criptografia e segurança de dados
7	anonymous	Confiabilidade e Proteção para atividades comuns, como sessões de Telemedicina ou transações simples.
8	anonymous	Propósito do dispositivo e sua posição na rede. Certos tipos de dispositivos atuam em atividades que requerem mais segurança, logo a segurança destes deve ser priorizada. Como exemplo, suponhamos uma rede IoT doméstica de uma residência autônoma. Dispositivos como lâmpadas e eletrodomésticos podem ser infectados, no entanto sua utilidade prática seria baixa, servindo como ponte para outros dispositivos. Entretanto, nesta mesma residência há câmeras de segurança e drones, dispositivos com maior relevância para um atacante. Ameaças direcionadas para estes dispositivos específicos devem ser classificadas com maior prioridade.
9	anonymous	Infelizmente algumas áreas de negócio compram dispositivos IOT e perguntam se é possível integração olhando para segurança da informação apenas depois da compra, além do tema de gestão de vulnerabilidades ser extremamente complexo em IOT devido a compatibilidade com Qualys, Nessus, etc. Para uma rede segura com IOT o gerenciamento de segurança da informação deve ser preciso e todos devem colaborar, algo que normalmente não acontece.
10	anonymous	Tempo de resposta para mitigar IoT comprometidos.

c. Segundo formulários disponibilizados aos especialistas:

Análise de Vulnerabilidades em Redes IoT Corporativas (Pesos por Critérios)

Atribua o grau de importância dos 4 critérios citados na pesquisa anterior, considerando as 9 principais vulnerabilidades encontradas em uma rede IoT corporativa.

1. Senhas frágeis de fácil decodificação
2. Serviços e interfaces de rede inseguros
3. Falta de mecanismo de atualização segura
4. Uso de componentes inseguros ou desatualizados
5. Proteção de privacidade insuficiente
6. Transferência e armazenamento de dados inseguros
7. Falta de gerenciamento de dispositivos
8. Configurações padrão de contas
9. Falta de Hardening Físico

Peso de cada critério:

- 1º lugar peso 0,6
- 2º lugar peso 0,3
- 3º lugar peso 0,1
- 4º lugar peso 0,0

Section 1

...

1. Qual dos critérios abaixo possui maior grau de importância considerando a vulnerabilidade **Senhas frágeis de fácil decodificação** para uma rede corporativa. *

Frequência de ocorrência

Impacto de degradação de rede

Impacto de queda de rede

Impacto financeiro

2. Atribua o grau de importância dos 3 critérios a seguir, considerando a vulnerabilidade **Serviços e interfaces de rede inseguros** para uma rede corporativa. *

Impacto financeiro

Frequência de ocorrência

Impacto de degradação de rede

Impacto de queda de rede

3. Atribua o grau de importância dos 3 critérios a seguir, considerando a vulnerabilidade **Falta de mecanismo de atualização segura** para uma rede corporativa. *

Frequência de ocorrência

Impacto de degradação de rede

Impacto de queda de rede

Impacto financeiro

4. Atribua o grau de importância dos 3 critérios a seguir, considerando a vulnerabilidade **Uso de componentes inseguros ou desatualizados** para uma rede corporativa. *

Frequência de ocorrência

Impacto de degradação de rede

Impacto financeiro

Impacto de queda de rede

5. Atribua o grau de importância dos 3 critérios a seguir, considerando a vulnerabilidade **Proteção de privacidade insuficiente** para uma rede corporativa. *

Impacto financeiro

Frequência de ocorrência

Impacto de degradação de rede

Impacto de queda de rede

6. Atribua o grau de importância dos 3 critérios a seguir, considerando a vulnerabilidade **Transferência e armazenamento de dados inseguros** para uma rede corporativa. *

Impacto financeiro

Frequência de ocorrência

Impacto de degradação de rede

Impacto de queda de rede

7. Atribua o grau de importância dos 3 critérios a seguir, considerando a vulnerabilidade **Falta de gerenciamento de dispositivos** para uma rede corporativa. *

Impacto de degradação de rede

Frequência de ocorrência

Impacto de queda de rede

Impacto financeiro

8. Atribua o grau de importância dos 3 critérios a seguir, considerando a vulnerabilidade **Configurações padrão de contas** para uma rede corporativa. *

Frequência de ocorrência

Impacto de degradação de rede

Impacto de queda de rede

Impacto financeiro

9. Atribua o grau de importância dos 3 critérios a seguir, considerando a vulnerabilidade **Falta de Hardening Físico** para uma rede corporativa. *

