**FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"**

**Curso Superior de Tecnologia em Segurança da Informação**

Cristhy Ellen Freitas Barbieri

# VULNERABILIDADES DE DISPOSITIVOS IOT EM SMART HOMES

**Americana, SP**

**2022**

**FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"**

**Curso Superior de Tecnologia em Segurança da Informação**

Cristhy Ellen Freitas Barbieri

# VULNERABILIDADES DE DISPOSITIVOS IOT EM SMART HOMES

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do (a) Profa. Dra. Maria Cristina Aranda.

Área de concentração: Segurança da Informação.

**Americana, SP**

**2022**

Cristhy Ellen Freitas Babieri

# VULNERABILIDADES DE DISPOSITIVOS IOT EM SMART HOMES

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 01 de dezembro de 2022.

**Banca Examinadora:**

_____
Orientador(a): Maria Cristina Aranda
Doutora
Fatec Americana Ministro Ralph Biasi

_____
Banca 1: Rogério Nunes de Freitas
Mestre
Fatec Americana Ministro Ralph Biasi

_____
Banca 2: Lucas Serafim Parizotto
Especialista
Fatec Americana Ministro Ralph Biasi

## AGRADECIMENTOS

Primeiramente quero agradecer a Deus que sempre me deu coragem para superar todos os desafios. Agradeço aos meus familiares por todo apoio, paciência e compreensão e por sempre me incentivarem nos momentos mais difíceis.

Agradeço a minha orientadora Profa. Dra. Maria Cristina Aranda pelos ensinamentos e auxílio necessários para a elaboração do trabalho.

Por fim, mas não menos importante, agradeço aos amigos que estiveram comigo nessa jornada.

## RESUMO

A Internet das Coisas possibilita que diferentes objetos se conectem à Internet e façam interações com ela e com outros dispositivos. Nos últimos anos, se tornou um assunto recorrente e houve um aumento de dispositivos IoT conectados à rede de uma casa, transformando-a em uma *smart home* (casa inteligente), possibilitando maior segurança, comodidade e praticidade aos usuários. Contudo, esses ambientes conectados são muito sensíveis e ainda existem muitas questões que precisam ser analisadas e tratadas, como a coleta, armazenamento, processo e extração dos dados obtidos através dos dispositivos. O objetivo desse trabalho é explorar e analisar as ameaças e vulnerabilidades que afetam os dispositivos IoT utilizados em casas inteligentes e seus usuários. Para além da análise das principais vulnerabilidades, também foi elaborado e estudado o ecossistema de uma casa inteligente, tomando conhecimento a respeito de cada medida que possa ser tomada para tornar o ambiente cada vez mais seguro e conscientizar a respeito das ameaças presentes em um ambiente conectado.



**Palavras Chave:** Segurança da informação; Internet das Coisas; Vulnerabilidades.

## ABSTRACT

*The Internet of Things allows different objects to connect to the internet and interact with it and other devices. Over the past few years, it became a recurring subject and there has been an increase in the number of IoT devices connected to a home network, turning it into a smart home, allowing for more security, convenience and comfort. Nonetheless, these connected environments are specially sensitive and there are many questions that need to be addressed and treated, such as the collection, storage, processing and extraction of the data obtained from the devices. The goal of this piece of work is to explore and analyze the threats and vulnerabilities that affect IoT devices used in smart homes and their users.In addition to the main vulnerabilities, an ecosystem of a smart home was also drawn up, considering every measure capable of being taken to make the environment safer and raising awareness to the threats that exist in a connected environment.*



**Keywords:** *Information Security; Internet of Things; Vulnerabilities.*

**SUMÁRIO**

## LISTA DE FIGURAS

# 1 Introdução

Com o avanço inquestionável das tecnologias presentes no cotidiano e o aumento constante das interações entre ser humano e máquina, o comportamento das pessoas foi alterado e houve o surgimento de novas maneiras de interação, ler notícias, fazer compras, etc. A Internet deixou de apenas conectar computadores e passou a conectar também pessoas e coisas, possibilitando que a realização de diversas tarefas antes realizadas com a ação de um indivíduo passasse a ser controlada por dispositivos conectados à rede.

A partir desse conceito de ligar “coisas” surgiu o termo *Internet of Things* (IoT), que viabiliza a conectividade de inúmeros dispositivos, facilitando a interação e gerando muitos benefícios para a sociedade. Entretanto, diante dessas novas janelas de oportunidades surgem também questões relacionadas à segurança e privacidade.

Este artigo analisa e mapeia as vulnerabilidades da segurança em dispositivos IoT utilizados em *smart homes* (casas inteligentes), refletindo sobre como a Segurança da Informação está apta ou não para a quantidade de informações que transitam diariamente entre os dispositivos e pessoas, além de conhecer o funcionamento da IoT e seus mecanismos. Existem muitas questões que tornam esses dispositivos vulneráveis, como a falta de arquitetura e protocolos de comunicação, não existência de certificações, capacidade de processamento, etc.

Não há dúvidas de que a IoT é uma grande inovação, tem grandes vantagens e garante melhor qualidade de vida das pessoas e organizações, contudo ainda é necessário conhecer os problemas e barreiras que poderão ser enfrentados com o crescente aumento do uso desses dispositivos.

