INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS FLORIANO
CURSO TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

GUILHERME FRANCISCO DIAS DE ARAUJO DUARTE DAMASCENO

DESAFIOS NA APLICAÇÃO DE TECNOLOGIAS IOT EM RESIDÊNCIAS: UMA ANÁLISE SOBRE OS ATRIBUTOS DA SEGURANÇA DA INFORMAÇÃO

FLORIANO
2022

GUILHERME FRANCISCO DIAS DE ARAUJO DUARTE DAMASCENO

DESAFIOS NA APLICAÇÃO DE TECNOLOGIAS IOT EM RESIDÊNCIAS: UMA ANÁLISE SOBRE OS ATRIBUTOS DA SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso (artigo científico) apresentado como exigência parcial para obtenção do diploma do Curso de Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Floriano.

Orientador: Prof. Me. Silvino Marques da Silva Júnior.

FLORIANO
2022

DESAFIOS NA APLICAÇÃO DE TECNOLOGIAS IOT EM RESIDÊNCIAS: UMA ANÁLISE SOBRE OS ATRIBUTOS DA SEGURANÇA DA INFORMAÇÃO

Guilherme Francisco Dias de Araujo Duarte Damasceno[1]
Silvino Marques da Silva Júnior[2]

RESUMO

A Internet das Coisas tem se consolidado com sua acelerada expansão no cenário atual das tecnologias contemporâneas. Entender quais são as vulnerabilidades e as suas formas de prevenção/solução são de grande relevância social por abranger questões em torno da Segurança da Informação individuais e coletivas. O presente trabalho tem como objetivo identificar quais os riscos e precauções no uso de tecnologias de Internet das Coisas a nível residencial, apresentá-la no cenário das tecnologias atuais, além de abordar os principais aspectos que envolvem a Segurança da Informação a esse tema. Inicialmente é realizada a seleção de livros, documentos e artigos que contribuem para a fundamentação teórica do trabalho. Os artigos foram retirados das bases de dados *Springer Link*, *Science Direct* e *IEEE Xplore*. A partir das informações obtidas, foi realizada a aplicação de um questionário com alunos dos cursos de tecnologia da informação do Instituto Federal do Piauí - Campus Floriano. Alcançando, como resultado do levantamento desses dados, a identificação das vulnerabilidades e suas soluções nas tecnologias de Internet das Coisas residencial. Ao final, o trabalho contribui para auxiliar na transmissão de um tema presente na sociedade atualmente, atuando no conhecimento e na compreensão das boas práticas que incluem a Segurança da Informação na Internet das Coisas a nível residencial.
Palavras-chave: internet das coisas; segurança da informação; casas inteligentes; privacidade; tecnologia.

ABSTRACT

The Internet of Things has been consolidated with its accelerated expansion in the current scenario of contemporary technologies. Understanding what are the vulnerabilities and their ways of prevention/solution are of great social relevance as they cover issues around individual and collective Information Security. The present study aims to identify the risks and precautions in the use of Internet of Things technologies at a residential level, present it in the scenario of current technologies, in addition to addressing the main aspects that involve Information Security in this topic. Initially, the selection of books, documents and articles that contribute to the theoretical foundation of the study is carried out. The articles were taken from the Springer Link, Science Direct and IEEE Xplore databases. From the information obtained, a questionnaire was applied to students of information technology courses at the Federal Institute of Piauí - Floriano Campus. Achieving, as a result of this data collection, the identification of vulnerabilities and their solutions in residential Internet of Things technologies was identified. In the end, the study contributes to assist in the transmission of a theme present in society today, acting in the knowledge and understanding of good practices that include Information Security in the Internet of Things at a residential level.
Keywords: internet of things; information security; smart homes; privacy; technologies.

Data de aprovação: 11/01/2023 (data de apresentação do TCC)

---

[1] Graduando do curso Tecnologia em Análise e Desenvolvimento de Sistemas. Instituto Federal do Piauí - Campus Floriano. E-mail: caflo.2020114tads23@aluno.ifpi.edu.br.
[2] Professor Mestre do Instituto Federal do Piauí - Campus Floriano. Instituto Federal do Piauí - Campus Floriano. Email: silvinomarques@ifpi.edu.br.

1 INTRODUÇÃO

A internet nos traz diversas aplicações e soluções para o mundo moderno, sendo usada para praticamente qualquer tarefa realizada no trabalho, escolas ou em casa. Segundo Kurose e Ross (2021, p.26) "a Internet pode ser vista como uma infraestrutura que fornece serviços a aplicações distribuídas que são executadas nos sistemas finais".

O aumento da utilização da Internet das Coisas, do inglês *Internet of Things* (IoT), é uma realidade nos tempos atuais com a grande disseminação de aparelhos como os relógios inteligentes, assistentes virtuais, TVs inteligentes, além de casas e carros automatizados. Segundo a Lueth (2018), estima-se que o mercado global de gastos do usuário final de tecnologias IoT atinja a marca de US $1.567 bilhão até 2025, considerando a aceleração do mercado para IoT.

O desenvolvimento e ampliação desse ecossistema de IoT traz grandes benefícios para as pessoas na automação de situações diárias. São exemplos de aplicações a contagem dos passos em uma corrida, a troca de músicas na TV, a escolha da cor das lâmpadas e até mesmo a regulação de câmeras e sensores de segurança. Porém, com tantas vantagens, a tecnologia traz consigo as suas desvantagens. No caso da Internet das Coisas, o seu principal ponto de discussão é em torno da sua segurança da informação.

Segundo a empresa de seguranca Kaspersky (2021), no primeiro semestre de 2021 foram observados 1,5 bilhão de ataques à *honeypots* (ambientes propositalmente abertos à ataques para ser feito uma análise de comportamento dos atacantes), revelando um aumento mais que duplicado em comparação com a pesquisa feita em 2020 que quase atingiu a marca de 650 milhões de ataques (DAWS, 2021).

Dan Demeter (2021), consultor de segurança da Kaspersky, afirma que desde que os dispositivos IoT se tornaram essenciais no dia a dia, os criminosos virtuais mudaram o foco de atenção para essa área. Também é notável que desde que os usuários se interessaram por esses dispositivos inteligentes os ataques cresceram e muitas pessoas não se acham importantes o suficiente para serem atacadas, e esse é um dos motivos que a maioria dos ataques seriam evitáveis (DAWS, 2021).

Por ser uma tecnologia ainda em fase de crescimento, consideravelmente nova e com uma expansão notável dos dispositivos de IoT e que estão conectados a internet, a segurança dessa rede tende a diminuir, pois o número de prováveis alvos crescem (BERLANDA, 2021).

Um outro ponto importante nas tecnologias IoT é que com o uso da comunicação sem fio, há algumas vulnerabilidades que já são conhecidas desse tipo de tecnologias e que passam a ser agravadas pelas dificuldades no uso de criptografias robustas, o que pode comprometer algumas propriedades da Segurança da Informação (SI) (LEITE, 2019).

Um dos casos de ataques hackers explorando as vulnerabilidades da Internet das Coisas é o do *malware* Mirai. Esse malware tem como objetivo infectar dispositivos inteligentes, em grande proporção os dispositivos IoT, os transformando em uma bots para a criação de uma *botnet* que servirá para fazer ataques distribuído de negação de serviço (DDoS), sobrecarregando os serviços e os tornando indisponíveis. Um dos serviços vítima do Mirai foi a Dyn, uma empresa que controla uma grande parte dos sistemas de nomes de domínio (DNS) da Internet. Esse ataque ocorreu no formato de DDoS, afetando diversos sites, como o Twitter, The Guardian, Netflix, e entre outros na Europa e Estados Unidos (WOOLF, 2016).

Observa-se que a temática apresentada possui relevância na sociedade por envolver uma tecnologia recente e com acelerado crescimento, englobando, principalmente, as questões em torno da segurança da informação individual e coletiva. Portanto, é relevante pesquisar: Quais são os riscos e precauções mais discutidos no uso de tecnologia de Internet das Coisas a nível residencial?

Deste modo, este estudo tem o objetivo de identificar quais os riscos e precauções no uso de tecnologias IoT em residências, por meio de seus atributos de segurança da informação. Dessa maneira, busca-se apresentar a Internet das Coisas no cenário da tecnologia nos dias atuais, identificar os seus principais aspectos que envolvem a Segurança da Informação, além de estimar as principais vulnerabilidades e suas formas de prevenção da Segurança da Informação aplicadas a Internet das Coisas em residências.

Esse estudo justifica-se pela relevância do assunto, considerando a alta demanda da tecnologia, a sua grande disponibilidade e pelo crescimento da estrutura recaindo sobre as residências, o que torna a Internet das Coisas um alvo dos hackers na internet atual. Esse é um ponto que deve ser abordado para disseminação de conhecimento prévio sobre as possíveis vulnerabilidades, ataques sofridos e formas de garantir a segurança da informação no escopo residencial.

