INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
CURSO SUPERIOR DE TECNOLOGIA EM TELEMÁTICA

GUILHERME VIDAL DE NEGREIROS LIMA

UMA VISÃO GERAL SOBRE SEGURANÇA EM SOLUÇÕES IOT PARA AMBIENTES RESIDENCIAIS

CAMPINA GRANDE – PB
2023

GUILHERME VIDAL DE NEGREIROS LIMA

UMA VISÃO GERAL SOBRE SEGURANÇA EM SOLUÇÕES IOT PARA AMBIENTES RESIDENCIAIS

Trabalho de Conclusão de Curso apresentado à banca examinadora do Curso Superior de Tecnologia em Telemática do IFPB *campus* Campina Grande, em cumprimento às exigências parciais para a obtenção do título de Tecnólogo em Telemática.

Orientador: Prof. Danyllo Wagner Albuquerque

CAMPINA GRANDE – PB
2023

L732v Lima, Guilherme Vidal de Negreiros.
Uma visão sobre segurança em soluções IOT para ambientes residenciais / Guilherme Vidal de Negreiros Lima.Campina Grande, 2023.
72 f. : il.

Trabalho de Conclusão de Curso (Graduação em Tecnologia em Telemática) - Instituto Federal da Paraíba, 2023.
Orientador: Prof. Me. Danyllo Wagner Albuquerque.

1.Dispositivos IoT 2.Cibercriminosos 3. Métodos de segurança I. Albuquerque, Danyllo Wagner. II. Título.

CDU 004.056

GUILHERME VIDAL DE NEGREIROS LIMA

UMA VISÃO GERAL SOBRE SEGURANÇA EM SOLUÇÕES IOT PARA AMBIENTES RESIDENCIAIS

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Tecnólogo em Telemática do IFPB *campus* Campina Grande, na Linha de Pesquisa de Segurança de redes.

Aprovado em 03 de agosto de 2023.

gov.br Documento assinado digitalmente
DANYLLO WAGNER ALBUQUERQUE
Data: 03/08/2023 14:26:54-0300
Verifique em https://validar.iti.gov.br

Prof. Danyllo Wagner Albuquerque
Instituto Federal da Paraíba

gov.br Documento assinado digitalmente
DAVID CANDEIA MEDEIROS MAIA
Data: 03/08/2023 14:20:07-0300
Verifique em https://validar.iti.gov.br

Prof. David Candeia Medeiros Maia
Instituto Federal da Paraíba

gov.br Documento assinado digitalmente
IGOR BARBOSA DA COSTA
Data: 03/08/2023 15:04:36-0300
Verifique em https://validar.iti.gov.br

Prof. Igor Barbosa Costa
Instituto Federal da Paraíba

Dedico este trabalho com gratidão e amor. A Deus, por sua presença constante. À minha família e à minha namorada, por seu apoio e incentivo. Esta conquista é nossa, e sou grato por cada uma de suas contribuições em minha jornada acadêmica.

AGRADECIMENTOS

Gostaria de dedicar este breve espaço para expressar minha profunda gratidão a todas as pessoas que contribuíram para a conclusão bem-sucedida deste trabalho de conclusão de curso.

Primeiramente, agradeço à minha família, minha namorada e amigos pelo apoio incondicional durante todo o processo de pesquisa e redação. Suas palavras de incentivo e encorajamento foram fundamentais para me manter motivado e perseverante em busca dos objetivos estabelecidos.

Não posso deixar de agradecer ao meu orientador e membros da banca avaliadora pela orientação acadêmica e pelo tempo e dedicação dispensados na revisão e orientação do meu trabalho. Suas sugestões e críticas construtivas foram essenciais para aprimorar a qualidade do meu trabalho.

Por último, mas não menos importante, desejo expressar minha gratidão à minha instituição de ensino, por me proporcionar a oportunidade de realizar este trabalho e por todo o suporte prestado ao longo do curso.

Agradeço sinceramente a todas as pessoas que, de alguma forma, contribuíram para a realização deste trabalho. Esse resultado não teria sido possível sem vocês.

Muito obrigado!

“Não podemos permitir que a busca pela conveniência comprometa a segurança. A segurança deve sempre ser uma prioridade.”

(Satya Nadella, CEO da Microsoft.)

RESUMO

À medida que a tecnologia IoT continua a evoluir, torna-se fundamental estar atento aos riscos de segurança em constante mudança e buscar soluções inovadoras para proteger os usuários e seus dados pessoais. Este trabalho aborda de forma abrangente os riscos de segurança associados aos dispositivos IoT em ambientes residenciais, com o principal objetivo de identificar e analisar os aspectos de segurança desses dispositivos. Para isso, foi realizada uma revisão da literatura especializada, que permite compreender as principais preocupações de segurança relacionadas aos dispositivos IoT. Além disso, identificamos ameaças e riscos potenciais, utilizando casos relevantes para ilustrar situações concretas em que essas vulnerabilidades podem ser exploradas. Com base nessa pesquisa, foram desenvolvidas recomendações práticas e específicas para mitigar essas vulnerabilidades, oferecendo orientações claras aos usuários para garantir a segurança de seus dispositivos IoT em ambientes residenciais. Este trabalho reconhece também a importância de abordar as questões de privacidade que surgem quando dispositivos IoT coletam e transmitem dados pessoais, os quais podem ser acessados por *hackers* mal-intencionados. Este trabalho destaca também a relevância de identificar e solucionar falhas de segurança em dispositivos IoT, além de promover a adoção de práticas seguras pelos usuários. A segurança na IoT é uma preocupação crescente e requer uma abordagem abrangente, que envolva fabricantes, provedores de serviços e usuários finais.

Palavras-chave: Dispositivos IoT, Vulnerabilidades, Casas inteligentes, Cibercriminosos, Métodos de segurança, Invasão.

ABSTRACT

As IoT technology continues to evolve, it becomes essential to be aware of the ever-changing security risks and seek innovative solutions to protect users and their personal data. This study comprehensively addresses the security risks associated with IoT devices in residential environments, with the main objective of identifying and analyzing the security aspects of these devices. To achieve this, a review of specialized literature was conducted to gain a deep understanding of the key security concerns related to IoT devices. Additionally, we identified potential threats and risks, using relevant cases to illustrate specific situations where these vulnerabilities can be exploited. Based on this research, practical and specific recommendations were developed to mitigate these vulnerabilities, providing clear guidance to users to ensure the security of their IoT devices in residential settings. This study also acknowledges the importance of addressing privacy issues that arise when IoT devices collect and transmit personal data, which can be accessed by malicious hackers. Furthermore, it highlights the relevance of identifying and resolving security flaws in IoT devices, as well as promoting the adoption of secure practices by users. Security in the IoT is a growing concern that requires a comprehensive approach involving manufacturers, service providers, and end-users.

Keywords: IoT devices, Vulnerabilities, Smart homes, Cybercriminals, Security measures, Intrusion.

LISTA DE ILUSTRAÇÕES

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

2FA	Autenticação em dois fatores;
ABINC	Associação Brasileira em Internet das Coisas;
Anatel	Agência Nacional de Telecomunicações;
ANPD	Autoridade Nacional de Proteção de Dados;
AURESIDE	Associação Brasileira de Automação Residencial e Predial;
BBB	*Better Business Bureau*;
BNDES	Banco Nacional de Desenvolvimento Econômico e Social;
CGI.br	Comitê Gestor da Internet no Brasil;
DDoS	*Distributed Denial of Service*;
DoS	*Denial of Service*;
IDC	*International Data Corporation*;
IDS	Sistemas de detecção de intrusões;
IDS/IPS	Sistemas de detecção e prevenção de intrusões;
IoT	*Internet of Things*;
ITU	*International Telecommunication Union*;
NIST	*National Institute of Standards and Technology*;
LGPD	Lei Geral de Proteção de Dados Pessoais;
OWASP	*Open Web Application Security Project*;
PF	Polícia Federal;
PIN	*Personal Identification Number*;
RBAC	Controle de acesso baseado em função;
RFID	*Radio-Frequency IDentification*;
TI	Tecnologia da Informação;
TIC	Tecnologias da Informação e Comunicação;
VPN	Redes Privadas Virtuais.

SUMÁRIO

1. INTRODUÇÃO

Internet das Coisas, traduzido da expressão em inglês *Internet of Things*, ou simplesmente IoT, é um conceito que se refere à interconexão de dispositivos físicos, veículos, edifícios e outros objetos que possuem sensores e/ou atuadores incorporados que permitem a coleta e transmissão de dados entre si ou com outros sistemas. Esses dispositivos podem ser controlados remotamente e interagir com o ambiente físico, criando um mundo cada vez mais inteligente e conectado [1]. A IoT é uma tecnologia que tem revolucionado a maneira como as coisas funcionam em nosso mundo conectado, e com a rápida expansão da tecnologia de rede e a proliferação de dispositivos móveis, os dispositivos IoT estão se tornando cada vez mais comuns em nossas vidas cotidianas [55].

Os dispositivos IoT tem o potencial de transformar a maneira como vivemos, trabalhamos e interagimos com o mundo ao nosso redor. Quando os dispositivos IoT são aplicados no ambiente residencial, permitem a comunicação inteligente entre eletrodomésticos, que podem ser controlados remotamente. Isso deu origem ao conceito de "*smart home*" ou casa inteligente. Hoje, esse conceito se caracteriza por residências que integram mecanismos automáticos por meio do *wi-fi* ou *bluetooth* para controlar, automatizar e otimizar funções residenciais. Seja para controlar a temperatura, garantir a segurança, ajustar a iluminação, entre outras diversas possibilidades, tudo isto utilizando um sistema dentro da própria casa, ou controlado remotamente utilizando o *smartphone*, *tablet*, ou um computador, simplificando o cotidiano das pessoas, garantindo mais praticidade, conforto, segurança e acessibilidade aos moradores, além de uso mais consciente da energia elétrica [56].

Como uma grande tendência, os dispositivos IoT possuem um grande impacto no desenvolvimento das tecnologias de informação e comunicação (TIC). Entretanto, juntamente com esta revolução da tecnologia há também uma grande preocupação com as possíveis vulnerabilidades que os dispositivos IoT podem sofrer. Uma vez que casas inteligentes podem ser compostas por vários dispositivos IoT, são basicamente portas digitais para acesso a informações pessoais dos usuários. É importante mencionar que muitos destes dispositivos não contam com métodos de segurança nativos de fábrica. Desse modo, cibercriminosos podem se aproveitar destas vulnerabilidades e capturar informações sensíveis armazenadas nestes dispositivos (e.g., endereço, telefone, senhas, números de cartões de crédito, credenciais de acesso, entre outros) para efetuar ações criminosas. Eles também podem invadir sua casa diretamente por meio de um dispositivo IoT, tomando o controle da câmera de segurança e espionando seus movimentos [57].

1.1. PROBLEMÁTICA

Com o avanço da tecnologia IoT e a ampliação do acesso à internet banda larga, cada vez mais dispositivos estão se tornando capazes de se conectar a uma rede sem fio, permitindo a criação de um ecossistema de dispositivos inteligentes que trocam informações constantemente. Além disso, com a diminuição dos custos dos dispositivos conectados, mais e mais pessoas têm acesso a essas tecnologias, o que tem impulsionado ainda mais o

crescimento dos dispositivos IoT. Com isso, vivemos em um mundo cada vez mais conectado, onde os dispositivos armazenam e trocam informações em tempo real. No entanto, é importante lembrar que a segurança e privacidade dos dados são questões fundamentais que precisam ser tratadas com seriedade nesse contexto.

Pensando em um cenário de interconectividade entre diversos dispositivos em uma casa, é importante lembrar que uma grande quantidade de dados pessoais está sendo constantemente coletada e transmitida, incluindo informações sobre os hábitos e rotinas dos moradores, seus horários de sono, rotina de trabalho, consumo de energia elétrica, entre outros. Esses dados são valiosos e podem ser acessados por *hackers* e utilizados para fins maliciosos, como roubo de identidade ou monitoramento indevido.

Além dos riscos associados ao acesso não autorizado aos dados pessoais coletados pelos dispositivos IoT, é importante destacar que esses dispositivos também podem se tornar alvos de ataques cibernéticos, tornando a rede vulnerável a outras ameaças, como a propagação de *malware* ou o sequestro de dispositivos. Dessa forma, é fundamental que medidas de segurança robustas sejam implementadas para garantir a privacidade e proteção dos dados pessoais coletados pelos dispositivos IoT em residências. É fundamental que os usuários estejam cientes dos riscos associados à coleta e transmissão de dados pessoais pelos dispositivos IoT em suas residências, isso é um fator crítico para o sucesso da implementação dessas medidas de segurança.

1.2. OBJETIVOS

Com base no panorama acima apresentado, este trabalho tem como objetivo identificar e analisar aspectos de segurança associados a dispositivos IoT conectados em ambiente residencial. Pretende-se com a realização desta pesquisa realizar um levantamento das vulnerabilidades mais comuns nos sistemas de automação residencial, com objetivo de identificar e listar as principais ameaças aos dispositivos IoT, além de estabelecer estratégias para proteger os usuários contra possíveis invasões.

Visando atingir o objetivo descrito, temos os seguintes objetivos específicos conforme itens descritos no que segue:

- Realizar uma revisão bibliográfica sobre o tema;
- Mapear as principais aplicações de dispositivos IoT em ambiente residencial;
- Identificar e catalogar as principais ameaças e vulnerabilidades à dispositivos IoT;
- Mapear os principais riscos associados a cada ameaça;
- Apresentar estratégias de segurança contra invasões.

1.3. METODOLOGIA

Para alcançar os objetivos propostos, é necessário adotar uma metodologia que permita a identificação e avaliação de ameaças potenciais e vulnerabilidades existentes em dispositivos IoT. Com base nisso, foram estabelecidas as seguintes etapas de pesquisa:

- Etapa 1 - Revisão bibliográfica. Nesta etapa foi realizada uma pesquisa bibliográfica em busca de material relevante associado a ameaças e vulnerabilidades sobre dispositivos IoT. Um dos resultados dessa etapa é a identificação do conceitos associados a dispositivos IoT, suas características e funcionalidades;
- Etapa 2 - Mapeamento das principais aplicações de dispositivos IoT em ambiente residencial: Foi realizada a identificação dos diferentes tipos de dispositivos IoT utilizados em residências. Adicionalmente, foi explorado como esses dispositivos estão sendo aplicados para melhorar o conforto, segurança e eficiência nas residências;
- Etapa 3 - Identificação das principais ameaças e vulnerabilidades aos dispositivos IoT: foi feita uma avaliação das principais ameaças conhecidas que afetam os dispositivos IoT de forma mais significativa;
- Etapa 4 - Mapeamento dos principais riscos associados a cada ameaça: Analisar os possíveis impactos das ameaças identificadas, considerando o contexto residencial;
- Etapa 5 - Elaboração de recomendações: com base na análise dos dados, serão elaboradas recomendações para mitigar as vulnerabilidades identificadas e melhorar a segurança de dispositivos em residências.

1.4. JUSTIFICATIVA

Uma pesquisa relacionada ao levantamento de vulnerabilidades de dispositivos IoT em ambiente residencial pode trazer diversos desdobramentos importantes. Em primeiro lugar, pode identificar falhas de segurança em dispositivos IoT e sistemas relacionados, o que permite que os desenvolvedores de *software* e construtores de soluções IoT corrijam essas vulnerabilidades e tornem os produtos mais seguros. Isso pode ajudar a evitar ataques maliciosos a dispositivos conectados à Internet, como câmeras de segurança, fechaduras inteligentes, termostatos e outros aparelhos domésticos.

Além disso, uma pesquisa sobre vulnerabilidades de dispositivos IoT em ambiente residencial pode ajudar a conscientizar o público em geral sobre os riscos de segurança associados ao uso destes dispositivos e promover a adoção de práticas de segurança recomendadas, como a mudança de senhas padrão, atualizações regulares de *firmware* e a utilização de redes seguras. Isso pode contribuir para uma maior confiança do consumidor em relação aos produtos IoT, o que, por sua vez, pode levar a um maior crescimento do mercado IoT.

Por fim, uma pesquisa sobre vulnerabilidades de dispositivos IoT em ambiente residencial pode ajudar a orientar a elaboração de políticas governamentais e regulamentações sobre a segurança de dispositivos IoT neste ambiente sensível. À medida que os governos buscam proteger os cidadãos e empresas contra as ameaças cibernéticas, pesquisas sobre vulnerabilidades de dispositivos IoT podem ajudar a moldar as políticas públicas e as regulamentações que visam a segurança cibernética, criando um ambiente mais seguro e confiável para o uso de dispositivos IoT.

1.5. ESTRUTURA DO TRABALHO

Os capítulos restantes que compõem o presente documento estão estruturados da seguinte forma:

- *Capítulo 2:* Apresenta definições gerais sobre o tema abordado neste documento, que servem como embasamento teórico aos leitores acerca da segurança de redes e privacidade de dados ligadas a dispositivos IoT;
- *Capítulo 3:* Identifica e discute os principais trabalhos relacionados a esta pesquisa, bem como destaca como este trabalho avança o estado da arte;
- *Capítulo 4:* Descreve os passos metodológicos realizados para construção desta pesquisa;
- *Capítulo 5:* Apresenta os principais resultados qualitativos, assim como apresenta discussão suplementar aos dados obtidos com esta pesquisa.
- *Capítulo 6:* Identifica as principais ameaças associadas a esta pesquisa bem como cita as principais ações para mitigar os seus efeitos;
- *Capítulo 7:* Apresenta as conclusões finais da pesquisa, bem como seus desdobramentos futuros de pesquisa.

2. FUNDAMENTAÇÃO TEÓRICA

Nesta seção, serão abordados os principais conceitos teóricos que são relevantes para uma compreensão aprofundada do tema em questão, permitindo apreciar sua importância no contexto da pesquisa. conceito de dispositivos IoT (Seção 2.1), história do IoT (Seção 2.2), trajetória dos dispositivos IoT no Brasil (Seção 2.3), A chegada dos dispositivos IoT em residências (Seção 2.4), lei geral de proteção de dados pessoais (Seção 2.5) e as considerações finais do capítulo (Seção 2.6).

2.1. CONCEITO DE DISPOSITIVOS IOT

Dispositivos IoT (*Internet of Things*, em português Internet das Coisas), é um conceito que se refere a objetos físicos que estão conectados à internet e têm a capacidade de coletar e transmitir dados, permitindo que esses objetos se comuniquem entre si e com outros sistemas de computação (Figura 1). Esses dispositivos podem ser equipamentos eletrônicos, eletrodomésticos, veículos, sensores, câmeras, entre outros, que estão equipados com sensores, *softwares* e conectividade de rede que permitem que eles troquem informações entre si e com outros sistemas de computação que estão presentes em diversas áreas, como automação residencial, saúde, indústria, transporte, entre outras [2].

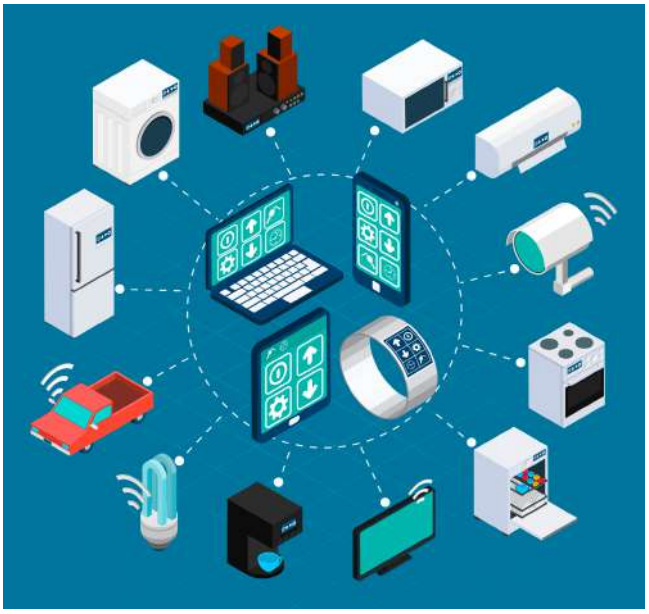


Figura 1: Conceito de *Internet of Things*, **Fonte:** freepik.com

A ideia fundamental do IoT é que os dispositivos possam criar um ambiente de rede inteligente, onde os dados coletados são processados por sistemas de computação para gerar informações úteis para os usuários. Essas informações podem ser usadas para melhorar a eficiência de processos, aumentar a segurança, otimizar o uso de recursos e criar novos serviços. Por exemplo, sensores de temperatura podem coletar informações sobre a temperatura ambiente e transmitir esses dados para um sistema central, que pode então controlar o ar-condicionado para manter uma temperatura confortável.