# 2 Revisão bibliográfica

## 2.1 Segurança da informação

A Segurança da Informação (SI) está ligada diretamente à proteção dos ativos, com o objetivo de preservar seu valor para um indivíduo ou organização. Devido à constante evolução tecnológica, a proteção da informação tornou-se um grande desafio. Fontes (2010), afirma que “a segurança da informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que têm por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada.”

Segundo Sêmola (2014, p.7):

> O sangue da empresa é a informação. Distribuída por todos os processos de negócio, alimentando-os e circulando por diversos ativos (tudo o que manipula direta ou indiretamente a informação, inclusive ela própria), ambientes e tecnologias, a informação cumpre papel de fornecer instrumentos para a gestão do negócio.

Diante disso, é importante assegurar a proteção da informação, reduzir perdas e garantir a continuidade dos negócios.

O conceito de SI é normatizado pela NBR ISO/IEC 17799:2001 criado a partir do padrão inglês (British Standard) BS-7799 e foi recodificado em 2005 para numeração NBR ISO/IEC 27002:2005, e os principais atributos que orientam a análise, planejamento e implementação da segurança da informação são a confidencialidade, integridade e disponibilidade.

- Confidencialidade é a propriedade que limita o acesso à informação somente aos indivíduos, entidades ou processos autorizados pelo proprietário da informação;
- Integridade é o requisito de proteção da exatidão e totalidade do conjunto de ativos;
- Disponibilidade é a capacidade de estar acessível e disponível para serem usados sob demanda de uma entidade autorizada.

Além dos três pilares, Sêmola (2014, p. 9) acrescenta outros dois aspectos:

- Legalidade: garantia do uso da informação conforme leis aplicáveis, regulamentos, licenças e contratos;
- Autenticidade: garantia na veracidade da fonte, de que os remetentes sejam os que dizem ser e que a mensagem não foi alterada.

Ferreira e Araújo (2006 *apud* FUKUDA, 2019, p. 18) adicionam também o conceito de não repúdio de autoria, onde o usuário que gerou ou alterou a informação (arquivo ou *e-mail*) não pode negar o fato, pois existem mecanismos que garantem sua autoria.

Posto isto, para garantir sucesso e preservar os dados que estão frequentemente sujeitos a ameaças e riscos devido à sua vulnerabilidade, é importante firmar e cumprir políticas de segurança, definindo normas e procedimentos que devem ser tomados para proteção e controle da informação.

A implantação de uma política de segurança reduz a probabilidade de ocorrência de quebra da confidencialidade, integridade e disponibilidade, e também da redução de danos causados por eventuais ocorrências.

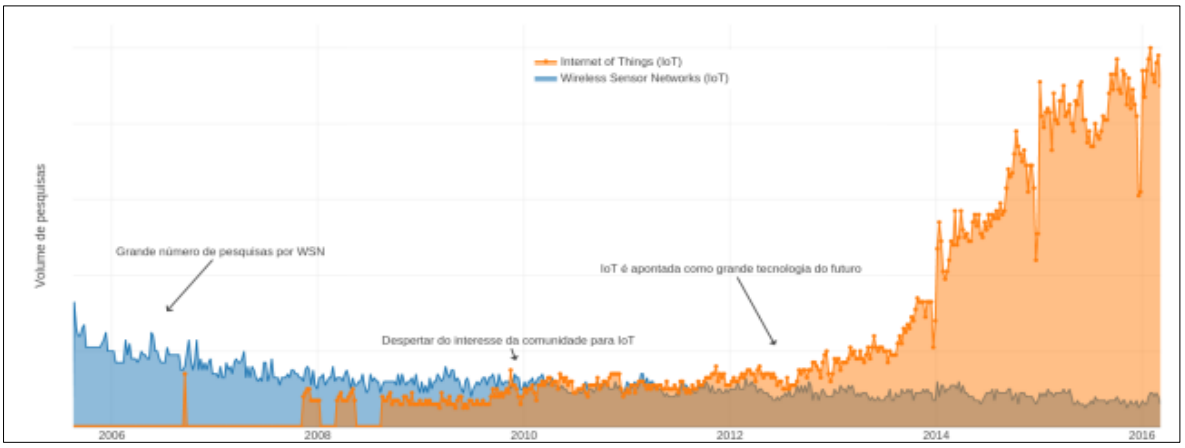
> A política, preferencialmente deve ser criada antes da ocorrência de problemas com a segurança, ou depois, para evitar reincidências. Ela é uma ferramenta tanto para prevenir problemas legais como para documentar a aderência ao processo de controle de qualidade. (FERREIRA, 2008, p.36)

As medidas de segurança da informação são de extrema importância e devem ser sérias e tratadas com prioridade em ações preventivas e não somente corretivas. O uso das informações tem impacto tanto para as organizações quanto para as pessoas, sem políticas, ferramentas e *frameworks* de segurança adequados os riscos se tornam problemas constantes, portanto é primordial investir em metodologias para garantir a proteção das informações.

## 2.2 Internet of Things

O termo *Internet of Things* (IoT) foi mencionado pela primeira vez em 1999 por Kevin Ashton em uma apresentação realizada na Procter & Gamble (ASHTON, 2009) e era associado ao uso da tecnologia RFID (*Radio Frequency Identification*). Contudo, na época, o termo ainda não era tão discutido, nem foco de grandes pesquisas e só passou a ser um pouco mais procurado por volta de 2005, mas foi em 2010 que foi possível identificar um crescimento considerável (Figura 1) do termo *Internet of Things* em relação a procura pelo *Wireless Sensor Networkss*.