O presente artigo ainda conta, além desta introdução, com outras 4 seções. Na sequência há a revisão teórica do assunto que aborda os principais conceitos de Internet das Coisas, a sua segurança e suas vulnerabilidades e formas de prevenção, ademais, aprofunda-se no assunto de Internet das Coisas a nível residencial. Na etapa seguinte é descrita a metodologia utilizada para a execução do presente trabalho. Após essa etapa, é apresentado os resultados e sua discussão obtidos na pesquisa de campo e nos trabalhos pesquisados. Por fim, é feita a conclusão deste artigo científico.

2 REVISÃO TEÓRICA

Esta seção descreve o estado da arte das principais questões que envolvem o tema de Internet das Coisas (IoT) residencial, sendo eles a definição de IoT, a identificação dos seus principais aspectos, o mapeamento das suas brechas e vulnerabilidades, além de formas de prevenção baseados em aspectos da segurança da informação.

2.1 APRESENTAÇÃO DE INTERNET DAS COISAS

Ao decorrer dos primeiros 40 anos, a Internet tem sido utilizada especialmente na função de conectar as pessoas pelo uso de e-mails, fóruns e, gradualmente, por meio dos sites de redes sociais, onde há a defesa de, cada vez mais, a visão de dados abertos ligados. Também é notável que atualmente a Internet tem sido utilizada para fazer a conexão de dispositivos, máquinas e outros objetos, pelas redes com e sem fio, criando uma nova disposição tecnológica chamada de *Internet of Things* (DUTTON, 2014).

A definição de Internet das Coisas, fugindo da pura semântica, é uma expressão que se referencia diretamente ao crescimento da comunicação entre as máquinas usando a internet (comumente chamado de *M2M*, do inglês *machine-to-machine*, que já ultrapassou o número de comunicação entre as pessoas via internet), o amadurecimento de variados utensílios, como geladeiras e torradeiras inteligentes, além de micro dispositivos, como sensores que, podem ser distribuídos de diversas formas para obter informações a partir de seu ambiente, os tornando constituidores da internet (MAGRANI, 2018).

Em poucas palavras a Internet das Coisas, não é nada mais que um prolongamento da Internet atual, que permite aos objetos diários, mas com capacidade de comunicação computacional, se conectarem à Internet. Essa conexão com a rede globalizada de computadores viabiliza, em primeiro momento, controlar os objetos de forma remota e, segundamente, possibilitar que esses próprios objetos consigam ser acessados como provedores de serviços. (SANTOS *et al*., 2016).

Essas novas capacidades, de objetos considerados normais, garantem uma ampliação de oportunidades nos ambientes acadêmicos e industriais. Porém com estas possibilidades também se manifestam os riscos com desafios tanto técnicos, quanto sociais. (SANTOS *et al*., 2016).

O entendimento em definição sobre o que é IoT está em que elas se focalizam em como os computadores, sensores e objetos trocam interações entre si e processam as informações e dados em um contexto de hiperconectividade (MAGRANI, 2018).

A princípio, o termo de hiperconectividade foi utilizado para retratar o estado de disponibilidade que os indivíduos têm para se comunicar em qualquer momento. Atualmente, o termo em questão está ligado às comunicações entre pessoas, entre pessoas e máquinas e entre as máquinas, usando diferentes meios de comunicação, assim, observa-se que há um fluxo constante de informações e uma larga produção de dados (MAGRANI, 2018).

No contexto de internet das coisas, é relevante evidenciar que uma “coisa” será um aparelho com um sensor, esse que coleta os dados e que pode ser conectado a uma rede de comunicações, como em empresa, residências, indústrias ou até mesmo diretamente à internet de forma física, como em cabos de rede ou fibra. Com isso, será possível ter essa “coisa” ligado por redes Wi-Fi, LTE, 4G, 5G, Bluetooth, RFID, comunicações rádio, etc (RIBEIRO, 2020).

Nessa composição, utilizando-se dos objetos inteligentes será possível detectar, controlar e viabilizar troca de informações entre eles, além de, acessar a serviços da Internet e interagir com as pessoas Dessa maneira, uma série de novas oportunidades de finalidades surgem, como nas cidades inteligentes (Smart Cities), na saúde (Healthcare), nas casas

inteligentes (Smart Home) e com elas afloram os desafios da tecnologia como nas regulamentações, padronizações e segurança (SANTOS et al., 2016).

O auxílio no dia-a-dia das pessoas é um dos pontos de grande valia da tecnologia de Internet das Coisas. Uma noção proeminente das tecnologias IoT visa melhorar a qualidade de vida na modernidade, como por exemplo, a melhoria das rotinas de pessoas idosas e com deficiência, os ajudando em sua autonomia e autoconfiança. Além disso, há dispositivos IoT que podem servir na implantação de sensores em fábricas para o monitoramento de poluição ambiental e vazamento de produtos químicos (NESHENKO *et al*., 2019).

Efetivamente a noção das tecnologias de IoT está incorporando soluções significativas para interações contemporâneas, seja no bem-estar ou na segurança. Nesse contexto, existem diversos esforços contínuos de IoT que garantem transformar a vida moderna e os modelos de negócios, aprimorando a eficiência, o nível dos serviços e a satisfação dos clientes (NESHENKO *et al*., 2019).

2.2 SEGURANÇA DA INFORMAÇÃO EM IOT

A Segurança da Informação (SI) é obtida pela implementação de uma mescla moldada de controles, que incluem políticas, processos, procedimentos, estruturas organizacionais e as funções tanto de software quanto de hardware. Um dos pontos de partida para a compreensão dessa área se dá em seus conceitos de confidencialidade, integridade e disponibilidade que é comumente chamada de tríade CID (HINTZBERGEN *et al*., 2018).

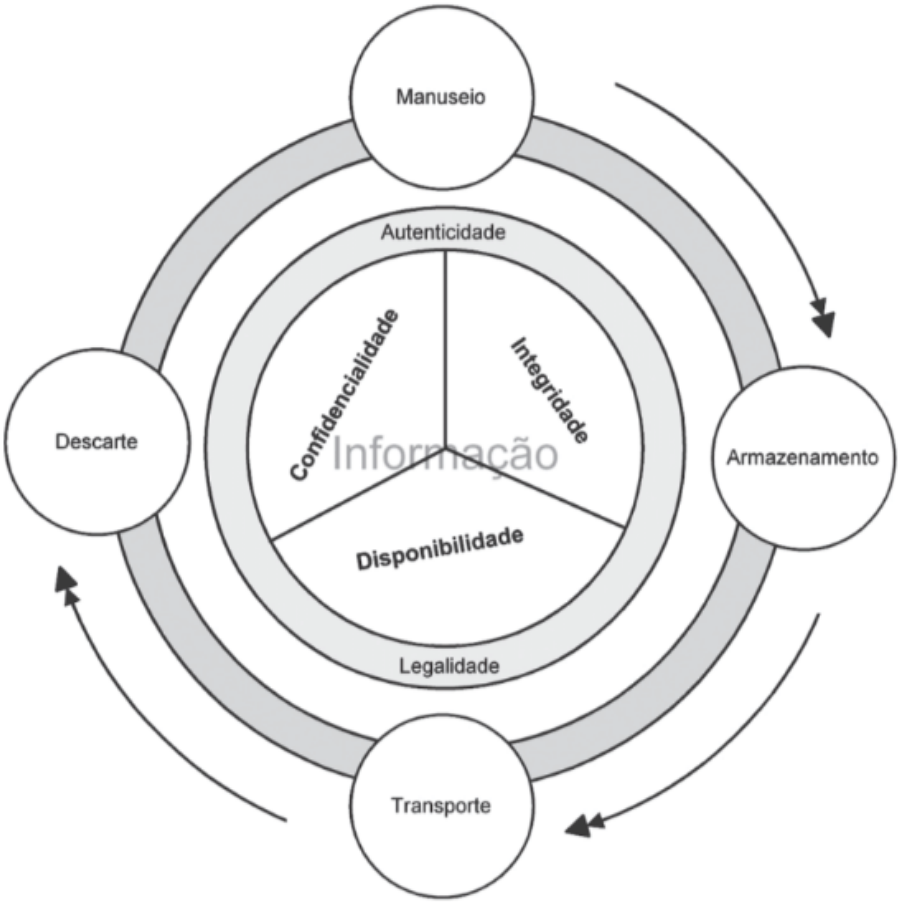
De acordo com Hintzbergen *et al*. (2018) a tríade CID constitui importantes princípios críticos de segurança. O primeiro trata-se da Confidencialidade, que pode ser definida como a demarcação sobre quem pode e/ou deve ter acesso a determinada informação, havendo a garantia precisa do sigilo que deve ser aplicado nos elementos de processamento de dados e a inviabilização da divulgação sem autorização. Em segundo, destaca-se a Integridade, que de acordo com o autor faz a referência a ser exato e consistente com o seu estado ou informação procurada, sendo que, qualquer mudança nos dados com ou sem permissão, é uma violação de dados. Por último, há a Disponibilidade que é caracterizada pela oportunidade, isto é, a informação está disponível quando requisitada. Ainda há a continuidade que é a possibilidade de trabalho mesmo em falhas e a robustez, ou seja, a existência de suporte a toda equipe que trabalhe em determinado sistema.