2.2. HISTÓRIA DO IOT

A IoT é uma tecnologia relativamente recente, que começou a se desenvolver nas últimas duas décadas. Na década de 1980, ainda não havia o conceito de IoT como é conhecido hoje. No entanto, nessa época, já existiam alguns sistemas de automação que permitiam o monitoramento e controle de equipamentos e processos industriais, que poderiam ser considerados os precursores da IoT. Além disso, na década de 80, já existiam sistemas de telemetria que utilizavam sensores e transmissores para enviar dados em tempo real para centros de controle. No entanto, esses sistemas eram geralmente projetados para aplicações específicas e não estavam conectados a uma rede global como a internet [3].

Então, foi durante a feira INTEROP '89 Conference de 1990, que John Romkey apresentou de fato o primeiro dispositivo IoT (Figura 2). O dispositivo em questão era uma torradeira que poderia ser ligada e desligada pela internet. Durante a apresentação o pão foi inserido manualmente, no ano seguinte o pão foi inserido por um pequeno guindaste que era controlado pela internet [4].

Figura 2: Internet Toaster, John Romkey, **Fonte:** livinginternet.com

Em 1991, Mark Weiser publicou um artigo intitulado "*The Computer for the 21st Century*", no qual ele discutia o futuro da IoT, embora ele usasse o termo "computação ubíqua" (1991, p.1) para se referir a ela. Ele previu que dispositivos conectados seriam integrados em todos os lugares de forma natural, eliminando a necessidade de instalação, configuração ou gerenciamento de recursos computacionais [5]. Esse artigo se tornou um marco na pesquisa sobre o tema e é citado amplamente na literatura sobre o assunto [5].

Em 1996, Venkatesh Kedarisetti também estudou sobre o assunto e previu que as tarefas domésticas seriam realizadas por casas especializadas. Então, em setembro de 1999, Kevin Ashton usou pela primeira vez o termo "*Internet of Things*" durante uma apresentação sobre *Radio-Frequency IDentification* (RFID) para rastrear produtos na cadeia de suprimentos (compra de matéria-prima, produção, armazenamento, movimentação interna, transporte e distribuição até o consumidor final) [3]. Na época, Ashton estava trabalhando em um projeto para a Procter & Gamble e percebeu que a tecnologia de RFID poderia ser utilizada para conectar objetos físicos à internet, criando um ambiente interconectado e

automatizado. A tecnologia apresentada por Ashton ganhou destaque, abrindo um leque de possibilidades [3].

Em 2000, a LG apresentou durante um evento na Coreia do Sul, o primeiro eletrodoméstico inteligente (Figura 3), uma geladeira que podia ser utilizada como dispositivo web, tv, rádio ou até mesmo quadro de avisos [2]. No entanto, foi em 2005 que o IoT ganhou a atenção dos governos em relação à privacidade e segurança de dados, com uma publicação da ITU (União Internacional de Telecomunicações) chamada de ITU Internet Reports 2005: The Internet of Things, que mostrou como a tecnología RFID conseguiría conectar objetos, sensores, sistemas embarcados e nanotecnologia, além de superar desafios importantes, como padronização, privacidade, frequência e questões éticas e sociais [6].

Figura 3: Internet Digital DIOS, **Fonte:** Folha de São Paulo

Em 2005, o primeiro objeto inteligente em larga escala, chamado de Nabaztag (figura 4), foi comercializado. Um dispositivo em forma de coelho que podia se conectar a internet para baixar previsões do tempo, ler e-mails, receber relatórios do mercado de ações, notícias, era despertador e também tocava MP3 [7].

Figura 4: Nabaztag, **Fonte:** Autodesk Instructables

Em 2008, ocorreu a primeira edição da *Internet of Things Conference* em Zurique, na Suíça. Posteriormente, uma segunda edição foi realizada em 2010 em Tóquio. Esses eventos pioneiros reuniram pesquisadores e profissionais líderes da academia e da indústria, com o objetivo de facilitar o compartilhamento de aplicações, resultados de pesquisa e conhecimentos sobre IoT [8].

Em 2011, discutiu-se a criação de padrões internacionais para a criação de objetos conectados em um panorama global. Então a ITU vem reunindo especialistas para a consolidação de um padrão global [2]. No ano seguinte, em 2012, a União Europeia fez uma consulta pública para que os cidadãos apontassem suas necessidades e seguranças em relação ao IoT [9], e foi então que em 16 e 17 de julho do mesmo ano, Londres sediou o 1º *Open IoT Assembly*, uma conferência que reunia especialistas, desenvolvedores e entusiastas do IoT para discutir e compartilhar ideias sobre o futuro da tecnologia [10].

Então em 2016, os dispositivos IoT já eram uma realidade, na qual já existiam cerca de 4,9 bilhões de dispositivos conectados em uso. E de acordo com o site IoT Analytics[1], é esperado que em 2025 haja cerca de 30,9 bilhões de dispositivos IoT conectados (Gráfico 1), quase 4 dispositivos por pessoa, que são impulsionados por tecnologias, como o 5G [11].

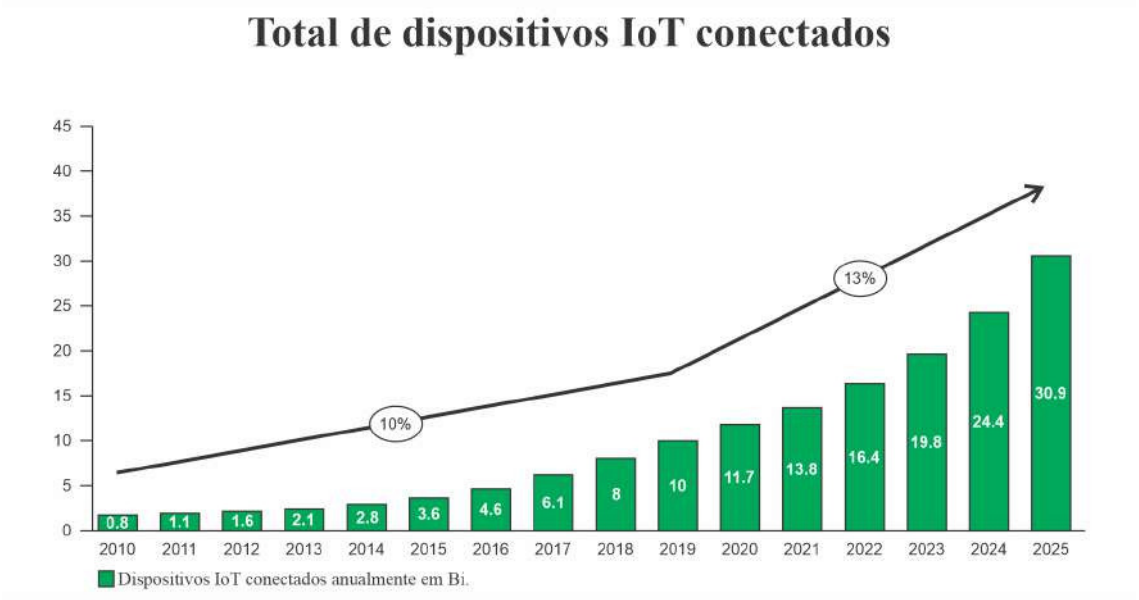


Gráfico 1: Total de dispositivos IoT conectados, **Fonte:** IoT Analytics (2021)

2.3. TRAJETÓRIA DOS DISPOSITIVOS IOT NO BRASIL

A IoT começou a ganhar força no Brasil em meados dos anos 2010, quando Salvador foi palco do primeiro evento focado em IoT, chamado de "1º Congresso de Tecnologia, Sistemas e Serviços com RFID". O evento foi organizado pelo CIMATEC SENAI e Saint Paul Etiquetas Inteligentes. Na segunda edição, em outubro de 2011 em Búzios, o evento mudou de nome para Congresso Brasileiro de Internet das Coisas e RFID [2].

[1] Link: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

No ano seguinte, o Fórum Brasileiro de Internet das Coisas foi criado com o objetivo de destacar a relevância dos dispositivos IoT para a sociedade, bem como apresentar novas tecnologias e evidenciar como o Brasil pode se tornar um participante global nesse segmento. Em 2016, em colaboração com o grupo BMComm, o Fórum organizou o primeiro Congresso Brasileiro e Latino-Americano em Internet das Coisas, que teve como tema "Smartworld: a IoT como base para um mundo melhor" [12].

Em dezembro de 2015 foi fundada a ABINC (Associação Brasileira em Internet das Coisas), cujo propósito é representar o mercado perante a Anatel (Agência Nacional de Telecomunicações), o Ministério das Comunicações, autoridades constituídas e outros órgãos reguladores setoriais ou de fomento de pesquisa, por meio de seus associados [13].

O governo brasileiro também tem investido em iniciativas para impulsionar o desenvolvimento da IoT no país. Em 2017, foi lançado o Plano Nacional de Internet das Coisas em parceria com Banco Nacional de Desenvolvimento Econômico e Social (BNDES), que estabeleceu metas e ações para fomentar a inovação e o empreendedorismo na área, o estudo foi dividido em quatro fases [14]. Além disso, a Anatel tem trabalhado na regulamentação do uso de espectro de radiofrequência para a IoT e na expansão das redes móveis 5G, que será essencial para suportar a crescente demanda por dispositivos conectados em rede [15].

2.4. A CHEGADA DOS DISPOSITIVOS IOT EM RESIDÊNCIAS

De forma geral, uma *Smart Home* ou “casa inteligente” é uma casa ou residência que utiliza tecnologia e dispositivos inteligentes para automatizar e controlar funções como iluminação ou temperatura de forma centralizada e muitas vezes remotamente. É uma casa equipada com dispositivos inteligentes, como termostatos, lâmpadas, câmeras de segurança, fechaduras e eletrodomésticos, pode ser controlada remotamente através de um *smartphone* ou *tablet*, tornando a experiência do usuário muito mais prática e simples. Além disso, sensores ajustam automaticamente a temperatura do ambiente e a iluminação, monitoram o consumo de energia, evitando o desperdício e reduzindo custos e impactos ambientais, enquanto dispositivos de segurança são acionados em caso de detecção de intrusos [16].

A ideia de "casa inteligente" começou a ser discutida na década de 70, quando os primeiros sistemas de controle doméstico foram desenvolvidos. No entanto, esses sistemas eram caros e complexos de instalar, e apenas alguns indivíduos e empresas tiveram acesso a eles. Porém, foi somente na década de 1990 que a tecnologia começou a avançar significativamente, com o desenvolvimento de protocolos de comunicação padronizados, como o X10, que permitiu a comunicação entre diferentes dispositivos [17]. Em 1996, surgiu uma inovação prática: as chaves Clapper. Elas permitiam que as luzes fossem acionadas através de palmas, tornando o ato de ligar e desligar as luzes muito mais simples. Embora tenha havido alguns problemas com ativações involuntárias, as chaves Clapper se tornaram um ícone dos anos 90, aparecendo em vários brinquedos e tecnologias domésticas [18].

Nos anos 2000, com o surgimento da tecnologia *wireless* e a popularização da internet, os dispositivos IoT em casas começaram a se desenvolver mais rapidamente. Desde

então os dispositivos IoT têm tido um grande impacto nas casas modernas, com dispositivos cada vez mais conectados, automatizados e interativos, permitindo uma maior conveniência e conforto para os moradores [17]. O lançamento do primeiro termostato inteligente da Nest em 2011 ajudou a popularizar ainda mais o conceito de *smart home* [19].

Hoje, a casa inteligente é uma realidade para muitas pessoas, com um número crescente de dispositivos e sistemas domésticos inteligentes disponíveis no mercado. Além disso, assistentes virtuais como *Amazon Alexa*[2], *Google Assistant*[3] e *Apple Siri*[4], continuam a evoluir, se tornando cada vez mais integradas ao cotidiano das pessoas.

2.5. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A utilização cada vez maior de dispositivos IoT em casas levanta preocupações sobre a segurança e privacidade dos dados pessoais. Para ajudar a lidar com esse problema, foi aprovada a Lei Geral de Proteção de Dados Pessoais (LGPD)[5], em vigor desde setembro de 2020. Essa lei estabelece regras claras para proteger os direitos fundamentais de liberdade e privacidade dos indivíduos, garantindo a segurança no tratamento, proteção e transferência de informações pessoais [20].

Com isso, a LGPD criou a Autoridade Nacional de Proteção de Dados (ANPD), um órgão responsável por fiscalizar e aplicar as penalidades previstas na lei. As sanções podem variar desde advertências até multas que podem chegar a 2% do faturamento da empresa, limitadas a um total de 50 milhões de reais por infração [21].

Nesse contexto, a LGPD enfatiza a importância da proteção dos dados pessoais dos usuários. Ela exige que as empresas adotem medidas técnicas e organizacionais adequadas para garantir a segurança dos dados pessoais coletados pelos dispositivos IoT. Isso inclui a implementação de mecanismos de segurança, tais como criptografia, autenticação e controle de acesso, com intuito de prevenir o acesso não autorizado, o vazamento de informações e outras ameaças à privacidade dos usuários [20].

A LGPD também destaca a importância da transparência no tratamento de dados pessoais. Os usuários devem ser informados de forma clara e acessível sobre quais dados estão sendo coletados, como serão utilizados e por quanto tempo serão armazenados. Além disso, os usuários devem consentir explicitamente com o tratamento de seus dados, e têm o direito de acessar, corrigir e excluir suas informações pessoais [20].

Em caso de violação de dados pessoais coletados por dispositivos IoT, a LGPD estabelece a obrigatoriedade de notificação às autoridades competentes e aos usuários afetados. As empresas são responsáveis por adotar medidas para mitigar danos e prejuízos decorrentes de incidentes de segurança e devem ser transparentes ao informar os usuários sobre tais violações [20].

---

[2] link: https://www.amazon.com.br/b?ie=UTF8&node=19949683011

[3] link: https://assistant.google.com/

[4] link: https://www.apple.com/br/siri/

[5] Link: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Vale ressaltar que a segurança dos dispositivos IoT vai além das disposições da LGPD. É fundamental que as empresas adotem boas práticas de segurança cibernética, como atualizações regulares de *firmware*, testes de segurança e monitoramento contínuo dos dispositivos IoT para garantir sua integridade e proteção contra ameaças. A LGPD pode ser considerada um componente adicional que complementa essas práticas e ajuda a fortalecer a proteção dos dados pessoais dos usuários de dispositivos IoT [20].

2.6. CONSIDERAÇÕES DO CAPÍTULO

Este capítulo apresentou o conceito de dispositivos IoT, que são objetos físicos conectados à internet e com a capacidade de coletar e transmitir dados, permitindo a comunicação entre si e outros sistemas de computação. Os dispositivos IoT têm sido usados em diversas áreas, como automação residencial, saúde, indústria, transporte e outros, para melhorar a eficiência de processos, aumentar a segurança, otimizar o uso de recursos e criar novos serviços. A IoT é uma tecnologia relativamente recente, que começou a se desenvolver nas últimas duas décadas. Nesta seção, foi abordada a história da IoT, desde a década de 1980, quando surgiram os primeiros sistemas de automação e telemetria, até 2005, quando foi comercializado o primeiro objeto inteligente em larga escala.

Com base na relevância crescente da IoT, torna-se fundamental examinar os trabalhos relacionados à área a fim de identificar as principais tendências, desafios e oportunidades. Nesse sentido, o próximo capítulo desta pesquisa tem como objetivo realizar uma abrangente revisão das pesquisas relacionadas à IoT. Foram investigados diversos estudos e trabalhos acadêmicos, visando obter uma compreensão aprofundada do campo e identificar lacunas que nosso estudo pretende preencher. Através dessa revisão, almeja-se fornecer uma visão aprofundada e atualizada do estado da arte da IoT, além de documentar as principais ameaças que afetam os dispositivos IoT.

Além disso, uma revisão abrangente permitiu que este estudo se posicionasse dentro do contexto atual da IoT. Compreendemos tendências emergentes, as tecnologias mais recentes e as estratégias de segurança inovadoras que estão sendo desenvolvidas. Isso nos ajudou a oferecer uma compreensão valiosa e atualizada sobre a evolução da IoT e a identificar áreas promissoras para pesquisas futuras.

Uma das principais contribuições deste estudo foi elaborado um documento abrangente e acessível, voltado não apenas para especialistas em segurança da informação, mas também para usuários comuns de dispositivos IoT. Com base nas principais ameaças identificadas, esse documento tem como objetivo fornecer orientações claras e práticas para que os usuários possam tomar medidas efetivas para proteger seus dispositivos e dados pessoais. Acredita-se que a conscientização e a educação são fundamentais para lidar com os desafios de segurança inerentes aos dispositivos IoT.

3. TRABALHOS RELACIONADOS

Nesta seção serão descritos trabalhos relacionados com a pesquisa em questão. Inicialmente, Zimmeck [22] e colegas exploraram as questões de privacidade e segurança nos dispositivos IoT, propondo estratégias que os intermediários podem adotar para lidar com esses desafios. Os autores destacam as ameaças existentes, incluindo ataques cibernéticos, vazamento de informações e o uso inadequado de dados pessoais, e analisam o papel dos intermediários na proteção da privacidade e segurança dos usuários de dispositivos IoT. Eles propõem estratégias, como a criação de políticas claras de privacidade e segurança em dispositivos IoT, a implementação de medidas de segurança técnica, a adoção de práticas de gerenciamento de riscos e colaboração com outros intermediários, e a promoção de programas de educação e conscientização para os usuários de dispositivos IoT. O estudo concluiu que os intermediários desempenham um papel crucial na proteção da privacidade e segurança nos dispositivos IoT e destaca a necessidade de uma abordagem colaborativa e multidisciplinar para lidar com esses desafios.

Seguindo a mesma linha de pesquisa, o trabalho de Alawais [23] et al. abordaram questões de autenticação e autorização na Internet das Coisas (IoT). Os autores revisaram a definição da IoT e suas características, enfocando as implicações de segurança e privacidade associadas a essa tecnologia. Eles discutem as técnicas de autenticação e autorização, incluindo senhas, certificados digitais, autenticação baseada em token, controle de acesso baseado em função, controle de acesso baseado em atributos e controle de acesso baseado em políticas, fornecendo uma análise detalhada de suas vantagens e desvantagens. Além disso, o artigo aborda questões de privacidade relacionadas à autenticação e autorização em dispositivos IoT. Os autores concluem que a autenticação e autorização são fundamentais para a segurança dos dispositivos IoT e recomendam a implementação de técnicas adequadas para proteger os dispositivos e informações pessoais dos usuários.

Em seguida, o estudo de Huang Xin et al. [24] examina a questão da segurança e privacidade nos dispositivos IoT. Este estudo consiste em uma revisão abrangente da literatura existente sobre o tema, com o objetivo de identificar as principais ameaças à segurança e privacidade em dispositivos IoT, abordando as implicações éticas e legais da segurança e privacidade em dispositivos IoT, incluindo questões de responsabilidade e governança. Além disso, os autores discutem as implicações para a privacidade do usuário, incluindo o risco de monitoramento e vigilância. No geral, o trabalho oferece uma visão geral das ameaças e técnicas de segurança e privacidade em dispositivos IoT, bem como as questões éticas e legais envolvidas.

Como último trabalho, destaca-se um estudo de Ahmed et al. [25] que aborda a segurança dos dispositivos IoT e as soluções baseadas em *blockchain* para solucionar os desafios de segurança. Ele começa apresentando a importância da segurança dos dispositivos IoT e as principais ameaças de segurança, como ataques DDoS e roubo de identidade. O texto revisa as soluções existentes para a segurança dos dispositivos IoT, incluindo criptografia, autenticação e monitoramento. Em seguida, o artigo apresenta soluções baseadas em *blockchain*, destacando as diferentes formas de integração e suas vantagens e desvantagens.

Por fim, o texto discute os desafios e áreas em aberto na pesquisa de segurança dos dispositivos IoT e *blockchain*, como interoperabilidade, confiança, governança e privacidade. O trabalho é uma revisão abrangente e atualizada que fornece informações úteis para pesquisadores e profissionais que trabalham com dispositivos IoT e segurança da informação.

Os artigos apresentados são, em sua maioria, revisões bibliográficas, que fornecem uma visão abrangente das ameaças e vulnerabilidades à segurança e privacidade nos dispositivos IoT. Tendo isso em mente, essa pesquisa se diferencia dos trabalhos citados por ter um foco específico em um ambiente residencial, enquanto a maioria dos estudos existentes sobre dispositivos IoT e segurança geralmente têm um enfoque mais amplo. Além disso, pretende-se focar em estratégias práticas de segurança e privacidade, com sugestões concretas de medidas que os usuários de casas inteligentes podem adotar para proteger suas informações e dispositivos. Espera-se, assim, contribuir para o avanço do conhecimento sobre a segurança em ambientes domésticos conectados e ajudar os usuários a tomarem decisões mais informadas sobre a segurança de seus dispositivos IoT.