Figura 1- Volume de pesquisas no Google sobre *Wireless Sensor Networks* e *Internet of Things*




**Fonte:** Santos et al., 2016

De acordo com Gartner, em tradução livre, A Internet das Coisas (IoT) é definida como uma rede de objetos físicos que contém tecnologia embutida para se comunicar e sentir ou interagir com o ambiente externo ou com estados internos. (GARTNER, 2021).

A União Internacional de Telecomunicações (ITU, do inglês International Telecommunication Union) define IoT como “uma infraestrutura global para a sociedade da informação, permitindo serviços avançados interligando coisas (físicas e virtuais) baseadas em tecnologias interoperáveis de informação e comunicação existentes e em evolução.” (ITU-T, 2012).

Nos últimos anos, a Internet das Coisas se tornou uma das tecnologias mais importantes, visto que possibilita que objetos comuns do cotidiano sejam capazes de capturar, processar, armazenar e transmitir dados, como uma extensão da Internet atual, trazendo inúmeras possibilidades para o ser humano e otimizando processos nas organizações.

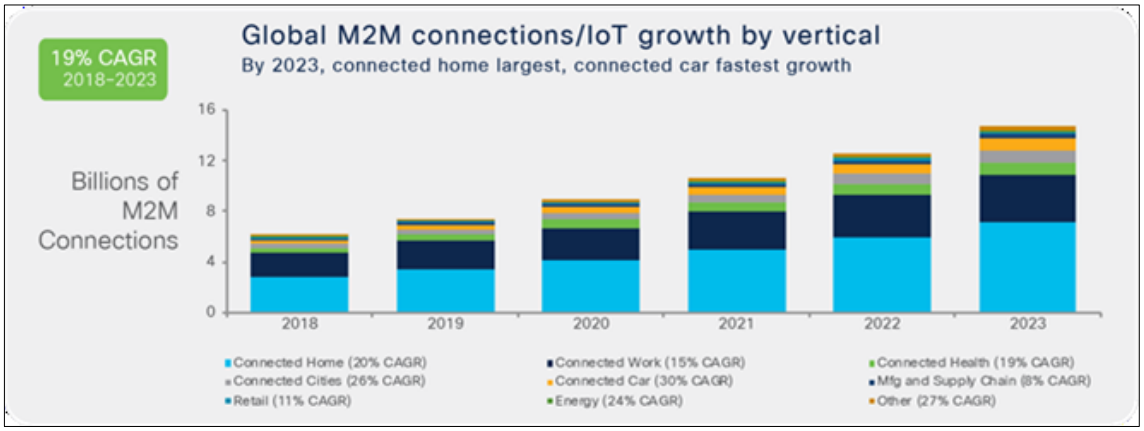
Segundo McKinsey & Company: "O ecossistema da IoT inclui fontes de dados (sensores) e outros dispositivos incorporados no mundo físico e conectados em redes analíticas através de recursos computacionais" (MCKINSEY & COMPANY, 2015 *apud* BARROS, 2021, p.24). Isto é, a Internet das coisas se manifesta de diversas formas, incluindo dispositivos de múltiplos propósitos (celulares, *tablets*, relógios e óculos inteligentes) e dispositivos especializados (sensores de temperatura, dispositivos ativos e passivos, etc) suportados por uma variedade de plataformas de *software* e *hardware*.

Há constante evolução e benefícios do uso de equipamentos IoT em diversas áreas como a indústria, principalmente após o surgimento da indústria 4.0, saúde, educação e urbano (cidades, casas e veículos inteligentes) favorecendo o desenvolvimento econômico, sustentabilidade e qualidade de vida.

Uma pesquisa divulgada pela Cisco (2020) prevê que a IoT movimentará cerca de US$ 19 trilhões até 2023, desses a América Latina será responsável por US$ 860 bilhões e o Brasil US$ 352 bilhões, esses dados comprovam que o setor vem crescendo muito rapidamente em todo o mundo.

De acordo com o Relatório Anual da Internet da Cisco (2020) aplicativos domésticos, como automação residencial, segurança doméstica e vigilância por vídeo, produtos da linha branca e aplicativos de rastreamento, representarão 48% do total de conexões M2M[1] (*Machine to Machine*) até 2023, com um CAGR (Taxa de Crescimento Anual Composta, do inglês *Compound Annual Growth Rate*) de 20% (Figura 2).

Figura 2- Crescimento global da conexão M2M por setores




**Fonte:** Cisco, 2020.

Os dados apresentados na Figura 2 demonstram a universalidade da Internet das coisas, devido a capacidade de se adaptar a várias realidades, auxiliando na evolução da humanidade a partir das decisões ou informações tomadas pela IoT.

Com os avanços tecnológicos e a adoção gradual de tecnologias de IoT foi possível o desenvolvimento de novos sistemas de informação e comunicação,

[1]Categoria de conexões M2M (que também é chamada de IoT)

porém juntamente com esses progressos há novos obstáculos como conectar a Internet à objetos com algumas limitações no âmbito tecnológico, como processamento, comunicação, memória e armazenagem de energia (LOUREIRO *et al*. 2003 *apud* SILVA; MUSSOLINE, 2019, p. 9)

Em geral, a Internet das coisas está cada vez mais presente no mundo, sendo possível notar seus reflexos em diversos setores da sociedade; na economia possibilitando ganhos de produtividade e crescimento econômico; na indústria facilitando processos; medicina, educação, entre outros, e haverá um grande crescimento nos próximos anos devido a chegada do 5G e mudanças nos sistemas trabalhistas, organizações e comunidades que se tornarão mais inteligentes e autônomos.