É importante ressaltar alguns outros conceitos importantes na Segurança da Informação. Segundo Laureano (2005), são importantes, por exemplo, as adições de Autenticidade e Legalidade. O primeiro se refere à garantia de que a informação ou o usuário da própria é autêntico, ou seja, atesta com exatidão, a proveniência dos dados ou da informação. Já o segundo conceito se refere à garantia legal, em termos jurídicos da informação, onde o sistema se adere a uma legislação.

O ciclo de vida da informação é constituído e identificado pelas fases vividas por ela e que a põe em risco. Esses momentos são vividos pelos ativos físicos, tecnológicos e humanos que usam a informação e que fazem por sua vez a sustentação dos processos (SÊMOLA, 2022).

Outro ponto importante é em referência aos dados e informações e como eles são tratados no seu ciclo de vida. Para Sêmola (2022), representando às situações onde as informações são expostas as ameaças que põem em risco as suas características, dessa forma atingindo sua segurança o diagrama, apresentado na Figura 1, revela todos os momentos do ciclo de vida que são dignos de atenção.

Figura 1 - Quatro momentos do ciclo de vida da informação, considerando os conceitos básicos da segurança e os aspectos complementares.



Fonte: Sêmola, 2013.

Sem ter em conta a forma de como a informação é caracterizada, todos esses momentos são aplicados. Com início no Manuseio, que é onde a informação é originada e manipulada. Em seguida do Armazenamento, momento onde a informação é armazenada. Conseguinte há o seu Transporte, que é representado por onde a informação iria ser levada de um ponto a outro. E por fim o seu Descarte, que é o momento final onde a informação é descartada (SÊMOLA, 2022).

No que faz referência a Segurança da Informação o NIST (*National Institute of Standards and Technology*), começou em 2013 dentro do *National Cybersecurity Center of Excellence* (NCCoE), a criação de seu *framework* voluntário, se embasando em padrões, diretrizes e melhores práticas que já existem, visando amenizar os riscos de segurança em infraestruturas críticas (PAULA, 2020).

Na visão da responsabilidade organizacional e empresarial da Segurança da Informação, o framework elaborado pela NIST, dá apoio nesse sentido, apresentando ações a serem tomadas por seus responsáveis no desafio da segurança cibernética. Segundo Mahn *et al*. (2021), o Cybersecurity Framework é uma ferramenta capaz de auxiliar uma organização a iniciar ou aperfeiçoar o seu programa de segurança cibernética. Além disso, o programa é capaz de estimular a comunicação entre as diversas partes interessadas com a segurança cibernética.

O Framework é organizado com cinco funções principais, que são: Identificação, Proteção, Detecção. Resposta e Recuperação. Os 5 termos são largamente populares, e quando ponderados em conjunto, são capazes de oferecer uma visão abrangente do ciclo de

vida do gerenciamento dos riscos que fazem referência à segurança cibernética. As tarefas de cada função são listadas a seguir no Quadro 1 (MAHN *et al*., 2021).

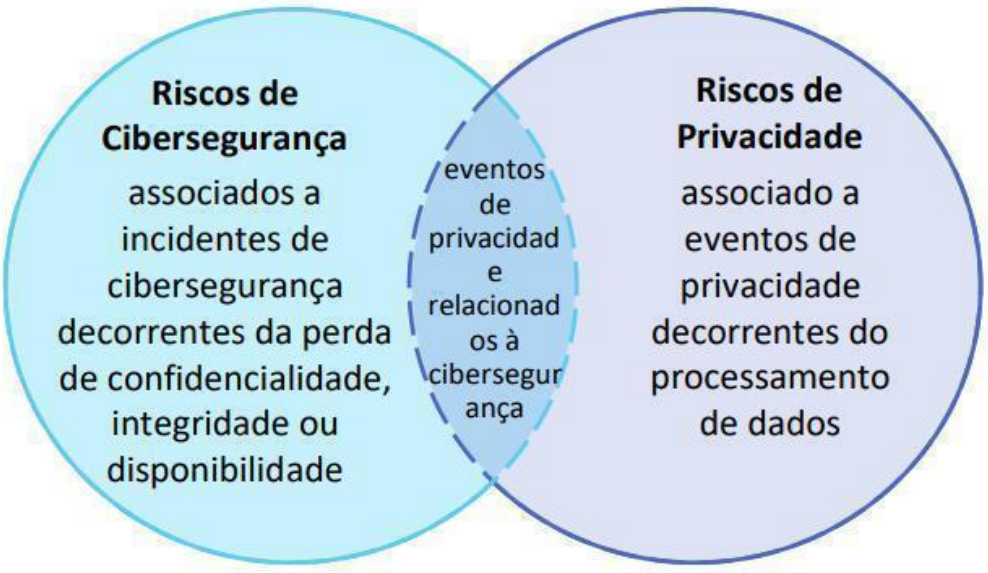
Quadro 1 - Tópicos do *Cybersecurity Framework*.

Função específica	**Atividade realizada pela função**
Identificação	Fortalecer a compreensão organizacional a fim de gerir os riscos de segurança cibernética frente a sistemas, ativos, dados e recursos.
Proteção	Fomentar e implementar as soluções de segurança necessárias para a entrega de serviços
Detecção	Desenvolver e executar as tarefas adequadas para a identificação de ocorrências voltadas a eventos de segurança cibernética.
Resposta	Expandir e executar as atividades necessárias para responder durante a detecção de um evento de segurança cibernética.
Recuperação	Realizar os deveres adequados para conservar os planos de recuperação e realizar a recuperação de recursos ou serviços afetados em um evento de segurança cibernética.

Fonte: Elaborada pelo autor com base em MAHN *et al*., 2021.

Tendo em vista que o gerenciamento do risco de segurança cibernética tem contribuição com o do risco de privacidade, isso não é o bastante, pois os riscos de privacidade também podem advir de origens sem relação aos incidentes de cibersegurança, (como é apresentado na Figura 2), ter o entendimento geral das muitas origens da segurança cibernética e dos seus riscos de privacidade é essencial para apontarmos as soluções mais eficazes para esses riscos (BOECKL; LEFKOVITZ, 2020).

Figura 2 - Relação entre risco de segurança cibernética e privacidade.



Fonte: Boeckl e Lefkovitz, 2020.

Veja como o autor comenta do *Privacy Framework*.

> A abordagem do *Privacy Framework* para o risco de privacidade é considerar os eventos de privacidade como possíveis problemas que os indivíduos podem enfrentar decorrentes das operações do sistema, produto ou serviço com dados, seja em formato digital ou não digital, por meio de um ciclo de vida completo, desde a coleta de dados até o descarte (BOECKL; LEFKOVITZ, 2020, p. 3).

Em um cenário onde os indivíduos desconhecem os tipos de dados e informações são coletados e como eles são compartilhados, o setor privado procura potencializar o aproveitamento deles. Nesse sentido, as "coisas" também recebem alvos para ataques em larga escala, causando interrupções no funcionamento normal da Internet, nas redes que são associadas a ela, além de outros setores da sociedade. (HUREL; LOBATO, 2018).

O objetivo de segurança mais cobiçável da IoT está em proteger as informações coletadas, já que estas, coletadas de dispositivos físicos, também podem incluir informações confidenciais de usuários. Por essa razão, a segurança dos sistemas IoT precisam ser resistentes a ataques ligados aos dados, além de fornecer confiança, segurança e privacidade de dados (LEITE, 2019).

2.3 VULNERABILIDADES E PREVENÇÃO EM IOT

Os desafios para a implementação de segurança em dispositivos de Internet das Coisas (IoT) também são encontrados. Para Berlanda (2021), quando se trata de dispositivos IoT, diversos desafios são existentes, pois em uma implantação de conjuntos de dispositivos, muitos deles têm a tendência de serem idênticos ou quase idênticos. Dessa forma faz com que falhas encontradas em um deles possam ser exploradas nas demais. Além disso, a depender do uso do dispositivos, a sua instalação pode ser realizada com dificuldade de acesso, tornando a sua atualização ou configuração mais desafiadora.

No cenário apresentado, às pessoas com más intenções, podem usufruir dessas falhas para efetuar diferentes tipos de ataques, sendo ativos ou passivos, como são os ataques *man-in-the-middle*, *DDoS*, *sniffing* e outros. Esses ataques podem ter como foco apenas a ruptura de dados que passam pela rede, a alteração dos mesmos ou até a tentativa de tornar a rede indisponível (BERLANDA , 2021).