4. METODOLOGIA DE PESQUISA

Nesta seção, será apresentada a metodologia utilizada no desenvolvimento da pesquisa, incluindo o delineamento da pesquisa, a descrição da população e amostra utilizadas, o procedimento de coleta de dados e a análise dos dados obtidos. Dessa forma, será possível compreender de maneira clara e precisa como a pesquisa foi conduzida e quais foram os métodos utilizados para alcançar seus objetivos como mostrado na Figura 5.

Figura 5: Passos da metodologia de pesquisa, **Fonte:** Autor

Nas seções a seguir, serão fornecidos detalhes sobre cada uma das etapas percorridas nesta pesquisa.

4.1. REVISÃO BIBLIOGRÁFICA

A revisão bibliográfica realizada para esta pesquisa, foi um processo essencial para compreender e analisar o estado atual do conhecimento sobre o assunto. Essa etapa permitiu a identificação das principais fontes de informação, a coleta de dados relevantes e a análise crítica de diferentes perspectivas.

Nesta pesquisa, a abordagem qualitativa foi considerada a mais apropriada, pois permitiu obter informações detalhadas sobre as experiências e os desafios enfrentados pelos usuários em relação à segurança das soluções IoT em ambientes residenciais. Essa abordagem qualitativa possibilitou uma compreensão mais profunda das percepções e opiniões dos usuários, bem como das nuances e complexidades envolvidas no contexto da segurança.

Inicialmente, foi realizada uma extensa pesquisa em bases de dados acadêmicas (*IEEE Xplore*[6], *ACM Digital Library*[7], *Google Scholar*[8]) e em sites especializados em segurança cibernética, utilizando palavras-chave relacionadas ao tema, como "dispositivos IoT em residências", "segurança de dispositivos IoT" e "ameaças aos dispositivos IoT". Essas pesquisas permitiram obter uma ampla gama de artigos científicos, conferências e teses relevantes.

Em seguida, foram realizadas leituras de títulos e resumos dos trabalhos encontrados, a fim de selecionar aqueles que eram mais pertinentes ao escopo do trabalho. Com os artigos selecionados, foi feita uma leitura aprofundada dos conteúdos dos trabalhos. Durante essa etapa, foram identificados conceitos-chave, metodologias utilizadas, resultados obtidos e conclusões dos estudos. Além disso, foram anotados os principais pontos levantados por cada

[6] link: https://ieeexplore.ieee.org/Xplore/home.jsp
[7] link: https://dl.acm.org/
[8] link: https://scholar.google.com/

autor, destacando-se as diferentes ameaças, riscos e vulnerabilidades associados aos dispositivos IoT em residências, bem como as possíveis medidas de segurança e mitigação propostas.

Por fim, com base na revisão bibliográfica, foi possível construir um embasamento teórico sólido para o trabalho sobre ameaças e riscos a dispositivos IoT em residências. As informações coletadas e a compreensão obtida permitiram identificar as principais preocupações nesta área, bem como propor estratégias de segurança e sugestões para a proteção dos usuários em suas residências.

4.2. MAPEAMENTO DAS PRINCIPAIS APLICAÇÕES IOT EM RESIDÊNCIAS

Para iniciar o mapeamento, foi realizada uma pesquisa detalhada em fontes confiáveis, como artigos científicos, relatórios técnicos e documentos normativos. Bases de dados acadêmicas, como *IEEE Xplore*, *ACM Digital Library* e *Google Scholar*, foram exploradas usando palavras-chave relacionadas, como "aplicações de dispositivos IoT em residências", "dispositivos inteligentes para casas" e "internet das coisas em ambientes domésticos".

A partir dos estudos encontrados, foram analisadas as diferentes áreas de aplicação de dispositivos IoT em residências. Isso incluiu aspectos como automação residencial, segurança doméstica, monitoramento de energia, saúde e bem-estar, entretenimento e dispositivos conectados em geral. Cada área foi investigada para identificar os tipos de dispositivos e tecnologias IoT utilizados, bem como as funcionalidades e benefícios proporcionados aos moradores.

Durante o mapeamento, também foram considerados relatos de campo, estudos de caso e pesquisas que apresentavam exemplos reais de implementação de dispositivos IoT em ambientes residenciais. Essas fontes forneceram informações práticas e experiências concretas, enriquecendo o mapeamento e ajudando a identificar aplicações específicas e seu impacto nas residências.

4.3. IDENTIFICAÇÃO DAS PRINCIPAIS AMEAÇAS AOS DISPOSITIVOS IOT

Inicialmente, foi realizada uma revisão bibliográfica detalhada, buscando artigos científicos, relatórios técnicos, documentos normativos e pesquisas relevantes sobre o tema. Bases de dados acadêmicas, sites especializados em segurança cibernética e outras fontes confiáveis foram consultadas, utilizando palavras-chave como "ameaças a dispositivos IoT em residências", "segurança de dispositivos IoT domésticos" e "vulnerabilidades em dispositivos IoT para casas".

A partir da revisão bibliográfica, foram identificadas as principais ameaças mencionadas na literatura especializada. Isso inclui ameaças como violação de privacidade, ataques cibernéticos, roubo de dados pessoais, invasão de dispositivos, acesso não autorizado a redes domésticas, manipulação remota de dispositivos e interrupção de serviços.

Além disso, foram explorados estudos de casos reais, relatos de incidentes de segurança e notícias sobre ataques a dispositivos IoT em residências. Essas fontes forneceram *insights* valiosos sobre ameaças emergentes e casos práticos de exploração de vulnerabilidades em dispositivos IoT domésticos.

Uma vez identificadas as ameaças, elas foram catalogadas de forma organizada. Foram criadas categorias ou grupos de ameaças com base em características comuns, como o método de ataque, o tipo de vulnerabilidade explorada ou o impacto resultante. Isso permitiu uma compreensão mais estruturada das ameaças e facilitou a análise comparativa entre diferentes estudos e fontes de informação.

4.4. MAPEAMENTO DOS PRINCIPAIS RISCOS ASSOCIADOS AO IOT

Para realizar o mapeamento dos principais riscos associados a cada ameaça no trabalho sobre ameaças e riscos a dispositivos IoT em residências, foram adotadas diversas etapas visando uma compreensão aprofundada dos possíveis impactos e consequências de cada ameaça identificada.

Após a identificação e catalogação das ameaças, foi realizado um estudo sobre cada uma delas. Foram consultadas fontes como artigos científicos, relatórios técnicos, estudos de caso e pesquisas relevantes, buscando informações sobre os riscos específicos relacionados a cada ameaça em dispositivos IoT residenciais.

Além disso, foram examinados os impactos potenciais de cada ameaça para os usuários e suas residências. Isso inclui considerações sobre perda de privacidade, danos físicos, roubos de identidade, interrupção de serviços essenciais, riscos à segurança pessoal e financeira, entre outros. Com base nessa análise, os riscos associados a cada ameaça foram mapeados de forma estruturada. Foram identificadas as possíveis consequências adversas resultantes de cada ameaça.

4.5. ELABORAÇÃO DE RECOMENDAÇÕES

A elaboração de recomendações foi realizada com o objetivo de fornecer orientações práticas e medidas de segurança aos usuários para minimizar os riscos identificados. Após a identificação das ameaças e mapeamento dos riscos associados a cada uma delas, foi conduzida uma análise criteriosa dos resultados obtidos. Foram consideradas as melhores práticas de segurança cibernética, normas técnicas, diretrizes de organizações especializadas e pesquisas relevantes para embasar a elaboração das recomendações.

As recomendações foram elaboradas de forma clara e acessível, levando em consideração o público-alvo do trabalho, ou seja, os usuários comuns de dispositivos IoT em residências. Foram priorizadas recomendações que pudessem ser facilmente compreendidas e implementadas por esses usuários, independentemente de seu conhecimento técnico.

As recomendações abordam diferentes aspectos da segurança dos dispositivos IoT em residências. Foram incluídas orientações sobre configurações iniciais seguras, como a alteração de senhas padrão, a ativação de autenticação forte e a atualização regular dos

dispositivos. Além disso, foram fornecidas diretrizes sobre a proteção da rede doméstica, como a segmentação da rede, a utilização de *firewalls* e a criação de redes *wi-fi* separadas para dispositivos IoT.

Ao elaborar as recomendações, foi considerada a evolução constante das ameaças e tecnologias relacionadas a dispositivos IoT. Portanto, as recomendações foram projetadas para serem flexíveis e adaptáveis, de modo que pudessem ser atualizadas e ajustadas conforme novas ameaças e soluções de segurança surgissem.

5. RESULTADOS

Nesta seção, serão apresentados os principais resultados obtidos a partir da análise dos dados coletados. Isso inclui os achados de uma revisão bibliográfica abrangente sobre a segurança das soluções IoT residenciais, os principais desafios enfrentados pelos usuários e as práticas e tecnologias utilizadas para garantir a segurança dessas soluções. Além disso, serão discutidas as principais implicações desses resultados para o desenvolvimento de soluções IoT mais seguras e confiáveis para ambientes residenciais.

5.1. PRINCIPAIS APLICAÇÕES IOT EM AMBIENTE RESIDENCIAL

Os dispositivos IoT possuem diversas aplicações adaptáveis a diferentes tecnologias, fornecendo informações relevantes sobre atividades, sistemas e condições ambientais. Empresas de diversos setores estão adotando essa tecnologia para aprimorar, automatizar, controlar e simplificar processos domésticos. De acordo com dados divulgados pela Associação Brasileira de Automação Residencial e Predial (Aureside), o uso de dispositivos de IoT para casas inteligentes deve crescer 22% até 2025 [26], e segundo recente pesquisa da Business Insider, essa indústria de IoT irá crescer, até 2027, mais de 2,4 trilhões de dólares por ano [27].

Diante da crescente popularização do mercado de produtos inteligentes, grandes empresas estão direcionando seus investimentos para oferecer uma ampla gama de soluções que atendam tanto aos consumidores finais quanto às necessidades corporativas. A seguir, serão listadas algumas aplicações e utilização de dispositivos IoT que estarão cada vez mais presentes na vida das pessoas nos próximos anos [28].

5.1.1 Assistente de voz

Uma assistente de voz é um programa de software que utiliza tecnologias avançadas de processamento de linguagem natural e inteligência artificial para permitir que os usuários interajam com dispositivos eletrônicos por meio de comandos de voz. Essas assistentes reconhecem e interpretam a fala humana, respondendo a perguntas, executando tarefas e fornecendo informações com base nos comandos recebidos. Ao combinar assistentes de voz com dispositivos IoT, é possível criar um ecossistema no qual os dispositivos podem ser controlados e monitorados por meio de comandos de voz. Por exemplo, é possível utilizar uma assistente de voz para ligar as luzes da casa, ajustar a temperatura do ar-condicionado, reproduzir música em um alto-falante inteligente e até mesmo fazer compras online [29].

Essa integração oferece aos usuários conveniência e facilidade na gestão e controle dos dispositivos IoT, eliminando a necessidade de interfaces físicas ou aplicativos móveis. Além disso, a interconectividade entre assistentes de voz e dispositivos IoT possibilita a criação de cenários mais avançados, como a automação residencial, em que diferentes dispositivos podem ser programados para interagir entre si com base em comandos de voz ou

eventos específicos. Entre os dispositivos populares utilizados pelos usuários estão o Amazon Echo[9] (Alexa), o Google Home[10] (Google Assistant) e o Apple HomePod[11] (Siri) [29].

5.1.2 Câmeras de segurança

Câmeras de segurança IP, como a Ring [12]da Amazon, são dispositivos de vigilância que fazem parte de um sistema conectado à internet para garantir a segurança. Essas câmeras têm o propósito de capturar e transmitir imagens e vídeos em tempo real para dispositivos remotos, como *smartphones*, *tablets* ou computadores. Além disso, elas podem ser integradas a outros dispositivos IoT e sistemas de automação residencial, proporcionando um ambiente de segurança inteligente [30, 58].

Essas câmeras oferecem uma variedade de recursos, como detecção de movimento, gravação em nuvem, visão noturna, áudio bidirecional (permitindo a comunicação entre a câmera e o usuário) e *streaming* de vídeo em alta definição. Além disso, muitas câmeras de segurança de dispositivos IoT são capazes de enviar alertas e notificações aos usuários em caso de atividade suspeita ou detecção de intrusões [30, 58].

Esses recursos avançados proporcionam uma maior tranquilidade aos usuários, permitindo que eles monitorem suas propriedades de forma eficaz e tomem medidas apropriadas, se necessário. As câmeras de segurança IP são uma parte essencial de um sistema de segurança doméstica moderno, oferecendo recursos de vigilância avançados e garantindo a proteção do ambiente residencial [30, 58].

5.1.3 Termostatos inteligentes

Termostatos conectados à internet, como o Nest [13]da Google, oferecem controle automatizado da temperatura em ambientes internos. Eles possuem sensores de temperatura e umidade, além de conectividade *Wi-Fi* ou *Bluetooth*, permitindo controle remoto por meio de um aplicativo em dispositivos móveis [31, 59].

Esses termostatos aprendem e se adaptam aos hábitos de temperatura dos usuários, ajustando automaticamente a temperatura para maior conforto e eficiência energética, utilizando algoritmos e inteligência artificial , o que permite poupar energia em casa, tanto de eletricidade como de gás. Além disso, os termostatos inteligentes proporcionam recursos como programação personalizada, detecção de presença, monitoramento de consumo de energia e compatibilidade com assistentes virtuais, como a Alexa da Amazon ou o Google Assistant, permitindo ajustes de temperatura por meio de comandos de voz [31, 59].

5.1.4 Fechaduras inteligentes

---

[9] link: https://www.amazon.com.br/echo-com-alexa/b?ie=UTF8&node=19877613011
[10] link: https://home.google.com/welcome/
[11] link: https://www.apple.com/homepod/
[12] link: https://www.amazon.com/stores/Ring/Ring/page/77B53039-540E-4816-BABB-49AA21285FCF
[13] link: https://store.google.com/br/product/google_nest_mini?pli=1&hl=pt-BR

Fechaduras inteligentes, como a August Smart Lock[14] ou a Yale Linus[15], são dispositivos avançados que substituem as fechaduras tradicionais e proporcionam segurança e comodidade adicionais. Essas fechaduras possuem métodos de autenticação, como senhas, códigos PIN (*Personal Identification Number*), cartões de acesso, impressões digitais ou reconhecimento facial. Além disso, podem ser controladas remotamente por meio de *smartphones*, *tablets* ou chaves virtuais usando *bluetooth* ou *wi-fi* [32, 60].

Uma das principais vantagens das fechaduras inteligentes é a capacidade de controlar o acesso de forma remota. Por exemplo, é possível trancar ou destrancar a porta usando um aplicativo em um dispositivo móvel, mesmo estando longe de casa. Isso facilita a concessão de acesso temporário a visitantes, como familiares ou prestadores de serviços, sem a necessidade de chaves físicas. Além disso, essas fechaduras oferecem recursos como notificações em tempo real sobre atividades de entrada e saída, bem como um histórico de acesso [32, 60].

5.1.5 Lâmpadas inteligentes

Lâmpadas conectadas, como as da Philips Hue[16], são dispositivos de iluminação que podem ser controlados e gerenciados remotamente por meio de tecnologias conectadas, como *wi-fi*, *bluetooth* ou *zigbee*. Essas lâmpadas são projetadas para substituir as lâmpadas tradicionais em residências e oferecem recursos avançados e personalizados. Isso permite que os usuários ajustem o brilho, a cor e a intensidade da luz de forma conveniente, sem a necessidade de interruptores físicos [33, 61].

Além disso, as lâmpadas inteligentes podem ser integradas a assistentes de voz, como a Amazon Alexa ou o Google Assistant, permitindo controlá-las por meio de comandos de voz. Isso adiciona um nível adicional de conveniência, permitindo que os usuários liguem ou desliguem as luzes, ajustem o brilho e até mesmo criem rotinas automatizadas por meio da voz [33, 61].

Outros recursos comuns das lâmpadas inteligentes incluem programação de horários de iluminação, simulação de presença para fins de segurança, sincronização com músicas ou filmes para criar experiências imersivas, e a capacidade de serem integradas a outros dispositivos de automação residencial, como sensores de movimento ou alarmes [33, 61].

5.1.6 Plugues inteligentes

Plugues inteligentes, também conhecidos como tomadas inteligentes ou *smart plugs*, são dispositivos eletrônicos que se conectam a uma tomada de parede para controlar o fornecimento de energia a aparelhos e dispositivos conectados. Eles são controlados por meio de aplicativos em *smartphones*, *tablets* ou dispositivos de automação residencial, permitindo ligar ou desligar os dispositivos conectados, programar horários de funcionamento e criar rotinas personalizadas [34].

---

[14] link: https://august.com/products/august-smart-lock-pro-connect
[15] link: https://yalehome.es/pt/linus-smart-lock/
[16] link: https://www.philips-hue.com/pt-br

Além disso, muitos plugues inteligentes oferecem recursos como monitoramento de consumo de energia. Essa funcionalidade proporciona conveniência e economia de energia, permitindo que os usuários controlem os aparelhos de qualquer lugar. Além disso, muitos plugs inteligentes são compatíveis com assistentes de voz, como a Amazon Alexa ou o Google Assistant. Exemplos populares de plugues inteligentes incluem o TP-Link Smart Plug[17] e o Belkin WeMo Switch[18] [34].

5.1.7 Sensores de ambiente

Os sensores de ambiente, como os da empresa Eve[19], são dispositivos eletrônicos que coletam informações sobre as condições do ambiente em que estão instalados. Eles desempenham um papel crucial em diversos contextos, desde residências inteligentes até espaços comerciais e industriais. Ao fornecer dados relevantes, esses sensores possibilitam o monitoramento e controle do ambiente, otimização do consumo de energia, garantia de segurança, melhoria do conforto e tomada de decisões embasadas [35, 62].

Por exemplo, um sensor de temperatura e umidade pode ajustar automaticamente o sistema de climatização em uma casa, levando em consideração as condições ambientais. Já um sensor de qualidade do ar é capaz de detectar substâncias nocivas e acionar sistemas de ventilação ou purificação do ar. Além disso, sensores de luminosidade podem regular a iluminação de forma automática, proporcionando economia de energia [35, 62].

5.1.8 Eletrodomésticos inteligentes

Eletrodomésticos inteligentes são dispositivos eletrônicos conectados à internet que oferecem conveniência, eficiência e controle remoto. Eles se comunicam com outros dispositivos usando *Wi-fi*, *Bluetooth* ou *Zigbee*, permitindo que sejam controlados mesmo à distância. Além disso, podem ser integrados a assistentes de voz como Alexa, Google Assistant ou Siri para comandos por voz [36].

Esses eletrodomésticos têm recursos personalizáveis e automatizados. Por exemplo, uma máquina de lavar pode ser programada para iniciar uma lavagem em horário específico ou enviar notificações quando o ciclo estiver concluído. Um refrigerador inteligente monitora alimentos e envia alertas sobre itens vencidos ou em falta. Um forno inteligente pode ser pré-aquecido remotamente para facilitar o preparo de refeições [36].

Todos os dispositivos acima mencionados têm potencial para serem vulneráveis a ataques cibernéticos, no entanto, pesquisadores de segurança cibernética da multinacional Forescout Technologies, uma empresa líder em cibersegurança, conduziram uma análise abrangente de mais de 19 milhões de dispositivos conectados para identificar suas vulnerabilidades. A pesquisa, realizada em outubro de 2022, revelou que as câmeras IP são os dispositivos IoT mais suscetíveis a ataques cibernéticos [37]. Infelizmente, esses dispositivos costumam estar conectados à internet sem níveis adequados de proteção, sendo comumente

[17] link: https://www.tp-link.com/us/home-networking/smart-plug/
[18] link: https://www.belkin.com/products/wemo-smart-home/
[19] link: https://www.evehome.com/en

protegidos apenas por senhas padrão que muitos usuários não alteram. Isso facilita o trabalho dos cibercriminosos, que podem explorar essas falhas de segurança para acessar redes, computadores e servidores.

5.2. MITIGANDO AMEAÇAS E VULNERABILIDADES À DISPOSITIVOS IOT

De acordo com o OWASP IoT Top10, uma lista compilada pela *Open Web Application Security Project* (OWASP), uma comunidade global dedicada à segurança de aplicativos da web, existem as dez principais vulnerabilidades de segurança encontradas em dispositivos IoT [22, 38]. Essa lista tem o objetivo de destacar os problemas mais comuns enfrentados por esses dispositivos e auxiliar os desenvolvedores na mitigação dessas vulnerabilidades, que incluem:

5.2.1. Senhas fracas, fáceis de adivinhar ou codificadas

Quando se trata de senhas fracas e fáceis de adivinhar ou codificadas, isso pode representar um risco significativo para a segurança desses dispositivos e do sistema como um todo. Uma das ameaças mais comuns relacionadas a senhas fracas é a adivinhação de senhas. Muitas pessoas não dão a devida importância à criação de senhas fortes e únicas, geralmente utilizam uma senha fraca que carece de complexidade e é facilmente adivinhada, como sequências óbvias como "123456", "senha" ou "abc123". Essas senhas são extremamente fáceis de adivinhar e estão entre as primeiras opções que *hackers* e programas automatizados tentam ao atacar sistemas e contas online. Uma senha fraca permite que um invasor acesse facilmente informações confidenciais e comprometa a conta do usuário [40].