## 2.3 Indústria 4.0

Diante do crescente surgimento de novas tecnologias no mercado, o setor industrial precisou passar por modernização, mudando modelos de trabalho e processos, baseando-se em digitalização, distribuição e integração de dados. Essas mudanças abrangem um enorme sistema de tecnologias avançadas e é chamado de indústria 4.0 ou também Quarta Revolução Industrial.

"A Quarta Revolução Industrial, promoveu a integração de sistemas ciberfísicos, fundindo o real com o virtual e conectando sistemas digitais, físicos e biológicos, além de possibilitar a produção personalizada em massa" (SCHWAB, 2016 *apud* FERREIRA, 2020, p. 10).

A indústria 4.0 é uma realidade e as organizações que visam esse modelo precisam promover a digitalização das atividades para obterem sucesso em operações avançadas, ou seja, precisam investir em recursos que envolvem automação industrial e integração de diferentes tecnologias como IoT, Inteligência artificial, computação em nuvem, entre outros.

Segundo a IDC Brasil (2022) em 2022 o mercado brasileiro tem que conciliar a transformação digital e inovação, sempre atento a redução de custos, pois está em alta aplicações de IoT com objetivo de aumentar a eficiência e produtividade.

Contudo, juntamente com esses avanços há também o aumento de riscos de ataques cibernéticos nas operações industriais. A empresa de cibersegurança norte-americana Nozomi Networks avaliou as tendências e os principais pontos de

vulnerabilidade nas indústrias 4.0 e identificou que estas devem se preparar para novos tipos de ameaças aos ativos e operações.

“A quarta revolução industrial e a transformação acelerada pela pandemia estão a impulsionar a convergência entre TI e OT[1]. Os ambientes OT incluem, agora, mais tecnologia pronta a usar, incluindo máquinas TI e dispositivos IoT.” (NOZOMI NETWORKS, 2021, p. 5)

As mudanças que ocorreram no Brasil e no mundo a partir de 2020 por conta da Covid-19, também tiveram grande influência nesses ambientes, pois com a adoção de escolas e trabalhos remotos dezenas de milhões de dispositivos IoT foram conectados a redes corporativas, abrindo novas brechas para a exposição dos dados.

Segundo Chris Sherman, analista sênior da Forrester[2], em 2020 ocorreu um episódio em que cibercriminosos atacaram o executivo de uma empresa de serviços financeiros que trabalhava em casa. Os criminosos tentavam controlar o microfone do MacBook, porém não obtiveram sucesso.

Diante disso, os criminosos mudaram os planos e localizaram e invadiram um alto-falante inteligente conectado à rede doméstica via Bluetooth, dessa forma conseguiram atingir seu objetivo final, espionando as conversas do diretor e obtendo informações sobre a organização.

Este é só um dos tipos de ataques IoT que podem ocorrer, atualmente os dispositivos IoT estão presentes nos mais variados ambientes, nas casas, rastreadores de saúde, câmeras de segurança, carros conectados dentre tantos outros. Sendo assim, os ataques continuarão explorando diversos transmissores.

Segundo Luciano Saboia (2022), gerente de pesquisa e consultoria de telecomunicações da IDC Brasil, o crescente aumento do uso de IoT no Brasil e o surgimento de novas tecnologias, como por exemplo o 5G, trará mais eficiência e melhorias de um produto ou serviço, no entanto também aumentará ainda mais o uso de dados em tempo real, visto que gera um grande volume de dados, fornecendo todo tipo de informação, expondo a privacidade do usuário.

---

[1] *Operational technology* tradicionalmente associado a ambientes de manufatura e industriais, inclui sistemas de controle industrial, como controle de supervisão e aquisição de dados.

[2] Forrester é uma empresa norte-americana de pesquisa de mercado que presta assessoria sobre o impacto existente e potencial da tecnologia para seus clientes e o público.

## 2.4 Automação residencial

Automação residencial, também conhecida como domótica, é a integração e interação de dispositivos eletrônicos e tecnologias (conjunto de *hardwares* e *softwares*) interligados entre si através de uma rede de comunicação. Pode ser aplicada em diversas áreas como, climatização, iluminação, segurança, entretenimento, etc., e tornam o controle da residência mais seguro, prático, confortável e econômico.

Segundo Bolzani (2004):

> A automação residencial pode ser definida como um conjunto de tecnologias que ajudam na gestão e execução de tarefas domésticas cotidianas. A sua utilização tem por objetivo proporcionar um maior nível de conforto, comodidade e segurança além de um menor e mais racional consumo de energia.

As instalações de uma *smart home* (casa inteligente) exigem diversos elementos envolvidos, podendo ser controladas por interfaces simples, com ou sem fio, até centrais de automação mais complexas. Os elementos básicos de uma automação residencial são: controladores, sensores, atuadores, barramentos e interfaces.

Os controladores monitoram as informações dos sensores e das interfaces de entrada, enviando comandos para que o atuador ative ou desative algum comando (ACCARDI; DODONOV, 2012).