As aplicações IoT podem ser divididas em quatro camadas, sendo elas a camada de detecção, de rede, de *middleware* e de aplicação. Todas essas camadas em um dispositivo IoT usam diferentes tecnologias que carregam consigo uma série de brechas e ameaças à segurança. Além das quatro camadas, pode-se incluir os problemas de segurança relacionados aos *gateways* que fazem a conexão entre essas camadas (HASSIJA *et al*., 2019).

Em virtude da intensa variedade de protocolos, tecnologias e dispositivos em uma aplicação IoT, os conflitos de escolha significativos estão entre o custo-benefício, segurança, confiabilidade, privacidade, cobertura e latência. Se uma das métricas for melhorada, pode resultar em uma degradação de uma das outras métricas (HASSIJA *et al*., 2019).

Os requisitos de segurança para tecnologias IoT não são capazes de serem atingidos meramente juntando soluções específicas de cada camada. Efetivamente, é necessário levar em consideração o sistema IoT como um sistema completo e que a sua segurança deve ser elaborada como um encadeamento que é tão robusto quanto a sua conexão mais frágil. (FRUSTACI *et al*., 2018).

Consequentemente, para aprimorar a segurança da IoT, também é necessário haver uma cooperação entre as camadas, projetando soluções de segurança com a utilização de camadas cruzadas, dessa forma, ultrapassando problemas de integração heterogênea. Dessa

forma, a interoperabilidade, seria capaz de tornar um dos fatores favoráveis para a segurança da IoT. (FRUSTACI *et al*., 2018).

2.4 IOT RESIDENCIAL

O entendimento da importância na implementação de tecnologia IoT e seus dispositivos é de grande relevância para entender o seu contexto. As *Smart Home* (como são chamadas as casas inteligentes), agora são apontadas como uma das aplicações mais populares da IoT. A sua característica importante é a sua automação e o principal objetivo disso é visar reduzir o esforço humano e esse fator é de grande importância para os sistemas controlados remotamente (PAUL; GANESH; SUNITHA, 2018)

A IoT faz a troca de funcionalidade para a conectividade e a tomada das decisões orientada por dados, o que significa que um dispositivo pode ter mais utilidade se estiver interconectado com outros dispositivos. Porém, a IoT não é tão só uma junção de dispositivos e sensores conectados entre si, mas sim uma densa integração do mundo virtual e real, onde ocorre a conversação entre pessoas e dispositivos (MOCRII; CHEN; MUSILEK, 2018)

A caracterização de casa inteligente não seria possível sem a computação ubíqua (um termo de computação que faz referência a onipresença da computação no dia a dia das pessoas) e da variedade de sensores espalhados pelas casas. Porém, lamentavelmente, a utilização desses dispositivos, que usam transmissão sem fio, abre brechas de ataques à segurança e privacidade das pessoas da casa (MOCRII; CHEN; MUSILEK, 2018) .

O problema central dos pesquisadores está na segurança dos protocolos de IoT, em especial a segurança da certificação do usuário e a segurança dos aparelhos. Os esquemas de segurança nas casas inteligentes são considerados critérios críticos para muitos dispositivos com diferentes capacidades. Um invasor pode atingir os dados de um usuário mesmo quando uma criptografia segura está sendo usada, e essas informações podem ser usadas para obtenção de dados sensíveis aos moradores da casa (ZAIDAN *et al*., 2018).

Enquanto é elaborada a problemática, também é possível ser feita recomendações para a segurança das redes domésticas. Para Zaidan *et al*., (2018), ações como a interface de usuário também podem ser desenvolvidas em várias plataformas para tratar das demandas de segurança e evitar violações na transferência de informações para os objetos inteligentes.

Nos sistemas de IoT, em especial nas casas inteligentes, há muitas semelhanças com as redes de computadores comuns, incluindo alguns problemas de segurança. Dentro de uma rede doméstica podem haver aparelhos como computadores, smartphones e tablets que tem muito poder de processamento e tem constante monitoração dos usuários. No entanto, os dispositivos IoT possuem limitações de hardware e design que impossibilitam que as medidas de segurança tradicionais sejam implementadas (COSTA; BARROS; TAVARES, 2019).

Algumas dessas limitações dos dispositivos IoT são especificadas, segundo Haritha e Lavanya. (2017) como no Quadro 2 a seguir:

Quadro 2 - Limitações e problemas em dispositivos IoT.

Limitações dos dispositivos IoT	**Brechas causadas pelas limitações**
Uso de CPUs de baixa velocidade e funcionamento à bateria.	Os algoritmos criptográficos modernos necessitam de uma computação rápida.
Limitações de memória em comparação aos telefones e etc.	Os esquemas de segurança comuns não são elaborados com foco em dispositivos com restrição de memória.
Uso de interfaces de rádio de	As técnicas de segurança tradicionais não podem ser usadas

baixa taxa de dados para comunicação.	diretamente a sistemas de IoT pela mídia de comunicação com baixa largura de banda.
Sistemas IoT podem não receber patches necessários.	Dificuldades ou até inviabilização de atualizações de patches de segurança.
Entrada de dispositivos IoT na rede sem pré-configuração.	Essas mudanças inesperadas podem afetar o desempenho dos esquemas de segurança das topologias existentes.
Diferentes tipos de dispositivos IoT e diferentes com ampla variação de protocolos.	Entre as soluções de segurança atuais é difícil encontrar uma solução de segurança que comporte uma junção heterogênea de variados dispositivos IoT.

Fonte: Elaborada pelo autor com base em Haritha e Lavanya, 2017.

Poucos esquemas de segurança consideram os obstáculos frente à privacidade em sistemas baseados em IoT. Ademais, existem alguns problemas de segurança que são mal ajustados, como em tecnologias M2M, RFID, além da computação ubíqua, que precisam ser adaptadas completamente no paradigma IoT (HARITA E LAVANYA, 2017).

3 METODOLOGIA

A realização desse trabalho seguiu algumas linhas de desenvolvimento, sendo a primeira delas a realização de uma *pesquisa bibliográfica*, que se deu a partir do estudo de materiais já produzidos sendo principalmente de livros e artigos científicos; seguido de uma *análise documental*, pois buscou-se usufruir de relatórios e estatísticas de documentos sem um tratamento analítico e por fim um *levantamento de campo*, que teve o intuito de reunir informações do universo pesquisado (GIL, 2010).

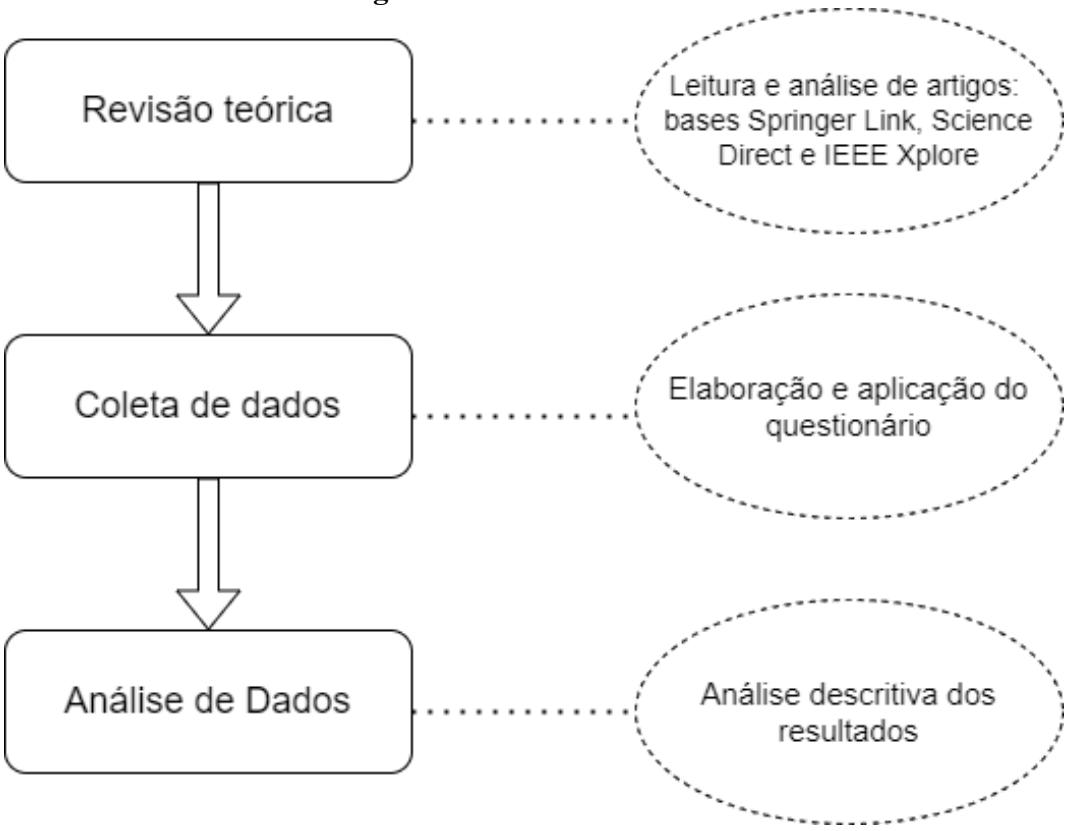
Quanto aos seus objetivos, este estudo é exploratório e descritivo, pois tem como objetivo proporcionar proximidade ao assunto desenvolvido ao longo do trabalho e realizar a introdução ao tema da pesquisa. Além disso, o estudo exploratório tem como intuito o de desenvolver conceitos tendo em vista a noção de problemas ou hipóteses de estudos anteriores, já o estudo descritivo é caracterizado pelo detalhamento de uma população ou de um fenômeno (GIL, 2010).