Além das senhas fracas, há também as senhas fáceis de adivinhar, que são baseadas em informações pessoais facilmente acessíveis, como nomes, datas de nascimento, números de telefone ou endereços. As pessoas costumam pensar que essas senhas são únicas e difíceis de serem descobertas, mas na realidade são informações que podem ser facilmente obtidas por meio de pesquisas em redes sociais ou outros métodos de engenharia social. Os *hackers* podem se passar por indivíduos confiáveis ou enviar e-mails falsos de *phishing* para enganar as pessoas a revelarem suas senhas. Isso pode ocorrer por meio de mensagens de e-mail, links maliciosos ou solicitações fraudulentas de redefinição de senha [41, 74].

Outra vulnerabilidade relacionada a senhas é a reutilização de senhas. Muitas pessoas têm o hábito de usar a mesma senha em várias contas online. Isso é extremamente arriscado, porque se uma senha for comprometida em uma plataforma, todas as outras contas com a mesma senha também estarão em risco. *Hackers* podem usar senhas comprometidas em violações de dados em larga escala para tentar acessar outras contas de um usuário [41, 74].

Outra prática comum é a codificação de senhas, que envolve o uso de padrões previsíveis ou substituições simples de caracteres. Por exemplo, substituir "a" por "@", "s" por "$" ou "o" por "0". Embora essas substituições possam parecer medidas de segurança eficazes, elas são facilmente descobertas por meio de técnicas automatizadas de *hacking* [41, 74].

Além disso, muitos dispositivos IoT são projetados com senhas padrão predefinidas que não são alteradas pelo usuário. Isso pode permitir que um invasor acesse facilmente o dispositivo, pois a senha padrão é amplamente conhecida e pode ser facilmente encontrada na internet [22, 74]. O que pode levar a um invasor a acessar um dispositivo IoT sem autorização, dando-lhe a capacidade de controlar o dispositivo, acessar dados confidenciais e até mesmo espionar as atividades dos usuários.

Diante dessas ameaças e vulnerabilidades, é essencial adotar boas práticas de segurança de senha. Felizmente, existem medidas que podem ser adotadas para mitigar esses riscos e fortalecer a segurança dos dispositivos IoT. A primeira etapa essencial é educar os usuários sobre a importância de senhas fortes e únicas. É fundamental que os usuários entendam a necessidade de alterar a senha padrão de fábrica dos dispositivos IoT e criar senhas complexas, que combinem letras maiúsculas e minúsculas, números e caracteres especiais. Além disso, é importante enfatizar que senhas únicas devem ser usadas para cada dispositivo, evitando o compartilhamento de senhas entre diferentes dispositivos ou contas [41, 52, 73].

Para criar senhas fortes para autenticação em dispositivos IoT é necessário que a senha contenha [41, 52, 73]:

- Senhas com pelo menos 12 caracteres. Quanto mais longa a senha, mais difícil será para um invasor adivinhá-la.
- Use uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais, como !, @, #, $, %, etc. Quanto mais diversificados forem os caracteres, maior será a complexidade da senha.
- Evite usar informações pessoais óbvias, como nomes, datas de nascimento, números de telefone ou endereços, como parte da senha. Essas informações são fáceis de serem adivinhadas ou descobertas por invasores.
- Evite sequências de caracteres óbvias, como "123456" ou "abcdef". Essas sequências são extremamente fracas e estão entre as primeiras opções que os invasores tentarão.
- Evite usar palavras comuns encontradas em dicionários, pois essas palavras podem ser facilmente quebradas por meio de ataques de dicionário. Se você optar por usar uma palavra, tente substituir algumas letras por números ou caracteres especiais.
- Considere usar uma frase complexa como base para sua senha. Por exemplo, "GostoDeCorrerNaPraia!".
- Não use a mesma senha para vários dispositivos. Se uma senha for comprometida, todas as suas contas estarão em risco, então utilize senhas únicas para cada conta.

No entanto, apenas uma senha robusta não garante uma segurança completa. É essencial implementar a autenticação em dois fatores (2FA) sempre que possível. Com o 2FA, além da senha, é necessário fornecer uma segunda forma de autenticação, como um código enviado por mensagem de texto ou um aplicativo de autenticação no celular. Isso adiciona uma camada extra de segurança, dificultando ainda mais o acesso não autorizado [63].

Além disso, é recomendável limitar as tentativas de senha incorretas implementando mecanismos de bloqueio temporário ou permanente. Após um número definido de tentativas de senha erradas, o acesso deve ser bloqueado. Essa medida ajuda a evitar ataques de força bruta ou adivinhação de senha, tornando mais difícil para invasores obterem acesso não autorizado [41].

5.2.2. Serviços de rede inseguros

Os dispositivos IoT são compostos por uma grande variedade de dispositivos conectados à internet, incluindo sensores, câmeras, termostatos, medidores inteligentes, entre outros. Esses dispositivos se comunicam com a internet por meio de redes, como *Wi-fi*, *Bluetooth*, celular, *Zigbee* e outras. Quando essas redes são inseguras, elas podem representar um risco significativo para a segurança de dispositivos IoT [22, 39, 44].

Uma das principais ameaças é o acesso não autorizado. *Hackers* e indivíduos mal-intencionados podem explorar vulnerabilidades em serviços de rede inseguros para obter acesso não autorizado a sistemas e dados sensíveis. Isso pode levar ao roubo de informações confidenciais, comprometimento da integridade dos dados, interrupção de serviços e perda financeira. Falhas de autenticação, senhas fracas, configurações de permissões inadequadas e falta de monitoramento de acesso são algumas das vulnerabilidades que podem ser exploradas nesse tipo de ataque [42, 43, 44].

Outra ameaça é a exposição de informações sensíveis. Serviços de rede inseguros podem expor informações sensíveis, como dados pessoais, credenciais de login e informações confidenciais da empresa. Isso pode resultar em roubo de identidade, violações de privacidade, comprometimento de contas e possíveis repercussões legais e de reputação. Configurações incorretas de permissões, falta de criptografia de dados em trânsito e em repouso, e falta de atualizações de segurança são algumas das vulnerabilidades que podem levar à exposição de informações sensíveis [42, 43, 44].

O ataque de negação de serviço (DoS) e os ataques de amplificação também são problemas associados aos serviços de rede inseguros. Atacantes podem direcionar esses serviços para sobrecarregar recursos, causando indisponibilidade e interrupção de serviços. Isso pode levar à perda de produtividade, interrupção de operações críticas e danos à reputação da organização. Configurações inadequadas de limitação de tráfego, falta de monitoramento de tráfego malicioso e falhas de segurança em protocolos de rede são algumas das vulnerabilidades que podem ser exploradas nesses tipos de ataques [42, 43, 44].

A injeção de código e a exploração de vulnerabilidades são ameaças que podem comprometer a segurança dos serviços de rede. Serviços inseguros podem conter vulnerabilidades que permitem a injeção de código malicioso ou a exploração de falhas conhecidas. Isso pode resultar na execução de comandos arbitrários, comprometimento de dados e controle total sobre o sistema afetado. Falhas de validação de entrada, falta de sanitização de dados, falta de atualizações de segurança e falta de monitoramento de atividades suspeitas são algumas das vulnerabilidades que podem ser exploradas nesses tipos de ataques [42, 43, 44].

Além disso, o *spoofing* é uma ameaça adicional relacionada aos serviços de rede inseguros. O *spoofing* envolve a falsificação de identidade ou origem, onde um atacante mascara sua identidade para parecer legítimo. Isso pode ser usado para enganar usuários ou sistemas, permitindo o acesso não autorizado, interceptação de dados ou manipulação de tráfego. É fundamental implementar mecanismos de autenticação robustos e verificar a integridade dos dados para mitigar os riscos associados ao spoofing [42, 43, 44].

Por fim, a interceptação e manipulação de tráfego são ameaças que podem comprometer a integridade e a confidencialidade dos dados em trânsito. Serviços de rede inseguros podem permitir que atacantes interceptem e manipulem o tráfego de dados, possibilitando a captura de informações confidenciais e a falsificação de dados. Isso pode levar ao roubo de dados sensíveis, falsificação de informações e comprometimento da segurança do sistema [42, 43, 44].

Em resumo, serviços de rede inseguros apresentam ameaças significativas à segurança cibernética. É crucial implementar configurações adequadas, políticas de segurança, atualizações de *software* e monitoramento constante para mitigar riscos e vulnerabilidades, incluindo o *spoofing*. A segurança dos serviços de rede é fundamental para proteger os sistemas, dados e a reputação das organizações contra ataques cibernéticos. Aqui estão algumas medidas importantes para mitigar os riscos e garantir serviços de redes para dispositivos IoT mais seguros [42, 64, 65]:

- Utilize criptografia robusta para proteger a comunicação entre dispositivos IoT e serviços de rede. Isso inclui o uso de protocolos seguros, como o HTTPS, e a implementação de *firewalls* e VPNs (Redes Privadas Virtuais) para garantir a proteção dos dados durante a transmissão.
- Separe sua rede em segmentos distintos para isolar os dispositivos IoT dos outros sistemas. Dessa forma, se um dispositivo for comprometido, o ataque não se espalhará para toda a rede, limitando os danos.
- Exija autenticação robusta para acessar serviços de rede e dispositivos IoT. Utilize senhas fortes, autenticação em dois fatores (2FA) e outros mecanismos avançados, como certificados digitais, quando disponíveis. Isso aumenta a segurança e dificulta o acesso não autorizado.
- Implemente sistemas de monitoramento de tráfego de rede para detectar atividades suspeitas ou não autorizadas. Essa prática permite identificar tentativas de invasão e comportamentos anormais nos dispositivos IoT e serviços de rede, possibilitando uma resposta rápida.
- Estabeleça políticas rigorosas de controle de acesso aos serviços de rede de dispositivos IoT. Conceda privilégios apenas aos usuários autorizados e restrinja permissões desnecessárias. Isso reduz o risco de acessos não autorizados e uso indevido dos serviços.
- Eduque os usuários sobre práticas de segurança, como evitar clicar em links suspeitos, não compartilhar informações confidenciais e realizar atualizações de segurança em seus dispositivos pessoais. A conscientização dos usuários é uma medida eficaz na prevenção de ataques cibernéticos.

É importante ressaltar que a segurança em dispositivos IoT e serviços de rede é um processo contínuo. Manter-se atualizado sobre as atualizações de segurança, esteja ciente das ameaças emergentes e esteja preparado para tomar medidas para proteger seus dispositivos e dados conforme necessário. Ao adotar essas práticas, estaremos fortalecendo a segurança dos serviços de redes para dispositivos IoT e minimizando os riscos de violações de segurança [42, 64].

5.2.3. Interfaces de ecossistema inseguras

As interfaces de ecossistema referem-se às plataformas, aplicativos ou sistemas que permitem aos usuários interagir e controlar seus dispositivos IoT. Quando essas interfaces são inseguras, elas podem fornecer uma oportunidade para os invasores explorarem vulnerabilidades e comprometer a segurança dos dispositivos IoT e dos dados associados. Alguns exemplos de interfaces de ecossistema inseguras incluem aplicativos móveis com falhas de segurança, sistemas web sem autenticação adequada ou protocolos de comunicação desprotegidos [22, 39].

Uma das principais vulnerabilidades é a falta de autenticação adequada nas interfaces de ecossistema. Quando não há uma autenticação robusta para verificar a identidade e as permissões dos usuários, pessoas não autorizadas podem acessar informações confidenciais e executar ações não autorizadas. Isso pode levar a vazamentos de dados, comprometimento de contas e até mesmo roubo de identidade [44, 74].

Além disso, *interfaces* de ecossistema inseguras podem ter vulnerabilidades de segurança que são exploradas por *hackers*. Isso inclui brechas de segurança no código, falta de criptografia de dados sensíveis, falta de controle de acesso adequado e erros de configuração. Os invasores podem explorar essas vulnerabilidades para obter acesso não autorizado, alterar dados, distribuir *malware* ou realizar ataques de negação de serviço [44, 74].

Outra vulnerabilidade significativa é a falta de monitoramento e detecção de atividades suspeitas nas interfaces de ecossistema. Sem sistemas de monitoramento adequados, é difícil identificar atividades maliciosas ou incomuns que possam indicar um ataque em andamento. Isso permite que os invasores operem de maneira discreta e prolongada, causando danos substanciais antes que sejam detectados [44, 74].

Além disso, interfaces de ecossistema inseguras também podem ser alvos de ataques de engenharia social. Os *hackers* podem usar táticas de manipulação psicológica para enganar os usuários e obter acesso não autorizado. Isso pode incluir *phishing*, onde os usuários são levados a fornecer informações confidenciais, ou *pretexting*, onde os invasores se passam por indivíduos confiáveis para obter acesso indevido [44, 74].

É importante mencionar também os problemas associados à falta de atualizações e *patches* de segurança nas interfaces de ecossistema. Se as atualizações de segurança não forem implementadas regularmente, as vulnerabilidades conhecidas não serão corrigidas, deixando os sistemas abertos a ataques conhecidos [44, 74].

Para mitigar essas ameaças e vulnerabilidades, é fundamental implementar práticas de segurança adequadas nas interfaces de ecossistema. Isso envolve implementar criptografia robusta para proteger a comunicação entre os dispositivos IoT e as *interfaces*, além de garantir uma autenticação sólida para verificar a identidade do usuário. Além disso, é fundamental realizar auditorias regulares de segurança para identificar possíveis falhas e agir rapidamente para corrigi-las [53].

É igualmente importante educar os usuários sobre os problemas associados às interfaces de ecossistema inseguras e incentivá-los a utilizar apenas interfaces confiáveis e atualizadas. A conscientização sobre boas práticas de segurança, como a importância de não compartilhar informações confidenciais e de manter as interfaces atualizadas com as últimas correções de segurança, desempenha um papel fundamental na proteção dos dispositivos IoT e na mitigação dos riscos de segurança [53].

Ao adotar essas medidas, fabricantes, desenvolvedores e usuários podem trabalhar juntos para garantir a segurança das interfaces de ecossistema IoT, protegendo a privacidade, a integridade dos dados e a confiança no ecossistema IoT como um todo.

5.2.4. Falta de mecanismo seguros de atualização

A falta de mecanismos seguros de atualização representa uma ameaça significativa à segurança de sistemas e softwares. Quando os mecanismos de atualização não são implementados corretamente ou são negligenciados, surgem riscos e vulnerabilidades que podem ser explorados por atacantes maliciosos. Neste texto, discutiremos as ameaças, riscos, vulnerabilidades e ataques associados à falta de mecanismos seguros de atualização [22, 39].

Um dos principais problemas é a exploração de vulnerabilidades conhecidas. Os desenvolvedores de *software* estão constantemente descobrindo e corrigindo vulnerabilidades em seus produtos. No entanto, se os usuários não atualizam regularmente seus sistemas e aplicativos, ficam expostos a ataques que exploram essas vulnerabilidades conhecidas. Os invasores podem tirar proveito de falhas de segurança não corrigidas para obter acesso não autorizado, roubar informações confidenciais ou causar danos aos sistemas [44].

Além disso, a falta de atualizações pode levar a sistemas desatualizados e obsoletos. Com o tempo, sistemas e *softwares* desatualizados podem apresentar incompatibilidades, mau funcionamento e falhas de segurança. Sem correções e melhorias regulares, os sistemas se tornam vulneráveis a ataques mais avançados e sofisticados. Os invasores podem aproveitar essas vulnerabilidades para penetrar nos sistemas e comprometer a integridade dos dados [44].

Outra vulnerabilidade é a falta de proteção contra *malwares* e códigos maliciosos. As atualizações de *software* muitas vezes incluem patches de segurança que corrigem falhas e fecham brechas exploradas por *malware*. Quando os usuários não atualizam seus sistemas, eles não têm acesso a essas correções vitais de segurança, deixando seus dispositivos e informações vulneráveis a infecções por *malware*. Isso pode levar a uma série de problemas, como roubo de dados, perda de privacidade e danos ao funcionamento do sistema [44].

Além disso, a falta de mecanismos seguros de atualização também pode abrir caminho para ataques de engenharia social. Os invasores podem se aproveitar da falta de conscientização sobre a importância das atualizações de segurança e enviar falsas notificações de atualização para enganar os usuários a baixar e instalar *malware* disfarçado. Esses ataques podem resultar em infecções por *malware* e comprometimento do sistema [44].

Para mitigar essas ameaças, é fundamental implementar mecanismos seguros de atualização. Para isso é essencial que os fabricantes de dispositivos IoT implementem mecanismos seguros de atualização. Isso inclui a criptografia dos pacotes de atualização, a assinatura digital para garantir a autenticidade dos pacotes e a autenticação robusta para confirmar a identidade do servidor de atualização. Além disso, os fabricantes devem fornecer informações claras sobre as atualizações de segurança e notificar os usuários quando uma atualização estiver disponível. Os usuários também devem ser incentivados a manter seus dispositivos IoT atualizados aplicando as atualizações fornecidas pelos fabricantes o mais rápido possível para proteger seus dispositivos IoT [54].

5.2.5. Uso de componentes vulneráveis ou obsoletos

O uso de componentes vulneráveis ou obsoletos em sistemas e softwares representa uma ameaça significativa à segurança cibernética. Quando os desenvolvedores utilizam componentes desatualizados ou com falhas conhecidas, estão expondo seus sistemas a possíveis ataques que podem ser explorados por atacantes maliciosos. Neste texto, abordaremos as ameaças, riscos, vulnerabilidades e ataques associados ao uso de componentes vulneráveis ou obsoletos [22, 39].

Uma das principais ameaças é a exploração de vulnerabilidades conhecidas nos componentes. À medida que os desenvolvedores identificam e corrigem falhas de segurança em seus produtos, os atacantes também acompanham essas atualizações para explorar as vulnerabilidades existentes em sistemas desatualizados. Se os componentes utilizados em um sistema não forem atualizados regularmente, as falhas conhecidas podem ser exploradas, permitindo que os invasores acessem informações sensíveis, executem código malicioso ou causem danos ao sistema [44].

Além disso, o uso de componentes obsoletos pode levar a sistemas desatualizados e incompatíveis. Com o tempo, os componentes podem se tornar incompatíveis com as versões mais recentes de outros *softwares*, sistemas operacionais ou protocolos de segurança. Isso pode resultar em mau funcionamento do sistema, falhas de segurança e interrupções na operação. Os invasores podem explorar essas incompatibilidades para interromper serviços, obter acesso não autorizado ou causar danos aos sistemas [44].

Outro problema é a falta de suporte e atualizações para componentes obsoletos. À medida que novas vulnerabilidades são descobertas e técnicas de ataque evoluem, os desenvolvedores continuam aprimorando seus produtos e fornecendo atualizações de segurança. No entanto, se um componente estiver obsoleto e não receber mais suporte, não haverá correções ou patches para as vulnerabilidades identificadas. Isso deixa os sistemas vulneráveis a ataques que podem explorar essas falhas não corrigidas [44].

Para mitigar esses riscos, é essencial que os fabricantes de dispositivos IoT implementem práticas de segurança adequadas em relação aos componentes que utilizam. Isso inclui a seleção cuidadosa de fornecedores confiáveis, a verificação da segurança dos componentes antes da sua inclusão nos dispositivos, a adoção de práticas de desenvolvimento seguro e a implementação de processos de atualização e correção de vulnerabilidades. Além disso, é importante que os fabricantes monitorem regularmente a segurança dos componentes utilizados e forneçam atualizações de segurança quando necessário [66].

5.2.6. Proteção à privacidade insuficiente

O ecossistema IoT é composto por uma grande quantidade de dispositivos que coletam dados de diferentes fontes, incluindo informações pessoais de usuários. Esses dados podem ser usados para fornecer serviços personalizados e melhorar a experiência do usuário, mas também podem ser usados para fins mal-intencionados, como roubo de identidade, extorsão ou espionagem. Um exemplo comum de proteção insuficiente à privacidade é a coleta de dados sem o consentimento adequado dos usuários [22, 39].