De acordo com Almeida (2009 *apud* ACCARDI; DODONOV, 2012, p. 157), responsáveis por detectar estímulos, os sensores medem e monitoram grandezas físicas e os convertem em valores computacionais (dados), são eles que encaminham informação sobre algum evento aos controladores.

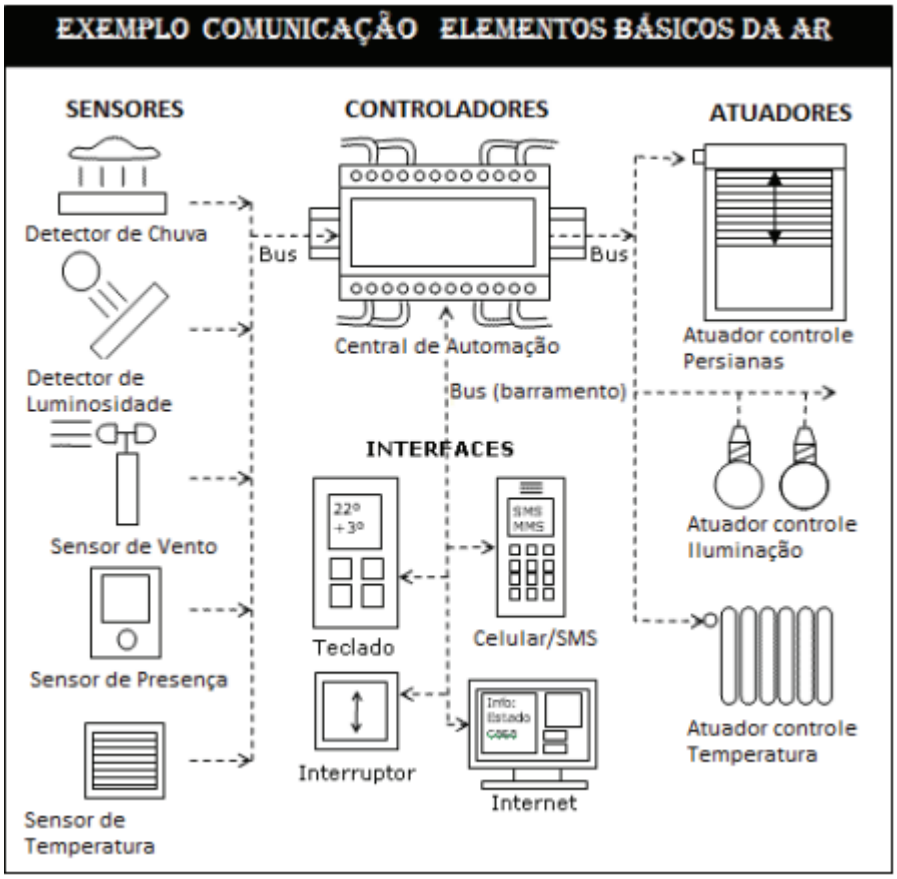
Os atuadores são dispositivos eletromecânicos, que recebem os comandos e ativam os equipamentos automatizados, são módulos ligados entre os equipamentos e a rede elétrica (ALMEIDA, 2009 *apud* ACCARDI; DODONOV, 2012).

Já o barramento é o meio físico responsável pelo transporte das informações (rede elétrica, telefônica, etc). (CASADOMO, 2010 *apud* ACCARDI; DODONOV, 2012, p.157). Podendo ser utilizados barramentos com ou sem fio.

Por último, as interfaces são os dispositivos que permitem ao usuário visualizar informações e interagir com o sistema de automação, podendo ser um controle, um celular, um computador, entre outras coisas (BOLZANI, 2004).

A Figura 3 apresenta um exemplo de como esses elementos se comunicam.

Figura 3- Exemplo de comunicação dos elementos básicos da automação residencial




**Fonte:** Accardi, Dodonov, 2012.

Freitas *et. al* (2010, p.2) afirmam que:

> Essa interação acontece devido aos microprocessadores cada vez mais presentes em dispositivos que fazem parte do cotidiano das pessoas, realizando assim, de maneira automática, tarefas rotineiras, tendo como base para atuação o comportamento previsível do usuário ou a partir de uma programação prévia.

Referindo-se a sistemas inteligentes, pode-se destacar ainda sistemas mais robustos que utilizam algoritmos de inteligência artificial baseados em conhecimento (NIKOLAOS, 2005 *apud* FREITAS et al, 2010, p.3), resolução de problemas, conhecimento incertos e raciocínio, formas e métodos de aprendizagem, comunicação, percepção e ação (RUSSEL; NORVIG, 2003).

Na automação residencial, existem diferentes formas de arquitetura, sendo as mais utilizadas a arquitetura centralizada e a descentralizada.

Em sistemas de arquitetura centralizada todos os dispositivos respondem a um dispositivo central dotado de inteligência e desempenho suficientes para receber e tratar as informações recebidas dos sensores e enviar os comandos aos atuadores (ALMEIDA, 2009 *apud* ACCARDI; DODONOV, 2012). Esta arquitetura reduz o custo, mas aumenta a complexidade do sistema.

No modelo de arquitetura descentralizada, podem existir vários controladores interligados por um barramento, que compartilham a administração dos sensores, atuadores e interfaces (CASADOMO, 2010 *apud* ACCARDI; DODONOV, 2012). Este modelo facilita a instalação e a interação com o usuário, no entanto se torna mais caro devido ao número de equipamentos utilizados e deixa o sistema mais imune a falhas.