A abordagem deste trabalho é do tipo qualitativa, pois busca apresentar uma revisão teórica de estudos sobre Internet das Coisas (IoT) e Segurança da Informação (SI), estimando as suas vulnerabilidades. Para isso, foi realizado um levantamento de dados com a aplicação de um questionário (*survey*) que contou com questões semi-abertas e fechadas, sendo estas através da escala Likert para a elaboração de 25 dos 33 questionamentos elaborados, junto a possíveis usuários de dispositivos IoT.

A pesquisa qualitativa se faz necessária por abordar os participantes de forma externa aos contextos de pesquisa, e entender os fenômenos sociais de diferentes formas, seja pela análise de experiências dos indivíduos ou grupos, pelas suas interações e comunicações e pela investigação de seus documentos e experiências (GIBBS, 2009).

A figura 3 descreve o fluxo da metodologia do trabalho.

Figura 3 - Fluxo do trabalho.



Fonte: Elaborado pelo autor, 2022.

Inicialmente, para o desenvolvimento desta pesquisa, foram selecionados os livros, artigos e documentos com publicações a partir do ano de 2005 até o ano de 2022, que contribuíram para fundamentar a revisão teórica do trabalho. Os artigos foram retirados das bases *Springer Link*, *Science Direct* e *IEEE Xplore*. A seleção dos artigos foi realizada por meio das seguintes palavras-chaves: "*Internet of Things*", "*Smart Homes*", "*Automation*", "*Security issues*", "*Security challenges*", "*IoT Solutions*" e "*Survey IoT*".

Na etapa seguinte, foi elaborado e aplicado um questionário com informações advindas da revisão teórica. A coleta de dados foi realizada por meio digital pela plataforma do *Google Forms* e o seu link de acesso foi divulgado em grupos de WhatsApp e nas salas de aula do IFPI - Campus Floriano. Com a análise dos dados coletados, foi possível obter os resultados que buscaram responder os objetivos estabelecidos inicialmente e elaborar as conclusões alcançadas ao fim do trabalho .

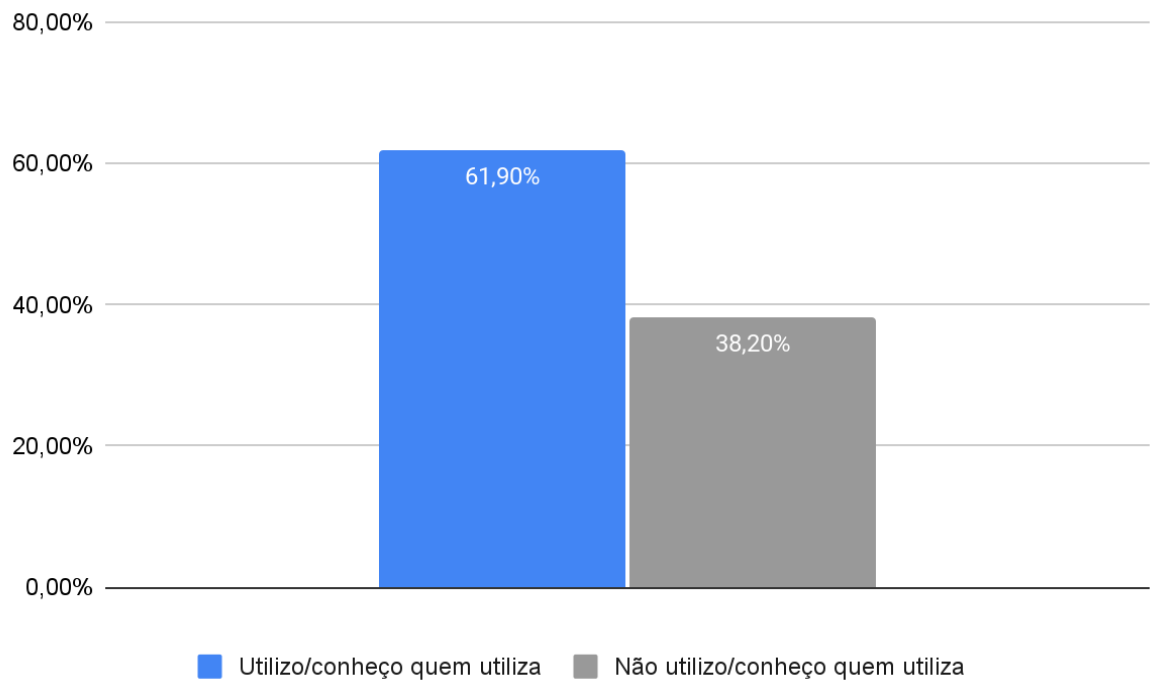
O questionário foi respondido por 89 alunos dos cursos de tecnologia da informação ofertados no Instituto Federal do Piauí - Campus Floriano, sendo desses, os cursos integrados ao médio, concomitante e superior. A faixa etária dos alunos se deu com a 14 a 20 anos sendo predominante, com 63 respondentes; seguido dos alunos com 21 a 25 anos ques representaram 23 das respostas da pesquisa e a minoria sendo representada por alunos com 31 ou mais anos que contaram com 3 respostas do questionário; destacando que 0% foi o valor dos alunos entre 26 a 30 anos.

4 RESULTADOS E DISCUSSÃO

Embora seja reconhecido na literatura que a tecnologia de Internet das Coisas tem passado por uma expansão, pouco é discutido sobre alguns dos principais riscos e precauções no seu uso a nível residencial. Assim, à luz da necessidade de entender as possíveis brechas dessa tecnologia e a necessidade de proteção no contexto da internet atual, este trabalho respondeu quais são alguns dos principais riscos e precauções no uso de tecnologia de Internet das Coisas a nível residencial.

Para explorar essa questão, os resultados dos gráficos abaixo foram baseados em dados de pesquisas no contexto dos alunos dos cursos de tecnologia da informação integrados ao médio, concomitante e superior do IFPI - Campus Floriano e em trabalhos já realizados que envolvem essa temática. No questionário, buscou-se coletar informações a respeito dos aparelhos inteligentes que os participantes da pesquisa utilizam em ambientes residenciais, bem como saber o grau de conhecimento da utilização desses dispositivos por terceiros.

Gráfico 1 - Conhecimento prévio sobre IoT residencial

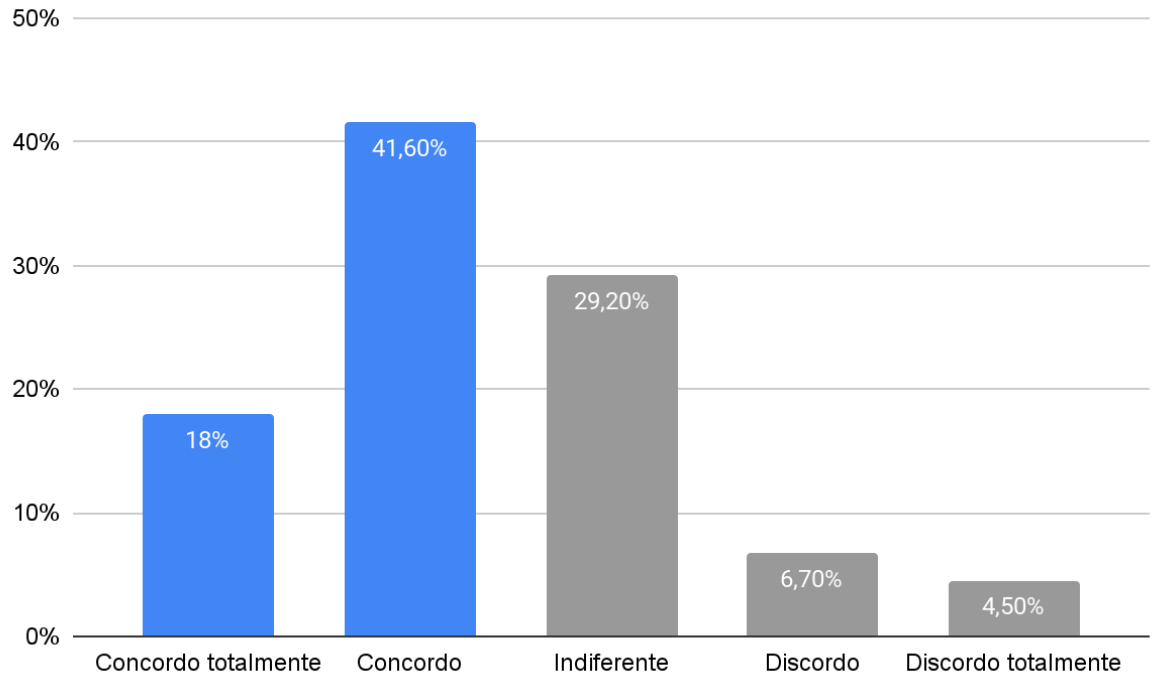


Fonte: Elaborado pelo autor, 2022.