Uma das principais ameaças é o acesso não autorizado aos dados pessoais. Se as organizações não adotarem medidas de segurança adequadas, como criptografia, controle de acesso e autenticação robusta, indivíduos mal-intencionados podem obter acesso indevido a informações sensíveis. Isso pode resultar em roubo de identidade, fraudes financeiras, violações de confidencialidade e danos à reputação dos usuários [45].

Além disso, a falta de proteção à privacidade também pode levar a vazamentos de dados. Se os sistemas não forem adequadamente protegidos contra ataques cibernéticos, os *hackers* podem explorar vulnerabilidades e obter acesso aos dados pessoais armazenados. Esses vazamentos podem expor informações confidenciais, como nomes, endereços, números de telefone, informações financeiras e até mesmo informações médicas. Os dados vazados podem ser usados para fins maliciosos, como chantagem, extorsão ou até mesmo para a realização de ataques mais direcionados [45].

Outro problema é a falta de transparência nas práticas de coleta e uso de dados. Quando as organizações não informam claramente aos usuários como seus dados serão coletados, armazenados e utilizados, os usuários perdem o controle sobre suas informações pessoais. Isso pode resultar em violações de privacidade, uso indevido de dados e até mesmo compartilhamento de informações com terceiros sem o consentimento adequado. Os usuários têm o direito de saber como suas informações estão sendo tratadas e devem ter a oportunidade de consentir ou não com o uso de seus dados [45].

Além disso, a proteção insuficiente à privacidade também pode resultar em ataques de engenharia social. Os invasores podem aproveitar as informações pessoais disponíveis publicamente ou obtidas de vazamentos de dados para manipular os usuários e obter acesso a mais informações confidenciais. Isso pode incluir a solicitação de senhas, números de cartão de crédito ou outras informações pessoais sob falsos pretextos. Os ataques de engenharia

social são frequentemente bem-sucedidos quando os usuários não estão devidamente informados e treinados para identificar essas ameaças [45].

Para proteger a privacidade nos dispositivos IoT, é essencial que os fabricantes implementem medidas de segurança adequadas para proteger os dados coletados pelos dispositivos. Isso inclui o uso de criptografia de dados, autenticação adequada e práticas de desenvolvimento seguro. Além disso, os fabricantes devem fornecer informações claras sobre como os dados serão usados e compartilhados e obter o consentimento dos usuários para coletar esses dados [45, 67].

Os usuários também têm um papel importante na proteção de sua própria privacidade. Eles devem estar cientes dos dados que estão sendo coletados pelos dispositivos IoT e de como esses dados serão usados e compartilhados. Eles também devem tomar medidas para proteger seus próprios dispositivos IoT, como mudar senhas padrão, atualizar o *firmware* regularmente e adotar práticas de segurança online [45, 67].

5.2.7. Transferência e armazenamento de dados inseguros

Os dispositivos IoT desempenham um papel fundamental na coleta e compartilhamento de uma quantidade significativa de dados, que podem conter informações pessoais, dados de sensores e outras informações sensíveis. No entanto, se esses dados forem transferidos e armazenados de forma insegura, podem se tornar alvo de ataques cibernéticos e violações de privacidade [22, 39].

Uma das principais ameaças é a interceptação de dados durante a transferência. Se os dados forem transmitidos sem a devida criptografia ou em canais de comunicação inseguros, os atacantes podem interceptar e capturar informações confidenciais. Isso pode ocorrer em redes *wi-fi* públicas, nas quais os dados são transmitidos sem proteção adequada, ou em casos de ataques de "*man-in-the-middle*", nos quais um invasor se posiciona entre o remetente e o destinatário para interceptar e alterar os dados [46].

Além disso, o armazenamento inadequado de dados também representa um risco significativo. Se os dados forem armazenados em servidores desprotegidos ou com configurações incorretas, eles podem ser alvo de ataques de *hackers*. Os invasores podem explorar vulnerabilidades nos sistemas de armazenamento, como servidores mal configurados, senhas fracas ou falta de atualizações de segurança, para acessar os dados armazenados. Isso pode resultar em roubo de informações confidenciais, violações de privacidade e até mesmo a exposição de dados sensíveis de clientes ou usuários [46].

Outra ameaça é a perda de dados durante a transferência ou armazenamento. Se não forem implementados mecanismos adequados de *backup*, replicação e recuperação de dados, há o risco de perda de informações críticas em caso de falhas nos sistemas ou desastres naturais. Isso pode levar à interrupção dos negócios, perda de dados irreversíveis e danos à reputação da organização [46].

Além disso, a falta de controle de acesso e autenticação fraca também é uma vulnerabilidade significativa. Se os sistemas não implementarem medidas adequadas para controlar quem pode acessar e modificar os dados, bem como para garantir que apenas usuários autorizados tenham permissão de acesso, os dados ficam expostos a possíveis abusos internos ou ataques de invasores externos que obtiveram credenciais de acesso [46].

A transferência e o armazenamento de dados inseguros em dispositivos IoT representam um risco significativo para a privacidade e a segurança dos usuários. Para mitigar esse problema, é necessário adotar medidas de segurança adequadas [46, 68]. Aqui estão algumas ações importantes a serem consideradas [69]:

- Utilizar protocolos de comunicação seguros, como SSL/TLS, para criptografar a transferência de dados entre os dispositivos e os servidores.
- Implementar autenticação forte para garantir a identidade dos dispositivos e usuários envolvidos na troca de dados.
- Criptografar dados sensíveis durante o armazenamento, tanto em dispositivos locais quanto em servidores remotos.
- Manter os dispositivos IoT atualizados com as últimas correções de segurança para evitar vulnerabilidades conhecidas.
- Utilizar técnicas de segmentação de rede e *firewalls* para proteger o tráfego de dados e evitar o acesso não autorizado aos dispositivos e servidores.
- Seguir as práticas recomendadas de segurança e privacidade, como a minimização de dados, o uso de políticas de retenção adequadas e a garantia de conformidade com regulamentações relevantes.

Além disso, é importante que os usuários estejam cientes dos riscos de transferência e armazenamento inseguros de dados e tomem medidas para proteger suas próprias informações. Isso pode incluir a escolha de dispositivos IoT de fabricantes confiáveis, a configuração correta das opções de segurança nos dispositivos e a revisão das políticas de privacidade e segurança fornecidas pelos fabricantes [69].

5.2.8. Falta de gerenciamento de dispositivos

O gerenciamento eficaz de dispositivos IoT é fundamental para garantir a segurança e a funcionalidade desses dispositivos. Isso inclui uma série de medidas, como a capacidade de atualizar o *software* do dispositivo para corrigir vulnerabilidades de segurança, monitorar o desempenho e controlar o acesso aos dispositivos. É importante ressaltar que os dispositivos IoT geralmente possuem ciclos de vida mais curtos em comparação aos dispositivos tradicionais. Isso significa que a falta de gerenciamento adequado pode resultar em dispositivos obsoletos e vulneráveis em uso, representando um risco significativo para a segurança dos dados e das redes [22, 39].

Uma das principais vulnerabilidades é a falta de atualizações de segurança. Quando os dispositivos não são atualizados regularmente com os *patches* de segurança mais recentes, eles permanecem vulneráveis a vulnerabilidades conhecidas. Os invasores podem explorar

essas falhas de segurança para obter acesso não autorizado aos dispositivos, roubar informações confidenciais ou comprometer a integridade dos sistemas. A falta de gerenciamento de dispositivos dificulta a aplicação consistente de atualizações críticas de segurança, tornando os dispositivos um alvo fácil para ataques [47].

A falta de configuração adequada dos dispositivos também representa um risco. Quando os dispositivos são implantados sem uma configuração segura, eles podem ter portas abertas desnecessárias, senhas padrão não alteradas ou permissões excessivas. Isso permite que os invasores acessem os dispositivos de forma não autorizada e explorem suas vulnerabilidades. Um exemplo comum é o uso de senhas padrão não alteradas em roteadores ou câmeras de segurança, o que facilita o acesso não autorizado e o controle desses dispositivos [47].

Outra vulnerabilidade é a falta de controle de acesso aos dispositivos. Quando não há políticas e mecanismos adequados para controlar quem pode acessar e usar os dispositivos, qualquer pessoa pode ter acesso irrestrito. Isso pode levar a um uso indevido dos dispositivos por funcionários mal-intencionados, invasão física por pessoas não autorizadas ou até mesmo o roubo dos dispositivos. O acesso não autorizado aos dispositivos pode resultar na exposição de dados sensíveis, interrupção dos serviços ou até mesmo no comprometimento de toda a rede [47].

Além disso, a falta de monitoramento dos dispositivos também representa uma vulnerabilidade. Quando não há um acompanhamento contínuo das atividades dos dispositivos, os ataques ou comportamentos maliciosos podem passar despercebidos. Os invasores podem explorar os dispositivos comprometidos para realizar atividades ilegais, como o envio de spam, ataques de negação de serviço ou o estabelecimento de *bots* para executar atividades maliciosas em larga escala. Sem um monitoramento adequado, essas atividades podem causar danos significativos antes de serem detectadas [47].

A falta de gerenciamento adequado dos dispositivos IoT pode levar a riscos de segurança e funcionamento inadequado. Para mitigar esse problema, é fundamental implementar práticas de gerenciamento eficazes. Aqui estão algumas medidas importantes a serem consideradas [47, 70]:

- Inventário e monitoramento: É essencial ter um inventário atualizado de todos os dispositivos IoT em uso. Isso permite rastrear e monitorar cada dispositivo, garantindo que estejam operacionais e atualizados com as últimas correções de segurança. Além disso, o monitoramento contínuo ajuda a detectar atividades suspeitas ou anormais nos dispositivos, permitindo uma resposta rápida a possíveis ameaças.
- Atualizações de *firmware*: Os dispositivos IoT devem receber atualizações regulares de *firmware* para corrigir vulnerabilidades conhecidas e melhorar o desempenho. É importante garantir que os dispositivos estejam configurados para receber automaticamente essas atualizações ou implementar um processo de atualização consistente para mantê-los seguros e funcionando corretamente.

- Políticas de acesso e autenticação: Estabeleça políticas claras de acesso e autenticação para os dispositivos IoT. Isso inclui a implementação de senhas fortes, autenticação em dois fatores (2FA) e a restrição de privilégios de acesso. Certifique-se de que apenas usuários autorizados tenham permissão para acessar e controlar os dispositivos, reduzindo o risco de invasões e uso indevido.
- Gerenciamento remoto: Utilize soluções de gerenciamento remoto para controlar e atualizar os dispositivos IoT de forma centralizada. Isso facilita a aplicação consistente de políticas de segurança, a instalação de *patches* de segurança e a implementação de configurações atualizadas. O gerenciamento remoto também permite o monitoramento em tempo real e a resolução de problemas de forma eficiente.
- Segurança de rede: Implemente medidas de segurança de rede, como *firewalls* e segmentação de rede, para isolar os dispositivos IoT de outros sistemas e limitar a exposição a possíveis ataques. A segmentação de rede também ajuda a controlar o tráfego entre dispositivos IoT, aumentando a proteção e a privacidade dos dados.
- Auditorias regulares: Realizar auditorias periódicas nos dispositivos IoT para identificar possíveis vulnerabilidades ou configurações inadequadas. Essas auditorias devem abranger aspectos como configurações de segurança, atualizações de *firmware* e conformidade com políticas de segurança estabelecidas. As descobertas dessas auditorias devem ser tratadas prontamente, com a implementação de medidas corretivas necessárias.
- Conscientização e treinamento: Eduque os usuários sobre boas práticas de gerenciamento de dispositivos IoT. Isso inclui orientá-los sobre a importância de atualizações de segurança, a configuração adequada dos dispositivos e o reconhecimento de possíveis sinais de comprometimento. Treinamentos regulares ajudam a garantir que os usuários estejam atualizados e conscientes das melhores práticas de gerenciamento de dispositivos IoT.

Ao adotar essas medidas de gerenciamento adequado, é possível mitigar os riscos associados à falta de gerenciamento de dispositivos IoT. Garantir a segurança, integridade e desempenho desses dispositivos é fundamental para aproveitar os benefícios da IoT de maneira confiável e protegida [70].

5.2.9. Configurações padrão inseguras

Os fabricantes frequentemente fornecem dispositivos IoT aos usuários com configurações padrão que podem apresentar falhas em termos de segurança, tornando-os inseguros ou inadequados. Isso inclui o uso de senhas fracas, nomes de usuário padrão e serviços de rede desnecessários ativados automaticamente. Infelizmente, muitos usuários de dispositivos IoT desconhecem a importância de alterar essas configurações padrão para proteger seus dispositivos [22, 39].

Uma das principais ameaças é a exploração de senhas padrão não alteradas. Muitos dispositivos e sistemas vêm com senhas padrão predefinidas, que são amplamente conhecidas e publicamente disponíveis. Os atacantes podem facilmente descobrir essas senhas e obter acesso não autorizado aos dispositivos ou sistemas. Com o acesso, eles podem roubar informações confidenciais, comprometer a integridade dos dados ou até mesmo controlar completamente o dispositivo ou sistema comprometido [44].

As configurações padrão podem permitir a abertura de portas desnecessárias e serviços não utilizados. Isso cria uma superfície maior de ataque, oferecendo aos invasores mais pontos de entrada potenciais. Os invasores podem explorar essas portas abertas e serviços não utilizados para encontrar vulnerabilidades e comprometer a segurança do sistema. Isso pode resultar em ataques de negação de serviço, invasão de privacidade, roubo de dados ou até mesmo no controle total do sistema comprometido [44].

Outra vulnerabilidade é a falta de criptografia nas configurações padrão. Se os dispositivos ou sistemas não estiverem configurados para usar criptografia por padrão, as informações transmitidas e armazenadas podem estar expostas a interceptações por atacantes. Isso pode permitir que eles acessem dados sensíveis, como senhas, informações financeiras e dados pessoais. A falta de criptografia também pode facilitar ataques de *spoofing*, onde os invasores se passam por dispositivos ou sistemas legítimos para obter informações confidenciais dos usuários [44].

Além disso, as configurações padrão podem permitir que dispositivos ou sistemas executem serviços desnecessários ou vulneráveis. Isso pode incluir serviços de rede não essenciais ou versões desatualizadas de *software* que contêm falhas de segurança conhecidas. Os invasores podem explorar essas vulnerabilidades para obter acesso não autorizado, instalar malware ou comprometer a integridade dos dados. Esses ataques podem resultar em roubo de informações, interrupção de serviços ou até mesmo na invasão de sistemas inteiros [44].

A utilização de configurações padrão inseguras em dispositivos IoT é um problema comum que pode comprometer a segurança desses dispositivos e das redes em que estão conectados. Para mitigar esses problemas, é necessário adotar medidas de segurança adequadas desde o início. Para isso, é necessário alterar as configurações padrão imediatamente após a instalação do dispositivo, incluindo senhas, nomes de usuário e serviços de rede ativados por padrão [44, 71].

Além disso, é importante verificar se há serviços ou funcionalidades desnecessárias ativadas no dispositivo IoT. Muitos dispositivos vêm com recursos ativados por padrão que podem representar riscos de segurança, por isso é importante desabilitar qualquer serviço que não seja essencial para o funcionamento do dispositivo [47, 71].

5.2.10. Falta de endurecimento físico

O endurecimento físico é uma prática essencial para fortalecer a segurança de dispositivos IoT, visando protegê-los contra ameaças físicas, como roubo, vandalismo ou acesso não autorizado. Embora muitos dispositivos IoT sejam projetados com a portabilidade

e a compacticidade em mente, essa característica pode torná-los suscetíveis a ataques físicos [22, 39, 44].

Uma das ameaças mais óbvias é o acesso não autorizado às instalações físicas. Se as medidas de segurança física não forem adequadamente implementadas, como portas trancadas, câmeras de vigilância, sistemas de controle de acesso e proteção de perímetro, pessoas não autorizadas podem entrar nas instalações e ter acesso direto aos ativos de TI. Isso pode levar a roubos, danos físicos, violação de dados e comprometimento da segurança geral do sistema [39, 44].

Além disso, a falta de endurecimento físico pode expor os ativos a ameaças ambientais. Por exemplo, a ausência de sistemas de controle de temperatura e umidade pode levar a danos nos equipamentos, como superaquecimento ou condensação excessiva. Falhas na proteção contra incêndios também podem resultar em danos graves ou destruição dos ativos físicos e, consequentemente, na perda irreversível de dados importantes [39, 44].

Outra ameaça é a possibilidade de manipulação física ou sabotagem dos ativos. Sem medidas adequadas de endurecimento físico, os atacantes podem acessar diretamente os dispositivos e sistemas, modificá-los, injetar *malware* ou implantar dispositivos de espionagem. Isso pode comprometer a integridade dos dados, a confidencialidade das informações e a disponibilidade dos sistemas. Os ataques físicos também podem ser mais difíceis de detectar e rastrear do que os ataques cibernéticos, tornando-os uma ameaça significativa à segurança [39, 44].

Além disso, a falta de proteção física adequada pode permitir o acesso a informações sensíveis. Por exemplo, se os servidores ou dispositivos de armazenamento não forem adequadamente protegidos em salas de servidores ou *data centers*, pessoas não autorizadas podem ter acesso direto a dados confidenciais. Isso pode levar a violações de privacidade, roubo de informações, perda de propriedade intelectual e danos à reputação da organização [39, 44].

Para mitigar esses riscos, é crucial implementar práticas de endurecimento físico na IoT. Uma medida importante é posicionar os dispositivos IoT em locais seguros e de difícil acesso para pessoas não autorizadas. É fundamental evitar deixá-los expostos em áreas de fácil alcance ou visibilidade, como próximos a janelas ou portas. Além disso, é altamente recomendável utilizar gabinetes ou invólucros resistentes para proteger os dispositivos IoT contra danos físicos e manipulação não autorizada. Esses invólucros devem ser fabricados com materiais duráveis e de difícil violação, como aço ou alumínio, e podem ser equipados com fechaduras para garantir acesso restrito [44, 72].

No caso de dispositivos IoT instalados em ambientes externos, é essencial verificar se estão protegidos contra intempéries, como chuva, umidade, calor excessivo ou frio extremo. Certifique-se de que os invólucros ou gabinetes ofereçam proteção adequada contra esses elementos. Além disso, é uma boa prática restringir o acesso físico aos dispositivos IoT apenas a pessoas autorizadas. Implemente medidas de controle de acesso, como bloqueios

com chave, cartões de acesso ou biometria, para assegurar que apenas indivíduos autorizados possam interagir fisicamente com os dispositivos [44, 72].

É fundamental destacar que, antes de descartar ou reutilizar dispositivos IoT, é necessário garantir que todas as informações sensíveis tenham sido devidamente removidas. Isso inclui dados de configuração, informações de autenticação e quaisquer outros dados que possam comprometer a segurança ou privacidade dos usuários [44, 72].

5.3. TAXONOMIA DE VULNERABILIDADES EM DISPOSITIVOS IOT EM AMBIENTE RESIDENCIAL

As vulnerabilidades associadas à utilização de dispositivos IoT em ambientes residenciais abrangem vários aspectos de segurança, tais como interfaces, dados, dispositivos, redes e infraestrutura. Agora, será explorado cada um desses itens em detalhes, de acordo com o que segue.

5.3.1. Segurança de dispositivos

Em relação à segurança de dispositivos, a Figura 6 abaixo ilustra uma série de vulnerabilidades associadas a ecossistemas com interfaces inseguras. Essas vulnerabilidades incluem senhas fracas, fáceis de adivinhar ou codificadas, uso de componentes vulneráveis ou obsoletos, configurações padrão inseguras e falta de endurecimento físico.

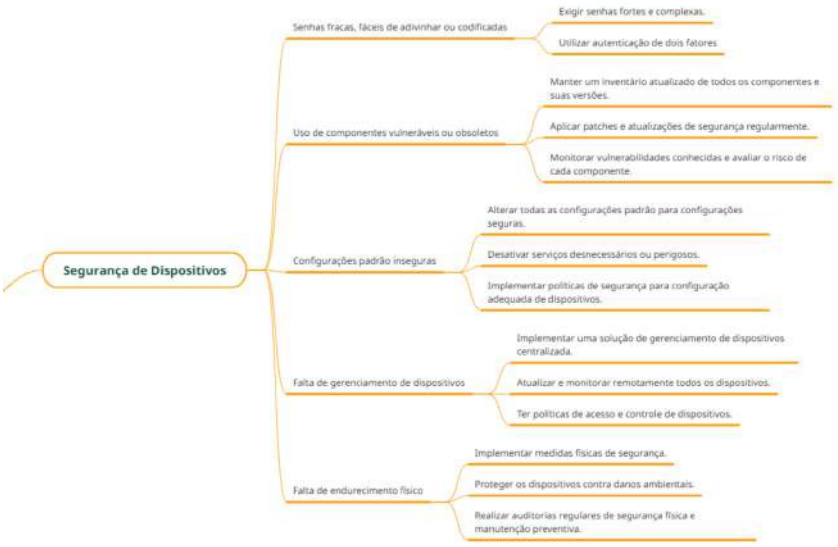


Figura 6: Segurança de Dispositivos, **Fonte:** Autor

- Senhas fracas, fáceis de adivinhar ou codificadas: Nesta categoria, o foco está na fragilidade das senhas utilizadas nos dispositivos. Para mitigar esse problema, é recomendado:
    - Exigir senhas fortes e complexas: Incentivar o uso de senhas que combinem letras maiúsculas e minúsculas, números e caracteres especiais.