A automação residencial utiliza vários elementos de maneira integrada, unindo os benefícios dos meios eletrônicos aos informáticos, obtendo assim uma gestão integrada de diversos equipamentos de uma casa. Um dos principais benefícios da domótica é a possibilidade de integrar sistemas, permitindo que tarefas rotineiras sejam realizadas automaticamente e de acordo com as necessidades, possibilitando a manipulação de forma manual ou automatizada.

## 2.5 Casas inteligentes

Conhecida como *smart home*, casa conectada ou casa automatizada, uma casa inteligente é equipada com tecnologias que proporcionam maior segurança, praticidade, comodidade e economia.

Aldrich (2003 *apud* REBOUÇAS, 2020, p.7), define casa inteligente como uma residência equipada com informática e tecnologia da informação, que antecipa e responde às necessidades dos ocupantes, trabalhando para promover seu conforto, conveniência, segurança e entretenimento por meio do gerenciamento de tecnologia em casa e conexões com o mundo.

Uma casa inteligente funciona com o uso de IoT, que permite a conexão de diversos dispositivos a um servidor comum, onde ocorrem as automações. Essa tecnologia possibilita maior facilidade no dia a dia, automatizando atividades e tarefas, tornando a rotina mais simples e eficiente.

Os dispositivos podem coletar e armazenar informações, hábitos e preferências do dispositivo ou toda a rede e serem controlados a distância ou até mesmo por comando de voz.

Alguns dos dispositivos mais utilizados em casas inteligentes são lâmpadas inteligentes, eletrodomésticos e fechaduras inteligentes (controle de acesso), assistente virtual (*smart speaker*), câmeras de segurança, entre outros.

As lâmpadas inteligentes possibilitam o agendamento de horário em que as luzes devem ligar ou desligar, selecionar nível de luz, entre outras funções. Os controles de acesso utilizando fechaduras inteligentes permitem controlar o trancamento e destrancamento das portas, autorizar entrada, horários e alertas.

Com o uso de câmeras de segurança conectadas é possível controlar, monitorar e realizar ações a distância. Os assistentes virtuais que são ativados por comandos de voz, facilitam a realização de atividades diárias. Podem ser sincronizados a outros dispositivos e realizarem ações como tocar música, fazer pesquisas, ligar e desligar aparelhos, etc.

Os eletrodomésticos inteligentes beneficiam o dia a dia, pois a partir deles é possível controlar quando estão e/ou serão ligados e auxiliar na redução do consumo de energia.

Assim como qualquer ambiente *online*, as *smart homes* apresentam várias ameaças à segurança, principalmente no que diz respeito a coleta de dados, pois armazena preferências dos moradores, hábitos, consumos, rotinas e tantas outras informações que se chegarem até pessoas mal-intencionadas, tornam o usuário vulnerável.

Em debate sobre cidades inteligentes, o Diretor Global de Crescimento, Inovação e Insight da Aon, David Bowcott explica: "Se não estiverem devidamente protegidos, esses ativos físicos agora conectados – quase vivos – podem ser usados como armas”.

De fato, uma casa inteligente traz grandes benefícios e vantagens na rotina das pessoas, no entanto é necessário se atentar sempre aos possíveis problemas de segurança.

## 2.6 Vulnerabilidades de dispositivos IoT

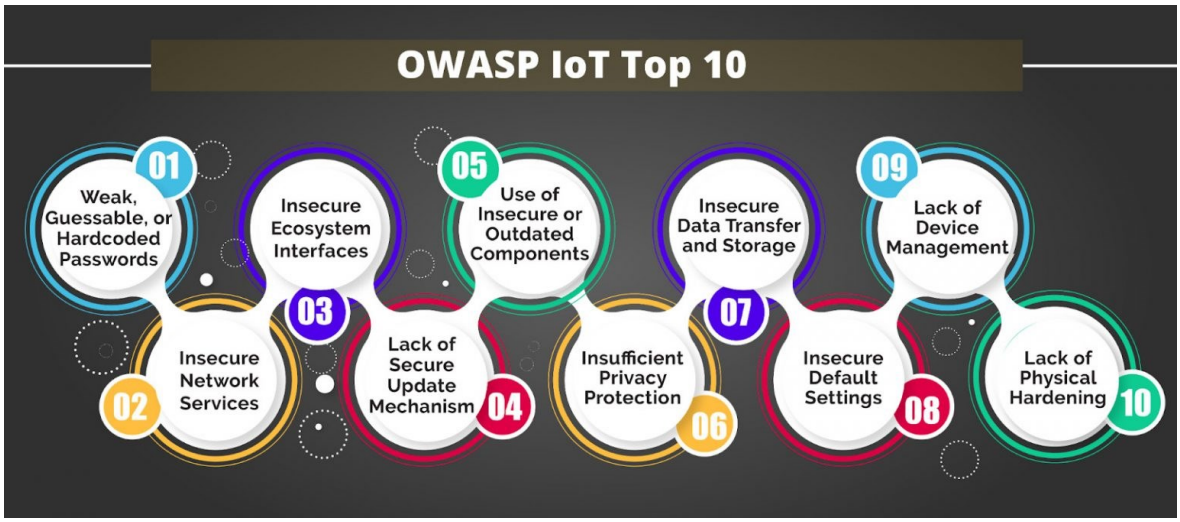
Os dispositivos IoT são muito recentes e ainda não há um mapeamento significantes das vulnerabilidades, consequentemente muitos ataques, até mesmo os mais básicos, acontecem em redes formadas por estes dispositivos.