Dos respondentes, 61,8% utilizam ou conhecem alguém que utiliza alguns dos exemplos que foram dados no questionário, como assistentes de automação, câmeras, lâmpadas e sensores - entre outros dispositivos inteligentes que podem ser usados em residências. A participação desses dispositivos inteligentes nas vidas das pessoas já se faz presente mesmo em um contexto de país que não está democratizado o uso da internet (VILELA E SILVESTRINI, 2017).

O gráfico 2 apresenta o resultado do levantamento sobre uma autocrítica em relação aos cuidados com os dispositivos inteligentes, os respondentes foram questionados se saberiam tomar os devidos cuidados a fim de evitar incidentes hackers.

Gráfico 2 - Tomar os devidos cuidados para evitar incidentes hackers.



Fonte: Elaborado pelo autor, 2022.

A maioria dos respondentes da pesquisa (59,6%) responderam “concordo” ou “concordo totalmente” sobre conhecerem os devidos cuidados para evitar ataques hackers. Com essa avaliação autocrítica dos respondentes, a expectativa seria a de que, pelo menos, mais da metade dos entrevistados teriam menos problemas relacionados a ataques hackers.

Porém, buscando observar o comportamento dos participantes em relação a hábitos de segurança básicos, foi levantado o questionamento sobre a troca de senhas, realização de varreduras com antivírus e realização de atualizações das aplicações que eles usam.

Tabela 1 - hábitos de segurança em dispositivos tecnológicos

	Nunca	Raramente	Ocasionalmente	Frequentemente	Muito frequente
Realiza troca de senhas	11,2%	43,8%	28,1%	12,4%	4,5%
Realiza scans antivírus	14,6%	32,6%	20,2%	25,8%	6,7%
Realiza atualizações	00,0%	15,7%	19,1%	32,6%	32,6%

Fonte: Elaborado pelo autor, 2022.

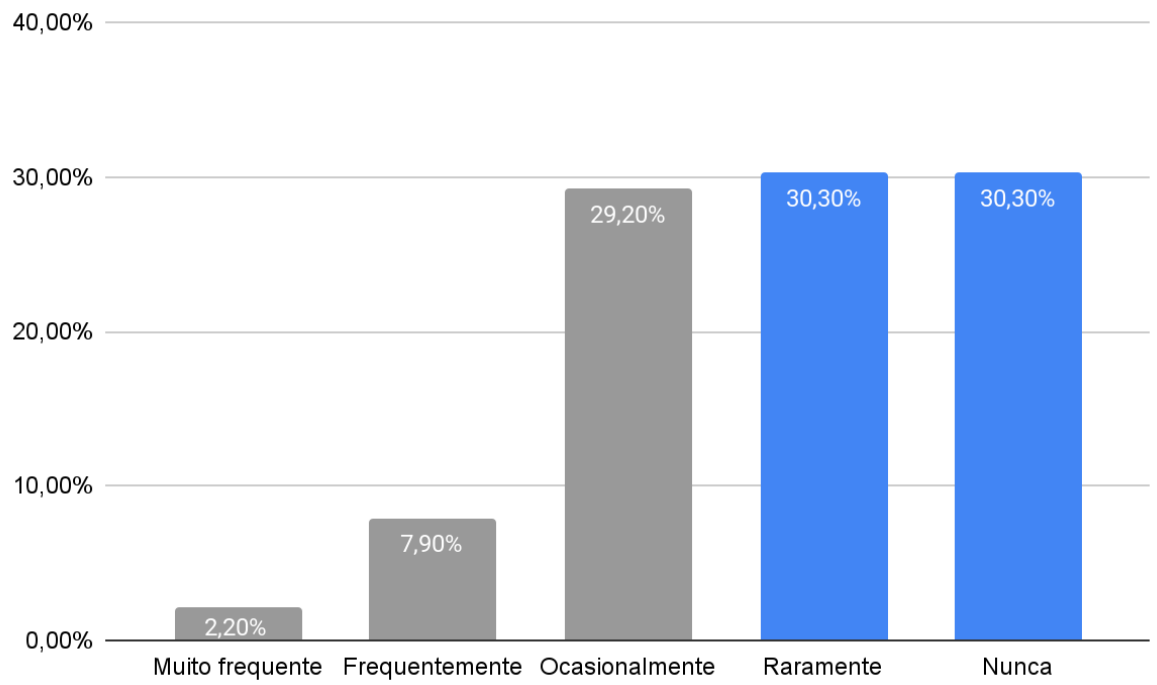
O comportamento dos participantes do questionário sugere um mau hábito em relação à segurança cibernética. Atitudes como a mudança de senhas nas porcentagem de 11,2% e 43,8% em condições como “nunca” e "raramente", respectivamente, refletem possíveis brechas em relação a tríade de confidencialidade, integridade e disponibilidade (CID) dos dados dos usuários, podendo acarretar na quebra da privacidade dos mesmos.

Com os dados coletados, pode-se observar que há uma falta de conhecimento no assunto de segurança da informação, recaindo sobre os dispositivos de internet das coisas, pois, com uma parcela de mais de 59% dos entrevistados afirmando que possuem a capacidade de tomar os devidos cuidados em um incidente sob os seus aparelhos tecnológicos, é esperado que os mesmos tenham e pratiquem soluções básicas de segurança da informação. A prática de troca de senhas, por exemplo, é comumente disseminada para ser realizada de forma corriqueira e nos resultados encontrados, as opções de "nunca" e "raramente" somaram mais de 59% dos entrevistados quanto a essa prática.

Ainda analisando o levantamento de campo, foi possível observar como os participantes do questionário estimaram quanto a participação deles em eventos voltados para a segurança da informação. A soma de mais de 60% dos questionados escolheram a opção de "nunca" ou "raramente" participarem desse tipo de ações educacionais.

Com essa baixa adesão à participação em eventos educacionais de segurança é possível interpretar o cenário como preocupante. Pois, com o ambiente cibernético sendo o "local" onde passamos mais tempo diariamente, a negligência de aspectos relacionados à segurança da informação pessoal e coletiva podem levar a brechas e incidentes nesses ambientes ocasionando a exposição de dados e informações que afetem a privacidade.

Gráfico 3 - Participação em ações educacionais voltadas à segurança.



Fonte: Elaborado pelo autor, 2022.

Observando o gráfico 3, é possível analisar como uma das suas principais vertentes, que recai sobre direitos de privacidade, ainda é pouco explorada de forma educacional. Com isso, podemos verificar uma carência dos participantes em ações educacionais referentes a uma demanda de conhecimento que ainda não foi suprida e que pode afetar diretamente as pessoas em seus aspectos de segurança em um ambiente tecnológico.

A partir do levantamento de campo realizado, foi possível observar algumas características e hábitos dos entrevistados, como nas trocas de senhas, com os resultados obtidos apontando para possíveis brechas deixadas pelos mesmos em seus usos de dispositivos tecnológicos. Dessa forma, pode-se realizar um arrolamento de algumas das

possíveis vulnerabilidades e algumas formas de prevenção no cenário de internet das coisas residencial.

A primeira vulnerabilidade que pode ser elencada é o fator humano, já que como vimos anteriormente, algumas convenções não colocadas em prática pelos usuários dos dispositivos inteligentes podem representar riscos no cenário de segurança. No trabalho realizado por Jacobsson, Boldt e Carlsson (2015), os atores humanos representam um elo frágil nos sistemas baseados em computação, o que também é um desafio complexo de se lidar na automação de casas inteligentes.

Ainda no trabalho de Jacobsson, Boldt e Carlsson (2015), o maior risco na classificação em relação aos aspectos humanos é a utilização de senhas fracas, que podem ser mitigadas pela aplicação de políticas de senhas e ferramentas de verificação. Outro fator importante é o de identificar os riscos voltados para o ser humano, que vão dos usuários finais ingênuos sendo alvos de ataques de engenharia social, até a funcionários descontentes que podem vazar informações, por exemplo, a fim de obter lucros. Algumas das soluções para lidar com essas ameaças são reunidas em políticas e contratos legais, bem como em esforços da educação do usuário final.

Algumas vulnerabilidades referentes aos dispositivos são abordadas no trabalho por Hassija et al. (2019) e podem ser compreendidas algumas das causas que afetam essa tecnologia atualmente, como no Quadro 3 a seguir:

Quadro 3 - Vulnerabilidade em dispositivos IoT.