    - Utilizar autenticação de dois fatores: Implementar um segundo fator de autenticação, como um código enviado por mensagem de texto ou um aplicativo de autenticação, para aumentar a segurança das contas.
- Uso de componentes vulneráveis ou obsoletos: Aqui, a atenção se volta para os componentes utilizados nos dispositivos, que podem conter falhas de segurança. Para abordar essa questão, é importante:
    - Manter um inventário atualizado de todos os componentes e suas versões: Ter um registro completo dos componentes utilizados e suas respectivas versões facilita o controle e a aplicação de atualizações.
    - Aplicar *patches* e atualizações de segurança regularmente: Manter os dispositivos atualizados com as correções de segurança mais recentes reduz as vulnerabilidades.
    - Monitorar vulnerabilidades conhecidas e avaliar o risco de cada componente: Acompanhar informações sobre vulnerabilidades e avaliar a criticidade de cada uma em relação aos componentes utilizados auxilia na priorização das atualizações.
- Configurações padrão inseguras: Nesta categoria, destaca-se a importância de modificar as configurações padrão dos dispositivos, que muitas vezes são inseguras. As medidas a serem tomadas incluem:
    - Alterar todas as configurações padrão para configurações seguras: Configurar dispositivos de acordo com as melhores práticas de segurança, alterando senhas padrão, desabilitando serviços desnecessários, etc.
    - Desativar serviços desnecessários ou perigosos: Identificar e desabilitar serviços ou funcionalidades que não são utilizados ou representam riscos à segurança.
    - Implementar políticas de segurança para configuração adequada de dispositivos: Definir diretrizes claras sobre a configuração segura dos dispositivos e garantir que sejam seguidas.
- Falta de gerenciamento de dispositivos: Aqui, o foco é a falta de controle e monitoramento dos dispositivos utilizados. Para abordar essa questão, é recomendado:
    - Implementar uma solução de gerenciamento de dispositivos centralizada: Utilizar uma plataforma centralizada que permita o gerenciamento e monitoramento de todos os dispositivos.
    - Atualizar e monitorar remotamente todos os dispositivos: Garantir que todos os dispositivos estejam com as versões atualizadas de *firmware* e *software*, além de monitorar atividades suspeitas.
    - Ter políticas de acesso e controle de dispositivos: Estabelecer políticas claras de acesso aos dispositivos, definir permissões e restrições de uso, e realizar auditorias periódicas para verificar a conformidade.
- Falta de endurecimento físico: Nesta categoria, a segurança física dos dispositivos é destacada, visando protegê-los contra danos ambientais e acesso não autorizado. As medidas a serem adotadas incluem:
    - Implementar medidas físicas de segurança: Utilizar fechaduras, gabinetes seguros e outros dispositivos de segurança física para proteger os dispositivos.

- Proteger os dispositivos contra danos ambientais: Garantir que os dispositivos estejam protegidos contra condições adversas, como umidade, calor excessivo, poeira, etc.
- Realizar auditorias regulares de segurança física e manutenção preventiva: Verificar periodicamente as condições físicas dos dispositivos, identificar e corrigir possíveis problemas de segurança, e realizar manutenção preventiva para evitar falhas.

5.3.2. Segurança de redes

Em relação à segurança das redes, a Figura 7 abaixo ilustra uma série de vulnerabilidades associadas a ecossistemas com interfaces inseguras. Essas vulnerabilidades incluem a falta de criptografia nas comunicações, falhas na autenticação e autorização, falta de controle de acesso à rede, falta de monitoramento de rede e detecção de intrusões e vazamento de dados e ataques de *spoofing*.

Figura 7: Segurança de Rede, **Fonte:** Autor

- Falta de criptografia nas comunicações: Nesta categoria, destaca-se a importância da criptografia para proteger as comunicações realizadas em uma rede. Para abordar essa questão, são recomendadas as seguintes medidas:
  - Utilizar protocolos de criptografia robustos: Implementar protocolos como SSL/TLS para garantir a segurança das informações transmitidas.
  - Implementar o uso de certificados digitais e chaves seguras para autenticação: Utilizar certificados digitais confiáveis e chaves criptográficas robustas para autenticar os participantes da comunicação.
- Falhas na autenticação e autorização: Nesta categoria, a atenção se volta para a autenticação e autorização dos usuários na rede. Para lidar com essa questão, são sugeridas as seguintes ações:

    - Utilizar controle de acesso baseado em função (RBAC): Atribuir permissões de acesso com base nas funções e responsabilidades de cada usuário, garantindo que eles tenham apenas as autorizações necessárias.
- Falta de controle de acesso à rede: Aqui, o foco está no controle de acesso à rede, com o objetivo de evitar acessos não autorizados. As medidas para abordar essa questão incluem:
    - Implementar *firewalls* e sistemas de detecção e prevenção de intrusões (IDS/IPS): Utilizar essas soluções para monitorar e controlar o tráfego de rede, identificando e bloqueando atividades suspeitas.
    - Segmentar a rede em zonas de confiança: Dividir a rede em segmentos isolados para restringir o acesso a recursos críticos apenas aos usuários autorizados.
    - Utilizar VLANs e VPNs para criar conexões seguras: Utilizar VLANs para separar e isolar tráfegos específicos, e implementar VPNs para estabelecer conexões seguras entre redes remotas.
- Falta de monitoramento de rede e detecção de intrusões: Nesta categoria, destaca-se a importância de monitorar a rede e detectar atividades intrusivas. Para abordar essa questão, é recomendado:
    - Implementar sistemas de monitoramento de rede em tempo real: Utilizar ferramentas de monitoramento que permitam identificar atividades suspeitas e reagir a possíveis ameaças.
    - Utilizar sistemas de detecção de intrusões (IDS) e sistemas de prevenção de intrusões (IPS): Implementar essas soluções para identificar e bloquear atividades maliciosas ou anômalas na rede.
- Realizar análise de logs e eventos: Monitorar registros e eventos de rede para identificar padrões suspeitos ou tentativas de intrusão.
- Vazamento de dados e ataques de *spoofing*: Aqui, o foco está na proteção contra vazamento de dados e ataques de *spoofing*. As medidas para abordar essa questão incluem:
    - Implementar medidas de proteção contra vazamento de dados: Utilizar técnicas de criptografia para proteger os dados em repouso e em trânsito, garantindo que somente os destinatários autorizados possam acessá-los.
    - Utilizar mecanismos de autenticação robustos: Implementar métodos de autenticação seguros, como autenticação de dois fatores (2FA), para prevenir ataques de *spoofing*, onde um atacante se passa por outra entidade.

5.3.3. Segurança de infraestrutura

Em relação à segurança de infraestrutura, a Figura 8 abaixo ilustra uma série de vulnerabilidades associadas a ecossistemas com interfaces inseguras. Essas vulnerabilidades incluem a proteção insuficiente contra desastres naturais e ataques físicos e vandalismo.

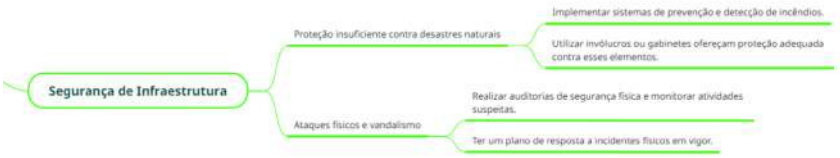


Figura 8: Segurança de Infraestrutura, **Fonte:** Autor

- Proteção insuficiente contra desastres naturais: Nesta categoria, destaca-se a importância de proteger a infraestrutura contra desastres naturais, como incêndios, inundações ou terremotos. Para abordar essa questão, são recomendadas as seguintes medidas:
    - Implementar sistemas de prevenção e detecção de incêndios: Utilizar equipamentos e sistemas, como detectores de fumaça, sprinklers ou sistemas de supressão de incêndio, para prevenir e detectar incêndios precocemente.
    - Utilizar invólucros ou gabinetes que ofereçam proteção adequada contra esses elementos: Garantir que os equipamentos e sistemas críticos estejam protegidos em gabinetes ou invólucros resistentes a desastres naturais, como caixas à prova de água, resistência a temperaturas extremas, etc.
- Ataques físicos e vandalismo: Nesta categoria, o foco está na proteção da infraestrutura contra ataques físicos, incluindo vandalismo ou invasões não autorizadas. Para abordar essa questão, são sugeridas as seguintes ações:
    - Realizar auditorias de segurança física e monitorar atividades suspeitas: Realizar avaliações regulares da segurança física da infraestrutura, identificar vulnerabilidades e monitorar atividades suspeitas, como tentativas de acesso não autorizado.
    - Ter um plano de resposta a incidentes físicos em vigor: Desenvolver e implementar um plano de resposta a incidentes físicos, que inclua procedimentos de emergência, contato com as autoridades competentes e medidas para minimizar danos e proteger a infraestrutura.

5.3.4. Segurança de interfaces

Em relação à segurança das interfaces, a Figura 9 abaixo ilustra uma série de vulnerabilidades associadas a ecossistemas com interfaces inseguras. Essas vulnerabilidades incluem a falta de mecanismos seguros de atualização, proteção insuficiente da privacidade e transferência ou armazenamento inseguro de dados.

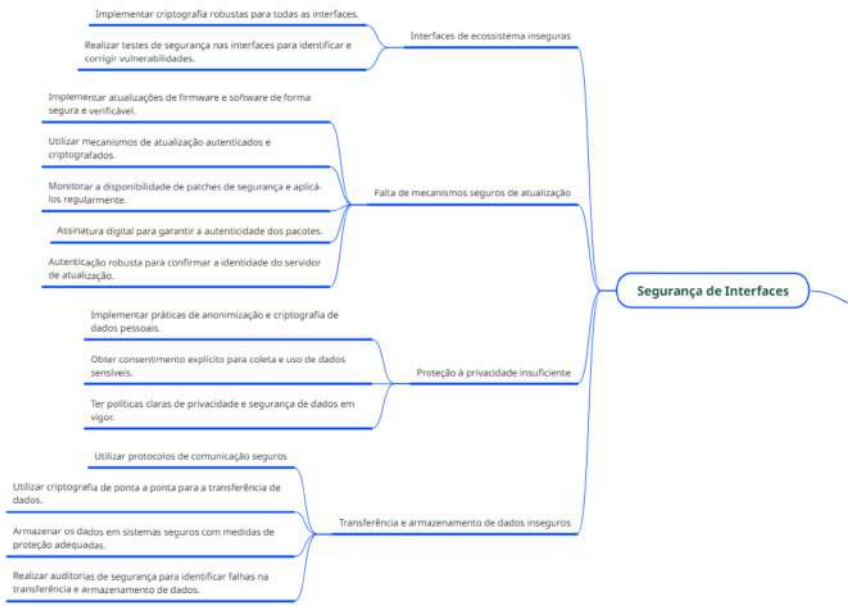


Figura 9: Segurança de Interfaces, **Fonte:** Autor

- Interfaces de ecossistema inseguras: Nesta categoria, destaca-se a importância de garantir a segurança das interfaces do ecossistema. As medidas sugeridas incluem:
    - Implementar criptografia robusta para todas as interfaces: Utilizar algoritmos de criptografia robustos para proteger as comunicações e dados transmitidos pelas interfaces.
    - Realizar testes de segurança nas interfaces: Realizar testes regulares de segurança para identificar e corrigir vulnerabilidades presentes nas interfaces do ecossistema.
- Falta de mecanismos seguros de atualização: Aqui, o foco está nos mecanismos de atualização de *firmware* e *software*. Para abordar essa questão, são recomendadas as seguintes medidas:
    - Implementar atualizações de forma segura e verificável: Garantir que as atualizações de *firmware* e software sejam aplicadas de forma segura e que sua autenticidade possa ser verificada.
    - Utilizar mecanismos de atualização autenticados e criptografados: Empregar métodos de atualização que utilizem assinatura digital, criptografia e autenticação robusta para garantir a integridade e autenticidade dos pacotes de atualização.
    - Monitorar a disponibilidade de *patches* de segurança e aplicá-los regularmente: Manter-se atualizado sobre os patches de segurança disponíveis e aplicá-los regularmente para corrigir vulnerabilidades conhecidas.
- Proteção à privacidade insuficiente: Nesta categoria, a preocupação é com a proteção da privacidade dos dados. As medidas sugeridas incluem:
    - Implementar práticas de anonimização e criptografia de dados pessoais: Utilizar técnicas de anonimização e criptografia para proteger dados pessoais contra acesso não autorizado.

    - Obter consentimento explícito para coleta e uso de dados sensíveis: Garantir que o consentimento explícito seja obtido antes da coleta e uso de dados sensíveis.
    - Ter políticas claras de privacidade e segurança de dados: Estabelecer diretrizes que descrevem como os dados são coletados, usados, armazenados e protegidos, em conformidade com as leis e regulamentações aplicáveis.
- Transferência e armazenamento de dados inseguros: Nesta categoria, o foco está na segurança durante a transferência e armazenamento de dados. As medidas sugeridas incluem:
    - Utilizar protocolos de comunicação seguros: Utilizar protocolos criptografados, como HTTPS, para garantir a segurança da transferência de dados pela rede.
    - Utilizar criptografia de ponta a ponta para a transferência de dados: Criptografar os dados de ponta a ponta para proteger sua confidencialidade durante a transferência.
    - Armazenar os dados em sistemas seguros com medidas de proteção adequadas: Utilizar sistemas de armazenamento seguros e implementar medidas de proteção, como controle de acesso e criptografia, para garantir a segurança dos dados em repouso.
    - Realizar auditorias de segurança: Realizar auditorias regulares de segurança para identificar possíveis falhas na transferência e armazenamento de dados e tomar medidas corretivas necessárias.

5.3.5. Segurança de dados

Em relação à segurança dos dados, a Figura 10 abaixo ilustra uma série de vulnerabilidades associadas a ecossistemas com interfaces inseguras. Essas vulnerabilidades incluem a falta de proteção adequada dos dados, falta de *backups* e recuperação de dados, violação da privacidade dos dados e acesso não autorizado aos dados.

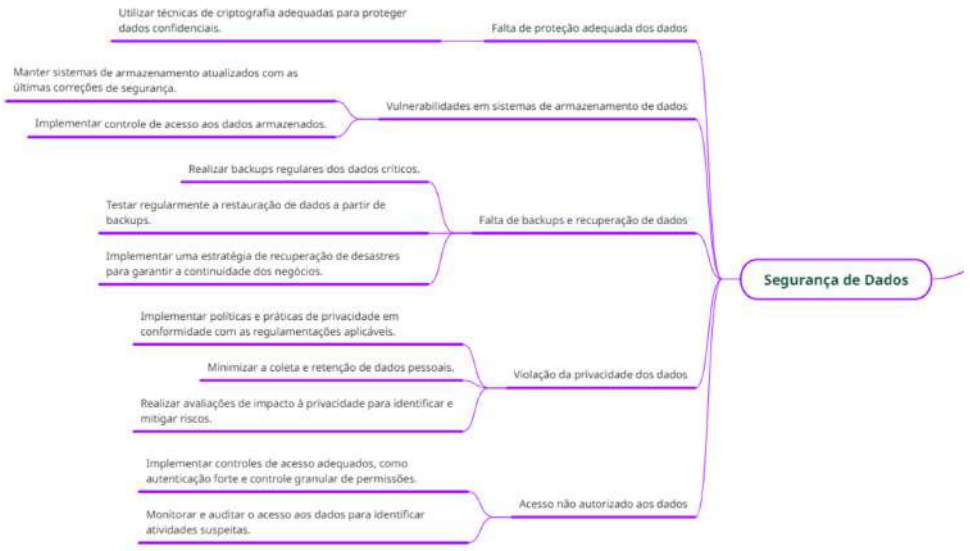


Figura 10: Segurança de Dados, **Fonte:** Autor

- Falta de proteção adequada dos dados: Nesta categoria, destaca-se a importância de proteger os dados confidenciais por meio de técnicas de criptografia adequadas. As medidas sugeridas incluem:
    - Utilizar técnicas de criptografía adequadas: Aplicar algoritmos de criptografia robustos para proteger os dados em trânsito e em repouso, garantindo que apenas usuários autorizados possam acessá-los.
    - Vulnerabilidades em sistemas de armazenamento de dados: Aqui, o foco está nas vulnerabilidades presentes nos sistemas de armazenamento de dados. Para abordar essa questão, são recomendadas as seguintes medidas.
    - Manter sistemas de armazenamento atualizados com as últimas correções de segurança: Aplicar regularmente *patches* e atualizações de segurança para corrigir vulnerabilidades conhecidas.
    - Implementar controle de acesso aos dados armazenados: Utilizar mecanismos de controle de acesso para garantir que apenas usuários autorizados possam acessar os dados armazenados.
- Falta de *backups* e recuperação de dados: Nesta categoria, destaca-se a importância de ter estratégias adequadas de *backup* e recuperação de dados. As medidas sugeridas incluem:
    - Realizar *backups* regulares dos dados críticos: Fazer cópias de segurança periódicas dos dados importantes para garantir a disponibilidade e a recuperação em caso de perda.
    - Testar regularmente a restauração de dados a partir de *backups*: Verificar se os *backups* estão funcionando corretamente e se os dados podem ser recuperados com sucesso.
    - Implementar uma estratégia de recuperação de desastres: Desenvolver e implementar um plano de recuperação de desastres que estabeleça procedimentos para a continuidade dos negócios em caso de falhas ou incidentes graves.
- Violação da privacidade dos dados: Nesta categoria, a atenção se volta para a proteção da privacidade dos dados, especialmente em conformidade com as regulamentações aplicáveis. Para abordar essa questão, são sugeridas as seguintes ações:
    - Implementar políticas e práticas de privacidade em conformidade com as regulamentações: Garantir que as políticas e práticas de privacidade estejam em conformidade com as leis e regulamentações de proteção de dados aplicáveis.
    - Minimizar a coleta e retenção de dados pessoais: Coletar apenas os dados pessoais necessários e estabelecer prazos adequados para a retenção desses dados.
    - Realizar avaliações de impacto à privacidade: Avaliar e mitigar os riscos à privacidade dos dados por meio de análises regulares e identificação de possíveis brechas de segurança.
- Acesso não autorizado aos dados: Nesta categoria, destaca-se a importância de implementar controles de acesso adequados para evitar acessos não autorizados aos dados. As medidas sugeridas incluem:

- Implementar controles de acesso adequados, como autenticação forte e controle granular de permissões: Utilizar métodos robustos de autenticação, como autenticação de dois fatores (2FA), e atribuir permissões de acesso baseadas em funções para garantir que somente usuários autorizados possam acessar os dados.
- Monitorar e auditar o acesso aos dados: Registrar e analisar atividades de acesso aos dados para identificar comportamentos suspeitos ou violações de segurança.

É importante ressaltar que existe um inter-relacionamento entre essas vulnerabilidades, o que significa que cada uma delas pode afetar diretamente ou indiretamente mais de um aspecto de segurança. Para obter uma visão mais abrangente e completa dessa taxonomia, recomenda-se a análise do apêndice A presente neste trabalho.

5.4. CONSEQUÊNCIAS DA FALTA DE SEGURANÇA EM DISPOSITIVOS IOT

A rápida evolução da tecnologia trouxe consigo uma infinidade de dispositivos conectados à Internet das Coisas (IoT) para nossas residências, oferecendo maior conveniência e controle sobre nossos ambientes domésticos. No entanto, à medida que nos encantamos com a comodidade desses dispositivos inteligentes, muitas vezes negligenciamos a importância de implementar medidas de segurança adequadas para proteger nossas informações pessoais e nossos lares.

A SonicWall, líder em soluções de segurança cibernética, divulgou em fevereiro de 2023 seu relatório semestral sobre ataques cibernéticos[20]. O estudo constatou que o ano de 2022 foi o segundo com maior número de tentativas de ataques de *ransomware* registradas globalmente. Entre as descobertas alarmantes, foi destacado que o Brasil ocupou a quarta posição como um dos principais alvos desse tipo de ataque em todo o mundo, ficando atrás apenas dos Estados Unidos, Reino Unido e Espanha (Gráfico 2). Com a rápida digitalização da economia brasileira, muitas vezes não há a devida atenção às práticas de segurança digital, o que acarreta na elevação da vulnerabilidade de pessoas e empresas a diversos tipos de ataques [48].