De acordo com Zani (2016):

> Os dispositivos de Internet das Coisas muitas vezes não são projetados para a segurança. [...] A proliferação de novos dispositivos, a baixíssima preocupação com segurança e alto valor dos dados contidos nesses objetos farão com que os ataques cibernéticos visando esses dispositivos cresçam de forma abundante.

Em 2018, o Open Web Application Security Project (OWASP), organização sem fins lucrativos que tem a contribuição de milhares de especialistas em desenvolvimento e segurança, realizou um estudo titulado de "*Top Ten – Internet of Things*" onde foram definidas as dez principais vulnerabilidades presentes em dispositivos IoT, conforme apresentado na Figura 4.

Figura 4- OWASP Top 10 - Internet of Things




**Fonte:** OWASP, 2018.

A lista das principais vulnerabilidades tem como base a gravidade da vulnerabilidade, facilidade de exploração e magnitude dos impactos.

1- Senhas fracas e *hardcoded*: as aplicações permitem senhas fracas sem requisitos mínimos ou mantém padrões de senhas para todos os dispositivos, muitas vezes não exigindo alterações de senhas. Esses

padrões são favoráveis a ataques e em casos de senhas padrão podem possibilitar o acesso não autorizado a demais dispositivos.

2- Serviços de rede inseguros: os serviços de rede executados nos dispositivos representam uma ameaça à confidencialidade e integridade do dispositivo, pois muitas vezes são desnecessários e possuem portas abertas permitindo o acesso remoto não autorizado e vazamento de dados.
3- Interfaces de ecossistema inseguras: várias interfaces como a interface da *web* e *mobile*, API e a nuvem que permitem a interação podem apresentar falhas de autenticação, criptografia ruim e falta de filtragem nas entradas e saídas.
4- Falta de mecanismos de atualização seguros: incapacidade de atualizar o dispositivo com segurança devido à falta de validação de *firmware*, transferência de dados não criptografada, falta de notificações de alterações de segurança devido atualizações podem comprometer a segurança dos dispositivos.
5- Uso de componentes inseguros ou desatualizados: uso de *hardware* e *software* de terceiros obsoletos e inseguros que podem comprometer o dispositivo e interromper seu bom funcionamento.
6- Proteção de privacidade insuficiente: os dados de usuário são armazenados no dispositivo de forma insegura e sem permissão, o que pode levar ao vazamento de dados críticos se invadidos por cibercriminosos.
7- Transferência e armazenamento de dados inseguros: falta de controle de acesso e criptografia na transmissão e armazenamento de dados. Os dados podem ser expostos em várias fases incluindo em repouso, em trânsito ou durante o processamento, o que dá oportunidade para que os dados sejam roubados e expostos.
8- Configurações padrão inseguras: falta de segurança nas configurações padrão dos dispositivos, restringindo que o usuário faça as modificações e os tornem mais seguros.

9- Falta de gerenciamento dos dispositivos: incapacidade de proteger todos os dispositivos implantados na rede, incluindo falta de monitoramento, manutenção e atualização.

10- Falta de proteção de acesso físico: não permite desativar interfaces de *debug* ou desenvolvimento, permitindo que *hackers* adquiram informações que podem facilitar um ataque remoto ou assumir o controle do dispositivo.

De acordo com o Relatório do McAfee Labs sobre ameaças de abril de 2017, os fabricantes de IoT precisam alcançar segurança nas interfaces, arquitetura e nos projetos dos produtos, pois estes serão cada vez mais poderosos e irão armazenar muitos dados.

## 2.7 Ataques a dispositivos IoT

Diante de tantas vulnerabilidades identificadas, há grandes possibilidades de uma ameaça encontrar brechas no dispositivo e comprometer sua segurança.

“Dentre as ameaças à segurança que tais sistemas estão sujeitos está a espionagem, vazamento de informações, ataques coordenados de negação de serviço (DDoS), acesso de pessoal não autorizado, etc.” (RAZZAQ *et al.,* 2017).

Segundo relatório divulgado pela empresa de cibersegurança NSFOCUS Security Labs (2020), especializado na descoberta e análise de ameaças, em 2020 o Brasil esteve entre os dez países mais visados em termos de ataques a dispositivos IoT.

Conforme o Relatório de Ameaças Cibernéticas da SonicWall Capture Labs (2019), as principais ameaças e ataques que podem ocorrer contra dispositivos IoT são:

- *Distributed Denial of Service* (DDoS): esse tipo de ataque tem como objetivo tornar algum serviço indisponível enviando diversas requisições desnecessárias, consumindo todo o poder de processamento do dispositivo, sobrecarregando o sistema e impedindo as requisições efetivas.
- Aumento de privilégios: explora vulnerabilidades de sistemas operacionais ou *softwares* para elevar o acesso de um usuário, obtendo privilégios que não lhe foram concedidos, dessa forma o agente malicioso pode usar desse