Vulnerabilidades/Ataques	**Explicação das vulnerabilidades/ataques**
Ataque de canal lateral	Esses ataques podem levar a exposição de dados confidenciais. As microarquiteturas dos processadores, emanação magnética e também o consumo de energia podem revelar informações confidenciais aos atacantes.
Espionagem e interferência	Os aplicativos IoT comumente são implantados em ambientes abertos. O resultado disso é que as aplicações de IoT são expostas a curiosos. Esses invasores podem espionar e capturar dados durante a transmissão de informações.
Ataque de inicialização	Os dispositivos de borda são expostos a ataques no processo de inicialização. Isso acontece pois os procedimentos de segurança não estão ativados neste ponto. Os invasores podem aproveitar essa brecha e atacar os dispositivos quando são inicializados.
Ataques de site de phishing	Os ataques de phishing comumente fazem referência aos ataques em que múltiplos dispositivos IoT podem ser visados sem esforço do atacante. Os invasores ficam na espera de que algum dispositivo IoT se torne vítima ao momento em que os usuários fornecem dados, como conta e senha, em páginas da web.
Ataques de DDoS/DoS	Nesse ataque o atacante faz uma inundação dos servidores do destino com uma grande quantidade de solicitações de requisições não solicitadas. Esse não é um ataque específico de IoT, porém por sua heterogeneidade e complexidade, se torna propensa a esse tipo de ataque.
Ataques de Controle de Acesso	É um mecanismo de autorização que permite somente usuários e processos legítimos acessarem os dados da rede. Esse ataque é de nível grave em aplicativos IoT, pois quando comprometido, ele

	torna-se vulnerável a ataques.
Ataque Injeção de código malicioso	Os atacantes podem invadir o sistema ou a rede se forem vulneráveis a scripts maliciosos e direcionamentos incorretos causados pela falta de verificações do código, dessa forma serviram como ponto de entrada do invasor. Um exemplo são os ataques com XSS (cross-site scripting).
Ataques de Sniffer	Os invasores podem fazer uso de aplicativos *sniffer* (farejadores) que permitem obter acesso a dados privados do usuário se não houver os protocolos de segurança para inibí-los.

Fonte: Elaborada pelo autor com base em Hassija et al., 2021.

A apresentação de alguns ataques, colocam o usuário em posição de vulnerabilidade no uso dos dispositivos tecnológicos em conjunto com a internet. Essa posição de atacado é ainda mais explorada quando não são colocadas em prática as ações de prevenção, tanto da parte do usuário, quanto da parte dos fabricantes.

Agora, as soluções das vulnerabilidades elencadas anteriormente são abordadas no trabalho realizado por Touqeer *et al*. (2021) e são explicadas no Quadro 4 a seguir:

Quadro 4 - Soluções em dispositivos IoT.

Vulnerabilidades/Ataques	**Prevenções/soluções das vulnerabilidades/ataques**
Ataque de canal lateral	A nível de hardware, pode-se ser levantado o reconhecimento de informações, randomização e o particionamento buscando impedir o vazamento das informações. A nível de software, é possível garantir a confidencialidade com um esquema de criptografia de chave pública resistente a vazamentos.
Espionagem e interferência	Monitoramento das atividades dos invasores pelo conhecimento antecipado das especificações dos canais com diferentes antenas sendo implantadas.
Ataque de inicialização	Uso de processo de inicialização com um código desenvolvido por um fornecedor confiável ou fabricante do equipamento original (OEM) sendo executado no dispositivo. Ao usar esse mecanismo, pode-se reduzir as chances de replicações de código de firmware por atacantes.
Ataques de site de phishing	Fazer o uso de *blacklists* ou esquemas de heurísticas, onde os e-mails não desejados são bloqueados no lado do cliente ou do servidor. Além disso, os usuários devem ser capacitados para diferenciar os sites reais dos de phishing. Em adição de outras soluções, a proteção de rede e autenticação do usuário podem ser úteis para detectar ataques dessa natureza.
Ataques de DDoS/DoS	Em um ambiente de realidade, as redes de sensores sem fio exigem uma análise de parâmetros em tempo real. Um sistema de detecção de intrusão (IDS) aplicado, deve detectar qualquer tipo de atividade DoS.
Ataques de Controle de Acesso	Com o uso de controle de acesso baseado em função, qualquer pessoa do ambiente tem acesso aos aparelhos específicos conforme

	a sua função. Um sistema centralizador é quem garante a atribuição de funções, adição de dispositivos e remoção com segurança.
Ataque Injeção de código malicioso	Os aparelhos IoT possuem menor poder de processamento, o que pode evitar a execução de códigos maliciosos pesados. Uma estratégia de detecção é usar a abordagem de analisar o tempo de execução normal e o comportamento anormal, o que pode indicar quando um código malicioso é usado.
Ataques de Sniffer	A fim de evitar ataques *sniffer*, os usuários devem conectar os dispositivos em redes confiáveis e não conectar em locais públicos, pois podem não ser devidamente monitorados e conter bugs. Além disso, a criptografia tem função importante na proteção do rastreamento de rede por cifrar os dados que saem do sistema IoT.

Fonte: Elaborada pelo autor com base em Touqeer et al., 2021.

Com a diversidade de vulnerabilidades se faz necessário uma vasta série de formas de prevenções e soluções para essas brechas. A necessidade de avanço tecnológico para ser usado na tentativa de realizar a manutenção da tríade CID é visto com as defesas usando tecnologias como o IDS, heurísticas, criptografia e entre outros. Além disso, é notável a importância da exploração desses assuntos de forma educacional na busca de usá-lo a nível de prevenção dos ataques e também a nível de políticas e regulamentações.

Ainda para Touqeer *et al*. (2021), a segurança de casas inteligentes pode ser assegurada com base na implementação de segurança em cada uma das camadas dos dispositivos inteligentes. O autor ainda apresenta um exemplo de casa inteligente conectada a um gateway residencial que faz conectividade com a internet e com alguns dispositivos inteligentes e as suas possíveis brechas, elas estão representadas no Quadro 5 a seguir:

Quadro 5 - Dispositivos/ameaças e soluções em dispositivos IoT.

Dispositivo/Ameaça	**Solução**
Fechadura inteligente	Senha forte, protocolos de alta segurança
Câmera inteligente	Senha forte, rede Wi-Fi residencial segura
Medidor de energia inteligente	Criptografia de versões do software
Ataque de armazenamento	*Boot* seguro, mútua autenticação
Ataque de *gateway*	*Gateways* seguros para assistente residencial
Acesso não autorizado	Proteção Wi-Fi, senha única

Fonte: Elaborada pelo autor com base em Touqeer et al., 2021.

A disposição de internet das coisas realizada pelos autores exemplifica alguns dispositivos e soluções de objetos inteligentes que podem estar presentes no cenário atual das residências. Com essa exemplificação é possível verificar que objetos corriqueiros podem ser alvos de ataques hackers e que eles possuem algumas soluções que estão dentro do alcance do utilizador dessas tecnologias.

Com base no exposto acima, é possível ressaltar os pontos primordiais em soluções para algumas das vulnerabilidades da tecnologia de Internet das Coisas a nível residencial, com o intuito de garantir a segurança e manutenção de princípios, como os de confidencialidade, integridade e disponibilidade, dos usuários finais dessa tecnologia. Em consonância com esforços vindouras da indústria e dos usuários é possível estabelecer formas de prevenção às vulnerabilidades existentes.

5 CONCLUSÃO

Este trabalho identificou vulnerabilidades e suas formas de solução no contexto de Internet das Coisas (IoT) a nível residencial. Considerando a alta demanda dessa tecnologia, a sua grande disponibilidade e o crescimento nas residências, que são ambientes mais suscetíveis a ameaças da internet, o trabalho aborda os conceitos de IoT, os seus atributos em relação a Segurança da Informação (SI), além das fragilidades dos dispositivos inteligentes bem como as maneiras de combatê-las.

Advindo dos objetivos da pesquisa, foi feito um *survey* com alunos dos cursos de tecnologia da informação ofertados pelo Instituto Federal do Piauí - Campus Floriano. Com esse questionário foi levantado possíveis vulnerabilidades que estariam presentes nas residências desse grupo apresentado. Além da realização do levantamento de campo, foi realizada a interpretação dos dados obtidos com achados da pesquisa bibliográfica. Com a análise das informações obtidas através da análise nas bases de dados *Springer Link*, *Science Direct* e *IEEE Xplore*, pode-se levantar vulnerabilidades e as suas formas de prevenção/solução.

Dessa forma foi possível alcançar os objetivos estabelecidos inicialmente, tendo como resultados, a avaliação de algumas das brechas/vulnerabilidades e as suas formas de prevenção/resolução, partindo da tanto da ótica das responsabilidades das provedoras dos serviços e dispositivos inteligentes, quanto das responsabilidades do usuário final.