[20] Link: https://www.sonicwall.com/pt-br/2023-cyber-threat-report/

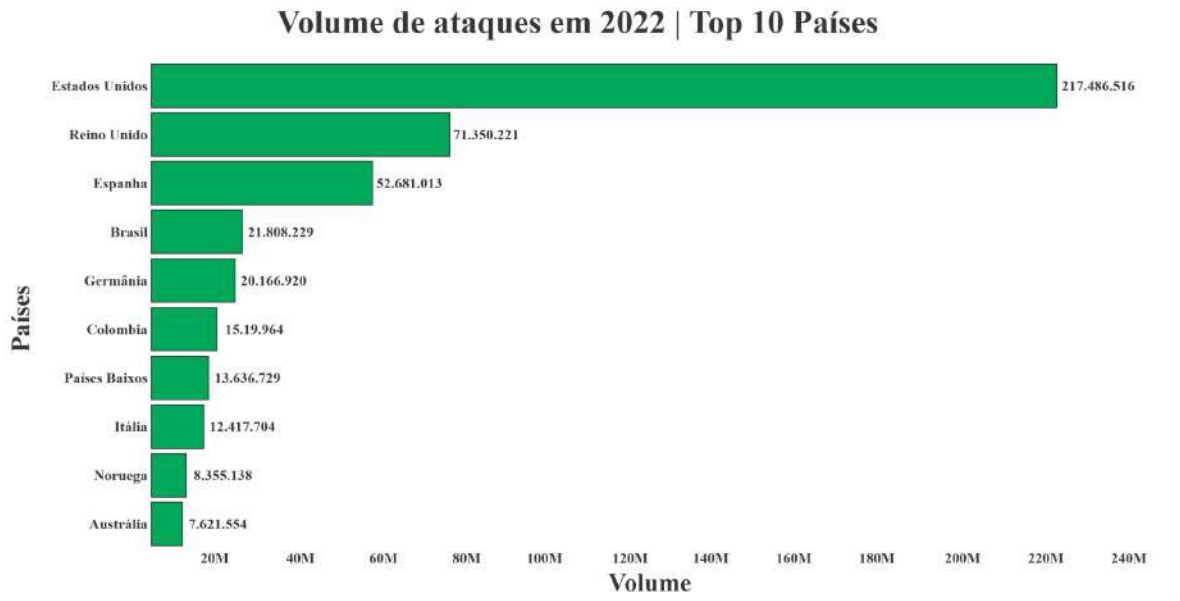


Gráfico 2: Volume de ataques em 2022, **Fonte:** sonicwall (2023)

Arley Brogiato, Diretor da SonicWall América Latina e Caribe, destacou que esses resultados reforçam a necessidade de que as organizações do Brasil se mantenham vigilantes em relação às ameaças cibernéticas que estão em constante evolução, já que os cibercriminosos estão cada vez mais sofisticados e encontrando novas formas criativas de atacar empresas e residências [48].

Podemos ver um exemplo recente disso, assim como foi relatado pela Better Business Bureau (BBB), uma organização sem fins lucrativos que atua como intermediária entre empresas e consumidores nos Estados Unidos, Canadá e México. Em fevereiro de 2023, a BBB emitiu um alerta sobre *hackers* que comprometem sistemas de *smart TVs* para aplicar golpes. Os usuários ao tentarem acessar um serviço de *streaming* em suas *smart TVs* são surpreendidos por *pop-ups* de erro que solicitam informações de cartão de crédito para o pagamento de supostas taxas de ativação ou números de telefone para contato com o suporte. Em um dos casos citados pela BBB, um cidadão americano afirmou ter sido instruído a adquirir US $300 em vales da loja da Xbox em troca de uma suposta proteção contra invasões em suas contas [49].

Outro exemplo relevante é um caso publicado em uma coluna do Tecmundo em 2018. A notícia descreve uma situação em que uma mulher dos Estados Unidos enfrentava um fenômeno conhecido como "abuso tecnológico". Ela residia em uma casa totalmente conectada, equipada com um sistema inteligente de automação que controlava lâmpadas, aquecimento, cortinas, sistema de som e câmeras de segurança. Infelizmente, seu ex-marido utilizava essa tecnologia para vigiá-la, monitorá-la e intimidá-la constantemente. De acordo com o relato, ocorriam diversas vezes durante a noite situações desconfortáveis, nas quais ela e seus cachorros eram acordados abruptamente por músicas altas, luzes piscando e televisores ligando e desligando incessantemente. Essa invasão dos sistemas inteligentes perturbava sua privacidade e causava um impacto negativo em sua vida diária [50].

Já aqui no Brasil, em 2020, a Polícia Federal (PF) conduziu uma investigação que revelou um preocupante caso de invasão de câmeras IP por cibercriminosos em mais de 35 municípios. Aproveitando-se do período de isolamento imposto pela pandemia de Covid-19, os *hackers* invadiram essas câmeras para obter registros da rotina dos moradores. Em seguida, os criminosos lucraram vendendo pacotes de imagens e vídeos na *dark web* ou utilizavam o material obtido para extorsão. Essa ação criminosa demonstra como os *hackers* se aproveitam das vulnerabilidades de sistemas de vigilância para invadir a privacidade das pessoas e cometer crimes online. A invasão das câmeras IP não apenas viola a segurança dos indivíduos, mas também alimenta um mercado negro de informações pessoais sensíveis [51].

Essas estatísticas e incidentes apenas ressaltam a importância crucial de implementar medidas de proteção robustas em dispositivos IoT, a fim de preservar a privacidade e a segurança dos usuários e evitar que esses dispositivos sejam utilizados em ataques cibernéticos. É fundamental que tanto as autoridades quanto os usuários estejam plenamente conscientes da segurança cibernética, adotando medidas preventivas para proteger seus dispositivos conectados à Internet e garantir a privacidade de suas vidas diárias.

6. AMEAÇAS À VALIDADE

Este capítulo tem como objetivo abordar as ameaças à validade do presente estudo, considerando a revisão bibliográfica qualitativa realizada sobre os principais dispositivos IoT em residências, bem como a identificação e catalogação das ameaças e riscos associados a esses dispositivos. Para garantir uma abordagem robusta e confiável, foram utilizadas as diretrizes da OWASP (*Open Web Application Security Project*) e da NIST (*National Institute of Standards and Technology*) como referência.

Validade interna. Uma possível ameaça à validade interna está relacionada à seleção dos artigos e documentos utilizados na revisão bibliográfica. Embora tenha sido empregada uma abordagem abrangente de busca visando a identificação do maior número possível de trabalhos, é possível que alguns estudos relevantes tenham sido omitidos. Além disso, as limitações inerentes aos estudos originais podem afetar a confiabilidade dos resultados obtidos na revisão.

Outra ameaça à validade interna diz respeito à análise e interpretação dos dados encontrados nos artigos. Com o intuito de minimizar o viés introduzido pela subjetividade na categorização das ameaças e riscos, foram estabelecidos critérios claros e objetivos de classificação. Esses critérios foram definidos com base nas diretrizes da OWASP e da NIST, fornecendo uma base sólida e confiável para a análise.

Para mitigar essas ameaças, foram adotadas estratégias específicas. A seleção das fontes seguiu critérios pré-estabelecidos, tais como a relevância do conteúdo, a atualidade e a reputação dos autores e periódicos. Esses critérios garantiram a inclusão de estudos relevantes e confiáveis na revisão bibliográfica

Validade externa. Esse tipo de ameaça está relacionada à possibilidade de generalizar os resultados obtidos neste estudo para outros contextos e populações. No entanto, é importante ressaltar que a generalização dos resultados está limitada ao escopo da revisão bibliográfica realizada, que se concentrou nos principais dispositivos IoT em residências.

Ao interpretar os resultados deste estudo, é crucial considerar as características específicas dos dispositivos IoT em residências abordados nesta pesquisa, reconhecendo que os resultados podem não ser diretamente aplicáveis a outros contextos ou diferentes populações. As conclusões deste estudo devem ser interpretadas levando em conta o contexto e as particularidades dos dispositivos IoT em residências.

Além disso, é fundamental ter em mente a rápida evolução da tecnologia IoT. Consequentemente, os resultados obtidos nesta pesquisa podem se tornar parcialmente obsoletos com o tempo, à medida que novos dispositivos e ameaças surgem. Portanto, é recomendável que futuras atualizações e revisões sejam realizadas para acompanhar o avanço tecnológico e fornecer uma visão mais abrangente e atualizada das ameaças e riscos associados aos dispositivos IoT em residências.

Dessa forma, a validade externa deste estudo é condicionada às características específicas do escopo da revisão bibliográfica e às limitações impostas pela evolução

contínua da tecnologia IoT. A compreensão adequada dessas restrições contribui para uma interpretação precisa e contextualizada dos resultados obtidos.

Validade de construção. Essa ameaça relaciona-se com a adequação das medidas e instrumentos utilizados na revisão bibliográfica para capturar de forma precisa as ameaças e riscos aos dispositivos IoT em residências. A utilização de referências como as diretrizes da OWASP e da NIST permitiu uma abordagem sistemática na identificação e categorização dessas ameaças, fornecendo um arcabouço confiável para a análise.

No entanto, é importante reconhecer que diferentes pesquisadores podem ter interpretações e classificações ligeiramente diferentes das ameaças. Embora tenham sido estabelecidos critérios claros para a categorização, é possível que algum grau de subjetividade tenha influenciado as escolhas realizadas.

Para mitigar essa ameaça à validade de construção, foram adotadas medidas específicas. Durante a revisão bibliográfica, os critérios de categorização foram aplicados de forma consistente e sistemática.

Validade de mensuração. A validade de mensuração aborda a qualidade dos dados coletados e a forma como eles foram analisados. Neste estudo, os dados foram coletados a partir da revisão bibliográfica, utilizando-se fontes confiáveis e reconhecidas. No entanto, é importante reconhecer que os dados encontrados nos artigos e documentos podem conter limitações e vieses inerentes aos estudos originais.

A análise dos dados foi realizada de forma sistemática e consistente, seguindo os critérios de categorização estabelecidos. No entanto, a subjetividade na interpretação dos resultados pode ter influenciado a análise e introduzido algum grau de viés na conclusão das ameaças e riscos identificados.

Para mitigar essa ameaça à validade de mensuração, foram adotadas medidas específicas. Durante a análise dos dados, foi buscada uma abordagem objetiva, garantindo a consistência na aplicação dos critérios de categorização, estabelecidos com base nas diretrizes da OWASP e da NIST.

Validade de conclusão. Esse tipo de ameaça é fundamental para garantir uma interpretação correta dos resultados e conclusões obtidas no estudo. No presente estudo, as conclusões foram embasadas na revisão bibliográfica sistemática e nas diretrizes da OWASP e da NIST, proporcionando uma base sólida para a análise das ameaças e riscos aos dispositivos IoT em residências.

É importante salientar, no entanto, que as conclusões apresentadas são resultado de uma síntese e interpretação dos estudos revisados, o que pode permitir interpretações divergentes por parte de outros pesquisadores. Portanto, é necessário considerar diferentes perspectivas e abordagens ao analisar e interpretar as conclusões deste estudo.

Além disso, é relevante destacar que a análise das ameaças e riscos aos dispositivos IoT em residências não abrange especificamente as medidas de mitigação ou soluções para

esses problemas. Essa é uma área de pesquisa complementar que pode oferecer *insights* valiosos para a implementação de estratégias de segurança e proteção. Portanto, futuros estudos podem se concentrar nesse aspecto, a fim de fornecer uma visão mais abrangente e prática sobre a segurança dos dispositivos IoT em residências.

7. CONSIDERAÇÕES FINAIS

Este estudo teve como objetivo investigar as ameaças e riscos associados aos dispositivos IoT em ambientes residenciais, com o intuito de ampliar a conscientização sobre a segurança nesse contexto cada vez mais conectado. Durante a pesquisa, foram analisados diversos aspectos relacionados à segurança dos dispositivos IoT, incluindo vulnerabilidades, potenciais ataques e medidas de proteção.

Para a aplicação de dispositivos IoT em ambientes residenciais, foram identificadas oito categorias de dispositivos, juntamente com exemplos práticos de uso baseados em literatura relevante. Essas categorias incluem assistentes de voz, câmeras de segurança, termostatos inteligentes, fechaduras inteligentes, lâmpadas inteligentes, plugues inteligentes, sensores de ambiente e eletrodomésticos inteligentes.

Os resultados revelaram uma variedade de ameaças enfrentadas pelos dispositivos IoT em ambientes residenciais, bem como suas consequências. Foi identificado que a falta de atualizações de segurança e senhas fracas são fatores-chave que podem levar a invasões e comprometimento da privacidade dos usuários. Além disso, destaca-se a importância crucial de proteger a rede doméstica, o roteador e os dispositivos individuais por meio de autenticação robusta, criptografia de dados e segmentação de rede.

É importante ressaltar que este estudo apresenta algumas limitações. A pesquisa foi baseada em artigos e documentos existentes, o que pode restringir a generalização dos resultados para outros contextos. Além disso, devido à rápida evolução da tecnologia IoT, o cenário está em constante mudança, tornando necessária uma vigilância contínua e atualização constante das práticas de segurança.

Diante dessas limitações, recomenda-se que estudos futuros possam expandir a amostra para incluir uma maior diversidade de dispositivos e ambientes residenciais, considerando diferentes perfis de usuários. Além disso, é fundamental investigar soluções técnicas avançadas, como a aplicação de inteligência artificial e aprendizado de máquina para detecção e prevenção de ameaças em tempo real.

Em suma, a segurança dos dispositivos IoT em ambientes residenciais é uma preocupação crescente. Este estudo destaca a importância de adotar medidas de proteção adequadas para mitigar as ameaças e riscos enfrentados. Os usuários devem estar cientes das melhores práticas de segurança, mantendo seus dispositivos e redes atualizados regularmente, além de utilizar senhas fortes e criptografia de dados.

Espera-se que este trabalho contribua para a conscientização e compreensão dos desafios de segurança enfrentados pelos dispositivos IoT em ambientes residenciais. Acredita-se que a pesquisa contínua nessa área seja essencial para garantir um futuro mais seguro e confiável para a Internet das Coisas em nossas casas.

REFERÊNCIAS

[1] COELHO, Pedro. Internet das Coisas-Introdução Prática. **FCA-Editora de Informática, Lda**, 2017.

[2] SINGER, Talyta. Tudo conectado: conceitos e representações da internet das coisas. **Simpósio em tecnologias digitais e sociabilidade**, v. 2, p. 1-15, 2012.

[3] ASHTON, Kevin et al. That 'internet of things' thing. **RFID journal**, v. 22, n. 7, p. 97-114, 2009.

[4] DEORAS, Sritshi. First ever IoT device-"The internet Toaster"[online].[cit. 2. 8. 2017]. **Dostupné z: http://iotindiamag. com/2016/08/first-ever-iot-device-the-internet-toaster**.

[5] WEISER, Mark. The computer for the 21st century. **ACM SIGMOBILE mobile computing and communications review**, v. 3, n. 3, p. 3-11, 1999.

[6] DIAS, Renata Rampim de Freitas; PERIN, E. Internet das coisas sem mistérios: uma nova inteligência para os negócios. **Renata Rampim de Freitas Dias.: São Paulo Netpress Books**, 2016.

[7] NABAZTAG. nabaztag.com. Disponível em: https://www.nabaztag.com/#. Acesso em: 13 mar. 2023.

[8] Internet of Things. International Conference for Industry and Academia March 26-28, 2008 / Zurich. 2008. Disponível em: http://www.the-internet-of-things.org/iot2008/. Acesso em: 13 mar. 2023.

[9] Commission European. Contribute to law-making. Disponível em: https://commission.europa.eu/law/contribute-law-making_en?form=IoTGovernance. Acesso em: 13 mar. 2023.

[10] IoT London. Open Internet of Things Definition. 2012. Disponível em: https://iot.london/open-internet-of-things-definition/. Acesso em: 13 mar. 2023.

[11] LUETH, Knud Lasse. State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time. IoT Analytics, 2020. Disponível em: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/. Acesso em: 23 de mar. 2023

[12] FÓRUM BRASILEIRO DE IOT. Disponível em: https://iotbrasil.org.br/. Acesso em: 23 de mar. 2023.

[13] ABINC. Sobre a ABINC. Disponível em: https://abinc.org.br/sobre/. Acesso em: 23 de março de 2023.

[14] BNDES. Plano Nacional de Internet das Coisas. 2017. Disponível em: https://www.bndes.gov.br/wps/portal/site/home/conhecimento/pesquisaedados/estudos/estudo

-internet-das-coisas-iot/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil. Acesso em: 23 de mar.2023.

[15] GOV.br. A Anatel retira barreiras regulatórias à Internet das Coisas e aplicações Máquina-a-Máquina. 2020. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-retira-barreiras-regulatorias-a-internet-das-coisas-e-aplicacoes-maquina-a-maquina. Acesso em: 23 de mar. 2023.

[16] HALVORSEN, Hans-petter et al. Case Studies in IoT -Smart-Home Solutions Pedagogical Perspective with Industrial Applications and some latest Developments. In: EAEEIE ANNUAL CONFERENCE, 27., 2017, Grenoble, France. HAL. Grenoble, França: Hal, 2017. v. 1, p. 1 - 9. Disponível em: https://hal.archives-ouvertes.fr/hal-01658856. Acesso em: 23 de mar. 2023.

[17] HENDRICKS, Drew. The history of smart homes. **IoT Evolution World**, 2014.

[18] SOMFY. A QUICK HISTORY OF HOME AUTOMATION. 2018. Disponível em: https://www.somfy.com.au/discover-somfy/blog/post/a-quick-history-of-home-automation. Acesso em: 05 de abril de 2023.

[19] Techtudo. “Termostato inteligente ajuda a manter a temperatura que você desejar”. 2011. Disponível em: https://www.techtudo.com.br/noticias/2011/10/termostato-inteligente-ajuda-manter-temperatura-que-voce-desejar.ghtml.

[20] ECOMPLY.io, Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://lgpd-brasil.info/. Acesso em: 24 de março de 2023.

[21] ECOMPLY.io, Artigo 55-J Competências ANPD - Autoridade Nacional de Proteção de Dados. Disponível em: https://lgpd-brasil.info/capitulo_09/artigo_55j. Acesso em: 24 de março de 2023.

[22] ZIMMECK, Sebastian. Privacy and Security in the Internet of Things (IoT): Strategies for Intermediaries. Information Systems Frontiers, [S.l.], v. 20, n. 2, p. 205-218, abr. 2018.

[23] ALAWAIS, Arwa. A Survey of IoT Authentication and Authorization Techniques. IEEE Internet of Things Journal, [S.l.], v. 5, n. 5, p. 4204-4226, out. 2018.

[24] HUANG, Xin; KULASEKERA, Kanchana Thilini; GAMAGE, Danushka Tharaka. Security and Privacy in Internet of Things (IoT): A Survey. Journal of Network and Computer Applications, [S.l.], v. 126, p. 198-213, jul. 2019.

[25] AHMED, Sajid; YANG, Xin-She; ABDULLAH, Abdul Hanan; KHALID, Safyan; ALBESHRI, Ali. IoT Security: Review, Blockchain Solutions, and Open Challenges. Future Generation Computer Systems, [S.l.], v. 82, p. 395-411, abr. 2018.

[26] AURISIDE. Automação Residencial - Riscos e Oportunidades. Disponível em: http://www.aureside.org.br/noticias/automacao-residencial---riscos-e-oportunidades. Acesso em: 24 maio 2023.

[27] Business Insider. The Future of IoT: Business Insider Intelligence Report. Disponível em: https://www.onectus.com/post/the-future-of-iot-business-insider-intelligence-report. Acesso em: 24 maio 2023.

[28] BLOKDYK, G. IoT Architecture: A Complete Guide. Brendale: 5STARCooks, 2020.

[29] SILVA, Kim Gesswein. **Assistentes de voz presentes em alto-falantes inteligentes: uma análise exploratória sobre os tópicos de pesquisa e as possibilidades de uso**. 2019. Dissertação de Mestrado. Pontifícia Universidade Católica do Rio Grande do Sul.

[30] QUADROS, Thiago de. **Sistema de vigilância inteligente com câmeras IP sem fio**. 2013. Trabalho de Conclusão de Curso. Universidade Tecnológica Federal do Paraná.

[31] ABASCAL GUTIÉRREZ, Verónica et al. Modelización energética de vivienda como estudio de la viabilidad en la instalación de un termostato inteligente. 2018.

[32] GROSSMANN, Gustavo Henrique. IoT Smart Lock (ISL): sistema de fechadura inteligente, utilizando protocolos de Internet das Coisas. 2018.