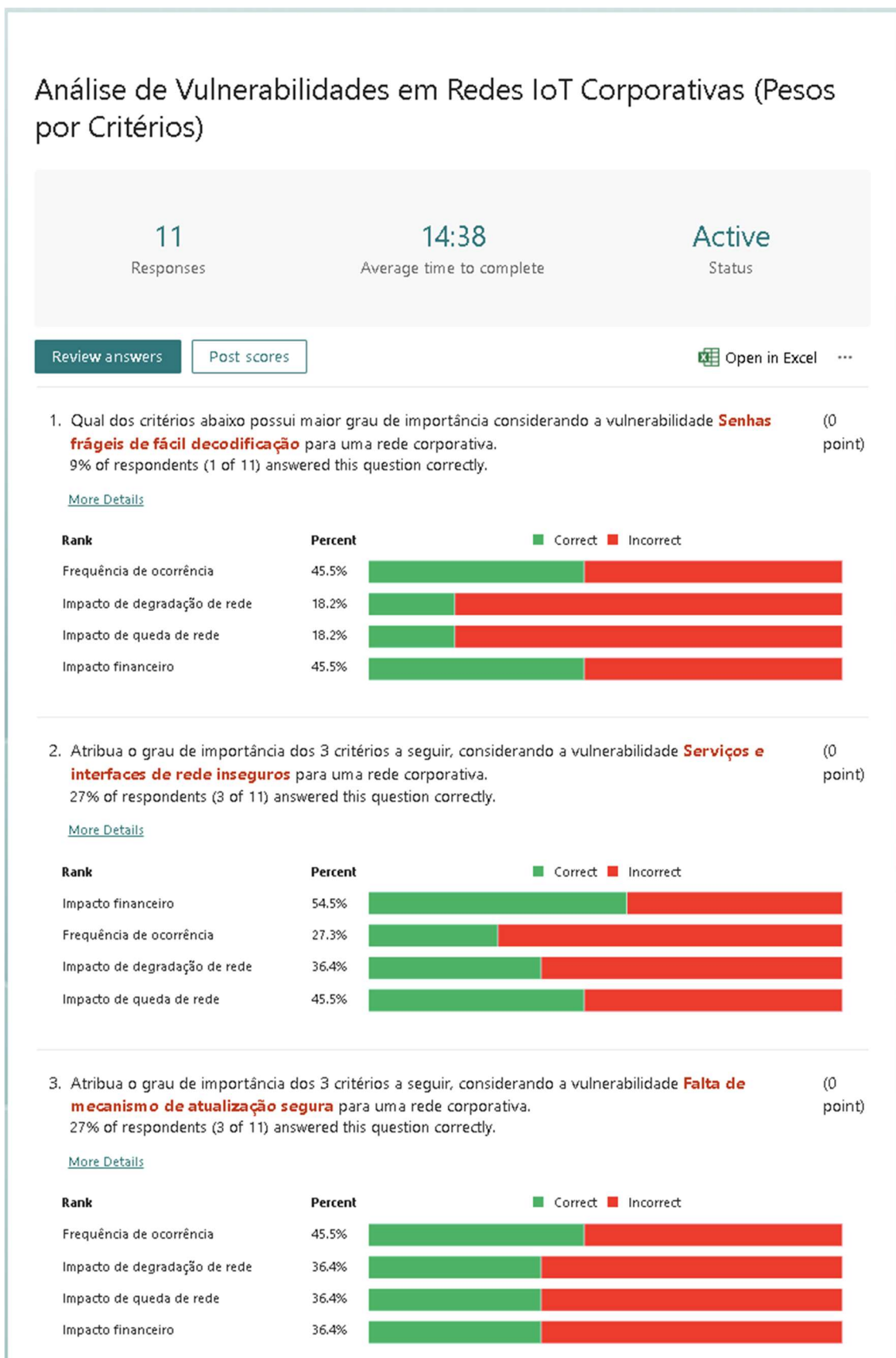
Frequência de ocorrência

Impacto de degradação de rede

Impacto de queda de rede

Impacto financeiro

d. Respostas coletadas do segundo formulário:



4. Atribua o grau de importância dos 3 critérios a seguir, considerando a vulnerabilidade **Uso de componentes inseguros ou desatualizados** para uma rede corporativa. (0 point)
 18% of respondents (2 of 11) answered this question correctly.

[More Details](#)



5. Atribua o grau de importância dos 3 critérios a seguir, considerando a vulnerabilidade **Proteção de privacidade insuficiente** para uma rede corporativa. (0 point)
 64% of respondents (7 of 11) answered this question correctly.

[More Details](#)



6. Atribua o grau de importância dos 3 critérios a seguir, considerando a vulnerabilidade **Transferência e armazenamento de dados inseguros** para uma rede corporativa. (0 point)
 55% of respondents (6 of 11) answered this question correctly.

[More Details](#)



7. Atribua o grau de importância dos 3 critérios a seguir, considerando a vulnerabilidade **Falta de gerenciamento de dispositivos** para uma rede corporativa. (0 point)
 18% of respondents (2 of 11) answered this question correctly.

[More Details](#)



8. Atribua o grau de importância dos 3 critérios a seguir, considerando a vulnerabilidade **Configurações padrão de contas** para uma rede corporativa. (0 point)
45% of respondents (5 of 11) answered this question correctly.

[More Details](#)



9. Atribua o grau de importância dos 3 critérios a seguir, considerando a vulnerabilidade **Falta de Hardening Físico** para uma rede corporativa. (0 point)
18% of respondents (2 of 11) answered this question correctly.

[More Details](#)