Os resultados obtidos contribuem para auxiliar na disseminação de um tema que se faz presente na sociedade atual, colaborando no conhecimento e discernimento de boas práticas que envolvem a segurança da informação na tecnologia de Internet das Coisas, com foco em residências. Além disso, esse trabalho também busca prover insumos para trabalhos futuros que abordem essa temática.

O trabalho encara determinadas limitações devido a exploração específica de Internet das Coisas residencial, além da a extensão do trabalho se restringir em pesquisar apenas a parte teórica das vulnerabilidades e suas soluções.

Como sugestão para trabalhos futuros, é sugerido realizar um trabalho de revisão sistemática onde poderá ser elencado outros artigos para desenvolvimento de novas pesquisas. Além disso, podem-se realizar testes práticos em dispositivos inteligentes residenciais mais vendidos, na tentativa de explorar as suas possíveis brechas e soluções das vulnerabilidades, caso estas sejam encontradas.

REFERÊNCIAS

BERLANDA, Rodrigo Grando. **Guia de segurança da informação para a conectividade de dispositivos IoT**, 2021. Trabalho de conclusão de curso (Curso Superior de Tecnologia em Gestão da Tecnologia da Informação) - Instituto Federal de Santa Catarina, Florianópolis, 2021. Disponível em: https://repositorio.ifsc.edu.br/bitstream/handle/123456789/2304/CSTGTI-TCC-RodrigoGrandoBerlanda-GuiadeseguranCadainformacaoparaaconectividadededispositivosIoT-Assinado.pdf?sequence=1. Acesso em: 15 jun. 2022.

BOECKL, Kaitlin R.; LEFKOVITZ, Naomi B. **NIST Privacy Framework**: A Tool For Improving Privacy Through Enterprise Risk Management, Version 1.0. Gaithersburg: National Institute Of Standards And Technology, 2020. Disponível em: https://www.nist.gov/publications/nist-privacy-framework-tool-improving-privacy-through-enterprise-risk-management. Acesso em: 08 jun. 2022.

COSTA, Luís; BARROS, João; TAVARES, Miguel. Vulnerabilities in IoT Devices for Smart Home Environment. **Proceedings of the 5th International Conference On Information Systems Security And Privacy**, [S.l.], p. 615-622, 2019. Disponível em: https://run.unl.pt/bitstream/10362/107397/1/ICISSP_2019_100.pdf. Acesso em: 18 jun. 2022.

DAWS, R. Kaspersky: Attacks on IoT devices double in a year. **IoT News**, 2021. Disponível em: https://www.iottechnews.com/news/2021/sep/07/kaspersky-attacks-on-iot-devices-double-in-a-year/. Acesso em: 22 mai. 2022.

DUTTON, William H.. Putting things to work: social and policy challenges for the internet of things. **Info**, [S.L.], v. 16, n. 3, p. 1-21, 6 maio 2014. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/info-09-2013-0047/full/html. Acesso em: 14 jun. 2022.

FRUSTACI, Mario et al. Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. **IEEE Internet of Things Journal**, [S.l.], v. 5, n. 4, p. 2483-2495, 2018. Disponível em: https://ieeexplore.ieee.org/document/8086136. Acesso em: 15 jun. 2022.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010. 184 p.

GIBBS, Graham. **Análise de dados qualitativos**. Porto Alegre: Artmed, 2009. 198 p.

HARITHA, A.; LAVANYA, A. **Internet of Things: Security Issues. International Journal of Engineering and Science Invention**, v. 6, p. 45–52, 2017. Disponível em: http://www.ijesi.org/papers/Vol(6)11/Version-2/G0611024552.pdf. Acesso em: 18 jun. 2022.

HASSIJA, Vikas et al. A Survey on IoT Security:Application Areas, Security Threats, and Solution Architectures. **IEEE Access**, [S.l.], v. 7, p. 82721-82743, 2019. Disponível em: https://ieeexplore.ieee.org/document/8742551. Acesso em: 15 jun. 2022.

HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018. 256 p.

HUREL, L. M.; LOBATO, L. C. **Segurança e privacidade para a Internet das Coisas**. Instituto Igarapé, 21 nov. 2019. Disponível em: https://igarape.org.br/wp-content/uploads/2018/11/Seguranc%CC%A7a-e-Privacidade-para-a-Internet-das-Coisas.pdf. Acesso em: 9 jun. 2022.

JACOBSSON, A.; BOLDT, M.; CARLSSON, B. A risk analysis of a smart home automation system. **Future Generation Computer Systems**, v. 56, p. 719–733, 2016. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0167739X15002812. Acesso em 15 dez. 2022.

KUROSE, James; ROSS, Keith. **Redes de computadores e a internet**: uma abordagem top-down. 8. ed. Porto Alegre: Bookman, 2021. 632 p.

LAUREANO, M. A. P. **Gestão de segurança da informação**, 2005. Disponível em: http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf. Acesso em: 7 jul. 2022.

LEITE, Leandro Rogério Corrêa. **Internet das Coisas (IoT)**: vulnerabilidades de segurança e desafios, 2019. Trabalho de conclusão de curso (Curso Superior de Tecnologia em Segurança da Informação) - Faculdade de Tecnologia de Americana, Americana, 2019. Disponível em: http://ric.cps.sp.gov.br/handle/123456789/3978. Acesso em: 13 jun. 2022.

LUETH, K. L. State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. **IoT Analytics**, 2018. Disponível em: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b. Acesso em: 22 maio. 2022.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: Fgv Editora, 2018. 192 p. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf. Acesso em: 09 jun. 2022.

MAHN, Amy et al. **Getting Started with the NIST Cybersecurity Framework**: A Quick Start Guide. Gaithersburg: National Institute Of Standards And Technology, 2021. Disponível em: https://www.nist.gov/publications/getting-started-nist-cybersecurity-framework-quick-start-guide. Acesso em: 08 jun. 2022.

MOCRII, Dragos; CHEN, Yuxiang; MUSILEK, Petr. IoT-based smart homes: A review of system architecture, software, communications, privacy and security. **Internet Of Things**, [S.l.], v. 1-2, p. 81-98, 2018. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S2542660518300477. Acesso em: 17 jun. 2022.

NESHENKO, Nataliia et al. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. **IEEE Communications Surveys & Tutorials**, [S.l.], v. 21, n. 3, p. 2702-2733, 11 abr. 2019. Disponível em: https://ieeexplore.ieee.org/document/8688434/. Acesso em: 14 jun. 2022.

PAUL, Chinju; GANESH, Amal; SUNITHA, C. An overview of IoT based smart homes. **2018 2nd International Conference on Inventive Systems and Control (ICISC)**, [S.l.], p. 43-46, 2018. Disponível em: https://ieeexplore.ieee.org/document/8398858. Acesso em: 16 jun. 2022.

PAULA, Marcus Vinícius Cândido de. **Segurança da informação e a internet das coisas**. 2020. Monografia (Graduação em Engenharia da Computação) - Faculdade de Tecnologia e Ciências Sociais Aplicadas, Centro Universitário de Brasília, Brasília, 2020. Disponível em: https://repositorio.uniceub.br/jspui/handle/prefix/15108. Acesso em: 7 jul. 2022.

RIBEIRO, Arlindo Jorge de Jesus. Problemas de Segurança na Internet das Coisas. Leiria: [s. n.], 2020. Disponível em: https://iconline.ipleiria.pt/handle/10400.8/5568. Acesso em: 10 dez. 2022.

SANTOS, B. et al. **Internet das Coisas**: da Teoria à Prática. 2016. Disponível em: https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/internet-das-coisas.pdf.

SÊMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2013. 192 p. Disponível em: https://www.livrodeseguranca.com. Acesso em: 20 dez. 2022

SÊMOLA, Marcos. **Information Security Management:** an executive view. 3. ed. Rio de Janeiro: *[s.n],* 2022. 222 p. Disponível em: https://www.infosecuritybook.com. Acesso em: 20 dez. 2022

TOUQEER, H. et al. Smart home security: challenges, issues and solutions at different IoT layers. **The Journal of Supercomputing**, v. 77, n. 12, p. 14053–14089, 2021. Disponível em: https://link.springer.com/article/10.1007/s11227-021-03825-1. Acesso em: 15 dez. 2022.

VILELA, T. R. F.; SILVESTRINI, J. P. A democratização do acesso à internet no Brasil. **Anais do Congresso Brasileiro de Processo Coletivo e Cidadania**, [S. l.], n. 5, 2018. Disponível em: https://revistas.unaerp.br/cbpcc/article/view/1024. Acesso em: 20 dez. 2022.

WOOLF, N. DDoS attack that disrupted internet was largest of its kind in history, experts say. **The Guardian**, São Francisco, 26 out. 2016. Disponível em: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet. Acesso em: 22 mai. 2022.

ZAIDAN, A. A. et al. A survey on communication components for IoT-based technologies in smart homes. **Telecommunication Systems**, [S.l.], v. 69, n. 1, p. 1-25, 2018. Disponível em: https://link.springer.com/article/10.1007/s11235-018-0430-8. Acesso em: 17 jun. 2022.