[33] KOSOUSKI, Felipe. Smart lighting: solução para controle de lâmpadas em smart homes. 2018. Trabalho de Conclusão de Curso. Universidade Tecnológica Federal do Paraná.

[34] LING, Zhen e cols. Vulnerabilidades de segurança da internet das coisas: um estudo de caso do sistema smart plug. IEEE Internet of Things Journal , v. 4, n. 6, pág. 1899-1909, 2017.

[35] FREITAS, Marla Souza et al. SENSORES INTELIGENTES E SUAS APLICAÇÕES NO COTIDIANO. Revista de Trabalhos Acadêmicos UNIVERSO, v. 1, p. 2179, 2016.

[36] MALCHE, Timothy; MAHESHWARY, Priti. Internet das Coisas (IoT) para a construção de sistemas domésticos inteligentes. In: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) . IEEE, 2017. pág. 65-70.

[37] Forescout. The Riskiest Connected Devices in Enterprise Networks, out. 2022. Disponível em: https://www.forescout.com/blog/the-riskiest-connected-devices-in-enterprise-networks/. Acesso em: 13 maio 2023

[38] Appsealing. Guide to OWASP IoT Top 10 For Proactive Security, 2021 .Disponível em: https://www.appsealing.com/owasp-iot-top-10/. Acesso em: 13 maio 2023.

[39] OWASP. Internet of Things. Disponível em: https://owasp.org/www-project-internet-of-things/. Acesso em: 12 maio 2023.

[40] ROCCIA, Rubens Douglas. Usuários respeitam as normas de criação de senhas seguras? Uma análise de datasets de senhas vazadas. 2021.

[41] KISSELL, Joe. **Aprendendo a proteger suas senhas**. Novatec Editora, 2018.

[42] ROSA, João Pedro Gomes. **Mecanismos de Segurança IoT**. 2021. Tese de Doutorado.

[43] BARCENA, Mario Ballano; WUEEST, Candid. Insecurity in the Internet of Things. **Security response, symantec**, v. 20, 2015.

[44] HAYASHI, Victor Takashi; ALMEIDA, Felipe Valencia. Visão Geral da Pesquisa Brasileira em Segurança para IoT. **Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação**, v. 4, n. 1, 2022.

[45] MACHADO JUNIOR, Dorival Moreira et al. Segurança da informação: uma abordagem sobre proteção da privacidade em internet das coisas. 2018.

[46] PAUFERRO, Gabriel Brogno Alcantara; DE PAIVA, Seila Vasti Faria; LESSA, Nayari Marie. IoT: conceitos de segurança de dados e criptografia. **Revista Cogitare**, v. 3, n. 2, p. 40-52, 2020.

[47] BOECKL, Katie et al. Considerações para Gerenciar Riscos de Privacidade e Segurança Cibernética na Internet das Coisas (IoT). 2019.

[48] SonicWall, 2023 cyber threat report, fev. 2023 Disponível em: https://www.sonicwall.com/pt-br/2023-cyber-threat-report/. Acesso em: 9 maio 2023.

[49] Better Business Bureau. BBB Scam Alert: Scammers may be targeting your smart TV , fev. 2023. Disponível em: https://www.bbb.org/article/scams/28221-bbb-scam-alert-scammers-may-be-target-your-smart-tv. Acesso em: 9 maio 2023.

[50] Payão, Felipe. Tecmundo: Homem usou IoT para stalkear a própria mulher dentro de casa, nov. 2018. Disponível em: https://www.tecmundo.com.br/seguranca/135925-homem-usou-iot-stalkear-propria-mulher-dentro-casa.htm. Acesso em: 11 maio 2023.

[51] PEDROSO, Ana Luiza. Mundo Conectado: Câmeras de segurança e babás eletrônicas são invadidas por hackers no Brasil, abr. 2020. Disponível em: https://mundoconectado.com.br/noticias/v/13135/cameras-de-seguranca-e-babas-eletronicas-sao-invadidas-por-hackers-no-brasil. Acesso em: 11 maio 2023.

[52] NIST. NIST Special Publication 800-63B. 2017. Disponível em: https://pages.nist.gov/800-63-3/sp800-63b.html. Acesso em: 27 maio 2023

[53] LEITE, Leandro Rogério Corrêa. Internet das Coisas (IoT): vulnerabilidades de segurança e desafios. 2019.

[54] PATIL, Apoorva Shripad et al. Security and Privacy Issues in the Internet of Things. In: **Information Security Practices for the Internet of Things, 5G, and Next-Generation Wireless Networks**. IGI Global, 2022. p. 70-91.

[55] KAUR, Jaideep; KAUR, Kamaljit. Internet of Things: A Review on Technologies, Architecture, Challenges, Applications, Future Trends. **International Journal of Computer Network & Information Security**, v. 9, n. 4, 2017.

[56] ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The internet of things: A survey. **Computer networks**, v. 54, n. 15, p. 2787-2805, 2010.

[57] AL-FUQAHA, Ala et al. Internet of things: A survey on enabling technologies, protocols, and applications. **IEEE communications surveys & tutorials**, v. 17, n. 4, p. 2347-2376, 2015.

[58] ABDALLA, Peshraw Ahmed; VAROL, Cihan. Testando a segurança da IoT: o estudo de caso de uma câmera IP. In: **2020 8º Simpósio Internacional de Forense Digital e Segurança (ISDFS)** . IEEE, 2020. pág. 1-5.

[59] TASTAN, Mehmet. Internet of things based smart energy management for smart home. **KSII Transactions on Internet and Information Systems (TIIS)**, v. 13, n. 6, p. 2781-2798, 2019.

[60] ALURI, Diamond Celestine. Smart lock systems: An overview. **International Journal of Computer Applications**, v. 177, n. 37, p. 40-43, 2020.

[61] PANDHARIPANDE, Ashish; CAICEDO, David. Smart indoor lighting systems with luminaire-based sensing: A review of lighting control approaches. **Energy and Buildings**, v. 104, p. 369-377, 2015.

[62] DONG, Bing et al. A review of smart building sensing system for better indoor environment control. **Energy and Buildings**, v. 199, p. 29-46, 2019.

[63] REESE, Ken et al. A usability study of five two-factor authentication methods. In: **Proceedings of the Fifteenth Symposium on Usable Privacy and Security**. 2019.

[64] RUFINO, Nelson Murilo de O. **Segurança em redes sem fio: aprenda a proteger suas informações em ambientes wi-fi e bluetooth**. Novatec Editora, 2019.

[65] BUNGART, José Wagner. **Redes de computadores: Fundamentos e protocolos**. Editora SESI-Serviço Social da Indústria, 2017.

[66] SÁNDOR, Hunor; SEBESTYÉN-PÁL, Gheorghe. Projeto de segurança ideal na Internet das Coisas. In: **2017 5º Simpósio Internacional de Forense e Segurança Digital (ISDFS)** . IEEE, 2017. pág. 1-6.

[67] YANG, Yuchen et al. A survey on security and privacy issues in Internet-of-Things. **IEEE Internet of things Journal**, v. 4, n. 5, p. 1250-1258, 2017.

[68] GUBBI, Jayavardhana et al. Internet of Things (IoT): A vision, architectural elements, and future directions. **Future generation computer systems**, v. 29, n. 7, p. 1645-1660, 2013.

[69] ALABA, Fadele Ayotunde et al. Internet of Things security: A survey. **Journal of Network and Computer Applications**, v. 88, p. 10-28, 2017.

[70] PERUMAL, Thinagaran; DATTA, Soumya Kanti; BONET, Cristiano. Estrutura de gerenciamento de dispositivos IoT para cenários domésticos inteligentes. In: **2015 IEEE 4ª Conferência Global de Eletrônicos de Consumo (GCCE)** . IEEE, 2015. pág. 54-55.

[71] ABDULLAH, Aishah et al. CyberSecurity: a review of internet of things (IoT) security issues, challenges and techniques. In: **2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)**. IEEE, 2019. p. 1-6.

[72] LEITE, Cristiano Monteiro. Políticas de segurança física e lógica em ambientes institucionais que utilizam tecnologia da informação. 2011.

[73] Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Ur, B., Vidas, T., ... & Cranor, L. F. (2011). Of passwords and people: measuring the effect of password-composition policies. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2595-2604).

[74] BARROS, Emerson de. Estudo de vulnerabilidades em dispositivos IoT TCP/IP. 2021.

GLOSSÁRIO

Ameaça: Uma ameaça é uma entidade ou evento potencialmente danoso que tem a capacidade de explorar uma vulnerabilidade existente em um sistema ou ambiente.

Ataque: É uma ação intencional de uma ameaça ou atacante para comprometer a segurança de um sistema, rede ou organização.

Ataques de negação de serviço (DoS): Um tipo de ataque cibernético no qual um único dispositivo envia uma quantidade excessiva de solicitações legítimas a um serviço, sistema ou rede com o objetivo de sobrecarregá-lo e torná-lo inacessível a usuários legítimos.

Ataques de negação de serviço distribuído (DDoS): Um tipo de ataque cibernético em que vários dispositivos distribuídos, geralmente comprometidos ou controlados remotamente, enviam um grande volume de tráfego simultaneamente para um serviço, sistema ou rede, com o objetivo de sobrecarregá-lo e torná-lo inacessível.

Backup: Cópia de segurança de dados ou informações para protegê-los contra perda ou corrupção.

***Bluetooth*:** Um padrão de comunicação sem fio que permite a troca de dados entre dispositivos próximos, como *smartphones*, *tablets* e fones de ouvido, sem a necessidade de cabos.

***Bots*:** Programas de computador automatizados que executam tarefas específicas, muitas vezes de forma repetitiva, geralmente associados a atividades maliciosas na Internet.

Cibercriminosos: Indivíduos que usam a tecnologia da informação para cometer crimes, como roubo de informações, fraude ou vandalismo digital.

Códigos PIN (*Personal Identification Number*): Combinações numéricas usadas como senhas ou códigos de acesso pessoais para autenticação em dispositivos eletrônicos ou serviços.

Criptografia: O processo de transformação de informações para torná-las ilegíveis para qualquer pessoa que não possua a chave de decodificação. É amplamente utilizado para proteger a privacidade e a segurança das comunicações digitais.

***Dark web*:** Uma parte da *World Wide Web* que não é acessível por meio de navegadores convencionais e requer software específico para ser acessada. É frequentemente associada a atividades ilegais e anônimas.

Engenharia social: Técnica usada para manipular ou enganar pessoas a fim de obter informações confidenciais ou acesso não autorizado a sistemas.

Exploração: Refere-se ao ato de aproveitar uma vulnerabilidade em um sistema ou software para obter acesso não autorizado, causar danos, roubar informações ou comprometer a integridade do sistema.

***Firewalls*:** *Software* ou *hardware* que controla o tráfego de rede, filtrando e bloqueando o acesso não autorizado a um sistema ou rede, enquanto permite a comunicação segura.

***Firmware*:** Um *software* embutido em um dispositivo eletrônico que fornece instruções para o funcionamento e controle do *hardware*.

Hacker: Pessoa com habilidades técnicas avançadas que usa seu conhecimento em computação para explorar sistemas de computadores ou redes, geralmente com intenções maliciosas.

***Hardware*:** Refere-se a todos os componentes físicos de um computador ou dispositivo eletrônico, como processadores, memória, placas-mãe, discos rígidos, teclados, monitores, entre outros.

***Insights*:** Descobertas ou percepções valiosas obtidas a partir da análise de dados ou informações.

Inteligência Artificial: Campo da ciência da computação que desenvolve sistemas capazes de realizar tarefas que normalmente exigiriam inteligência humana.

Interfaces: Pontos de interação entre um usuário e um sistema, como telas, menus ou dispositivos de entrada.

Internet: Uma rede global de computadores interconectados que permite a comunicação e o compartilhamento de informações em todo o mundo.

***Malware*:** Um termo geral que se refere a *software* malicioso, projetado para infiltrar-se em um sistema de computador e danificar, roubar informações ou obter acesso não autorizado.

***Man-in-the-middle*:** Ataque em que um terceiro intercepta e manipula a comunicação entre duas partes, sem o conhecimento delas.

Mitigação: é o processo de reduzir a probabilidade ou o impacto de uma ameaça explorar uma vulnerabilidade.

***Patches*:** Atualizações de software projetadas para corrigir falhas de segurança ou resolver outros problemas em sistemas ou aplicativos.

***Phishing*:** Prática de enviar mensagens falsas ou fraudulentas, geralmente por e-mail, fingindo ser de uma fonte confiável para obter informações pessoais ou financeiras dos destinatários.

***Pop-ups*:** Janelas ou caixas de diálogo que aparecem inesperadamente na tela de um dispositivo, geralmente contendo anúncios ou solicitações indesejadas.

***Pretexting*:** Técnica de manipulação em que um indivíduo cria um cenário falso ou pretextos para obter informações ou acesso não autorizado.

Protocolos: Conjuntos de regras e convenções que governam a comunicação entre dispositivos em uma rede. Eles definem como os dados são formatados, transmitidos, recebidos e interpretados.

***Radio-Frequency Identification* (RFID):** Uma tecnologia de identificação automática que usa sinais de rádio para ler e armazenar informações em etiquetas eletrônicas, permitindo a identificação de objetos ou animais.

***Ransomware*:** Um tipo de *malware* que criptografa os arquivos de um sistema infectado e exige um resgate para restaurar o acesso aos dados.

Risco: Refere-se à probabilidade de uma ameaça explorar uma vulnerabilidade específica, resultando em danos ou consequências indesejadas. O risco é uma combinação da probabilidade de ocorrência de uma ameaça e do impacto potencial caso ela ocorra. O gerenciamento de riscos envolve a identificação, avaliação e mitigação de riscos para proteger ativos e garantir a segurança.

***Smartphones*:** Telefones celulares avançados que oferecem recursos adicionais além de fazer chamadas, como acesso à Internet, aplicativos, câmeras e reprodução de mídia.

***Spoofing*:** refere-se a uma técnica utilizada na segurança da informação, onde um indivíduo ou um programa malicioso tenta falsificar ou mascarar sua identidade ou a origem de uma comunicação.

***Software*:** Conjunto de programas, instruções e dados que controlam o funcionamento de um computador ou dispositivo eletrônico. Exemplos incluem sistemas operacionais, aplicativos e jogos.

***Streaming*:** A transmissão contínua de áudio ou vídeo pela *Internet*, permitindo que o conteúdo seja reproduzido instantaneamente, em vez de ser baixado e armazenado antes de ser reproduzido.

Tablets: Dispositivos eletrônicos portáteis que apresentam uma tela sensível ao toque e são usados principalmente para navegar na Internet, assistir a vídeos, ler livros eletrônicos e executar aplicativos.

VLANs: É uma técnica de segmentação de redes que permite a criação de grupos lógicos de dispositivos em uma rede local. Esses grupos lógicos podem ser formados por dispositivos de diferentes locais físicos, mas eles se comunicam entre si como se estivessem conectados a um único *switch* físico.

VPNs (Redes Privadas Virtuais): Redes privadas que usam uma conexão criptografada para permitir que os usuários acessem a Internet de forma segura e anônima, como se estivessem conectados a partir de um local diferente do real.

Vulnerabilidade: Refere-se a uma fraqueza ou falha em um sistema, processo, *software* ou dispositivo que pode ser explorado por uma ameaça para causar danos ou comprometer a

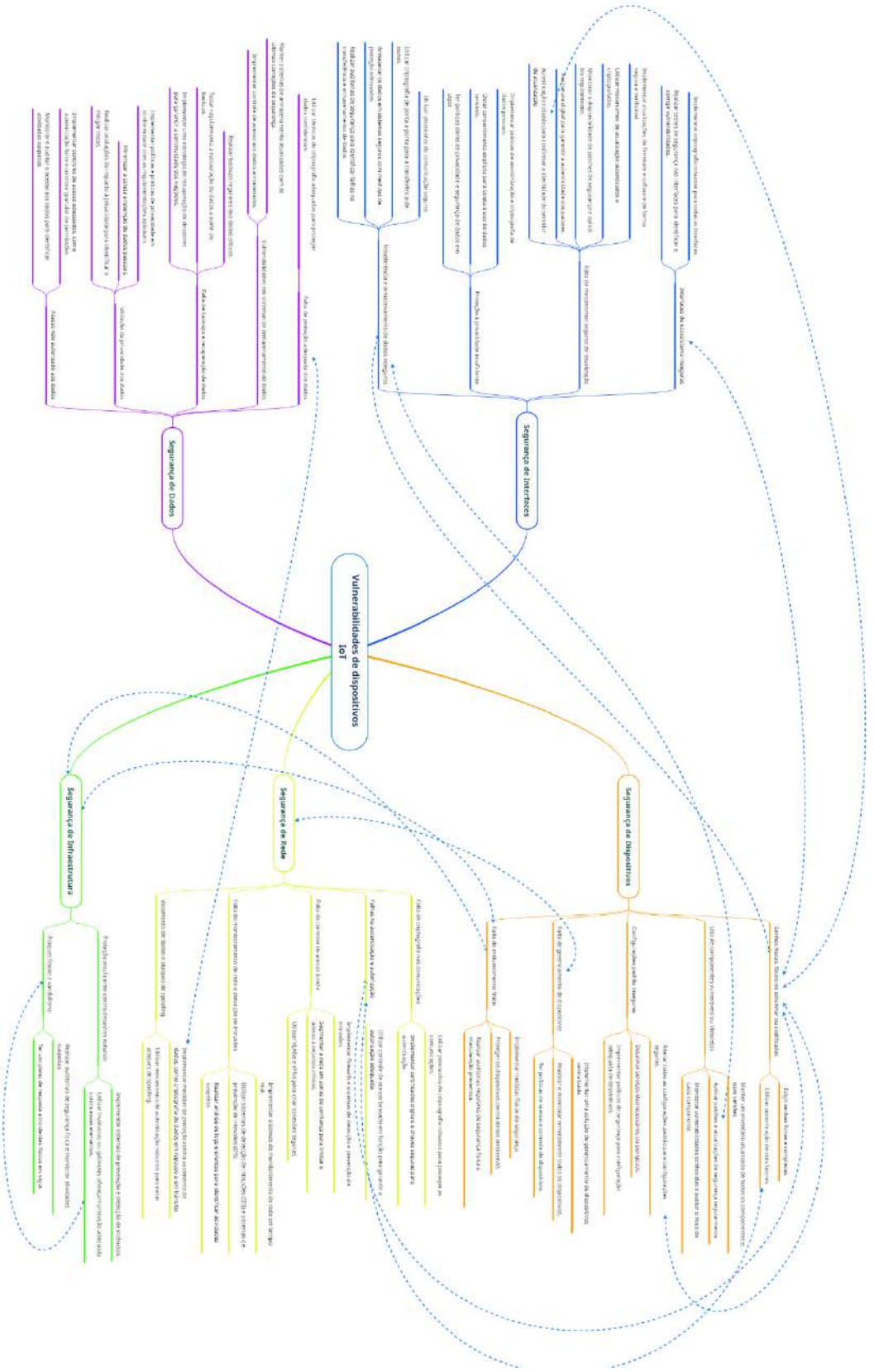
segurança. As vulnerabilidades podem ser causadas por erros de programação, configurações inadequadas, falta de atualizações de segurança, entre outros fatores.

***Wi-Fi*:** Uma tecnologia sem fio que permite a conexão de dispositivos eletrônicos a uma rede local de Internet, geralmente por meio de um roteador.

***World Wide Web*:** Também conhecida como *Web* ou WWW, é um sistema de informação global baseado em hipertexto que permite o acesso a documentos e recursos vinculados por meio de navegadores da web.

***Zigbee*:** Um padrão de comunicação sem fio de baixo consumo de energia usado principalmente para automação residencial e industrial.

APÊNDICE A - TAXONOMIA DE VULNERABILIDADES A DISPOSITIVOS IOT



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
Campus Campina Grande
R. Tranqüilino Coelho Lemos, 671, Dinamérica, CEP 58432-300, Campina Grande (PB)
CNPJ: 10.783.898/0003-37 - Telefone: (83) 2102.6200

Documento Digitalizado Restrito

Entrega do TCC

Assunto: Entrega do TCC
Assinado por: Guilherme Vidal
Tipo do Documento: Anexo
Situação: Finalizado
Nível de Acesso: Restrito
Hipótese Legal: Direito Autoral (Art. 24, III, da Lei no 9.610/1998)
Tipo do Conferência: Cópia Simples

Documento assinado eletronicamente por:

- **Guilherme Vidal de Negreiros Lima**, **ALUNO (201811210030) DE TECNOLOGIA EM TELEMÁTICA - CAMPINA GRANDE**, em 03/08/2023 20:07:12.

Este documento foi armazenado no SUAP em 03/08/2023. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 896187
Código de Autenticação: 0a50eeff3e