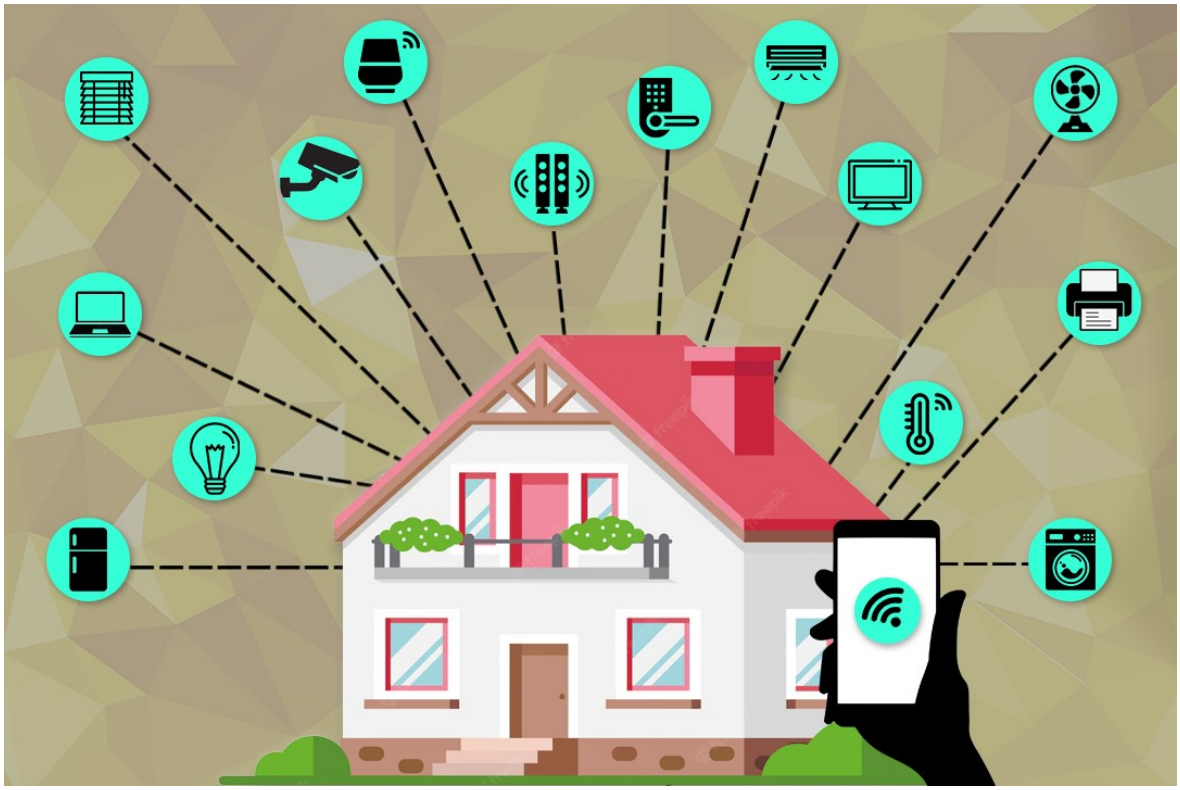
fato para obter informações privadas, instalar algum vírus, modificar ou deletar arquivos.

- Explorabilidade: esses ataques ocorrem principalmente através do protocolo TCP/IP Telnet, onde os agentes maliciosos escaneiam a Internet em busca de portas Telnet abertas. Além disso, cibercriminosos buscam também portas não padrão para o tráfego da *web*.
- Atualizações de *firmware:* como muitos dispositivos não verificam a integridade do *firmware* antes de atualizá-lo, isso pode abrir portas para uma versão desatualizada ou um código malicioso.
- Infecções por *malware*: os ataques por *malware* ou *software* malicioso obtém acesso ao dispositivo, monitora o usuário e captura dados. Geralmente esses ataques são favorecidos por credenciais fracas.
- *Ransomware*: é um tipo de *malware* que criptografa áreas de armazenamento do dispositivo tornando os dados inacessíveis.

## 3 Desenvolvimento

O ecossistema de uma *smart home* pode ser composto por diversos dispositivos, que variam de acordo com a necessidade e rotina de cada usuário. Foi elaborado o ambiente de uma casa inteligente, conforme Figura 5, que possui lâmpadas, fechaduras e cortinas inteligentes, câmeras de segurança, *smart TV*, *notebook*, impressora*, home theater*, máquina de lavar, geladeira, ar-condicionado, ventilador, termostato e *smart speaker* conectados.

Figura 5- Casa inteligente



**Fonte:** Elaborado pelo autor, 2022.

Em seguida, foram propostos três cenários para o mesmo ambiente, e como são tratados os dispositivos em casos de alta, baixa e média segurança.

Os dispositivos de uma casa inteligente precisam ser conectados à rede, para que comuniquem com a central e também entre si. A rede *wi-fi*, onde grande parte dos dispositivos são conectados, precisa ser protegida ou informações privadas poderão ser exploradas. Devido a isso, os critérios utilizados para definir

a segurança do ambiente, foram os princípios básicos da segurança da informação: confidencialidade, integridade e disponibilidade.

Para reforçar a confidencialidade do ecossistema é de grande valia a adoção de medidas preventivas, como a definição de acesso somente a pessoas autorizadas, implantação de sistemas de criptografia, autenticação de múltiplos fatores, definição de permissões de acesso, etc., garantindo, portanto, que somente pessoas autorizadas tenham acesso a rede onde são transmitidos os dados dos usuários.

O critério da integridade é crucial para que os dados circulem e sejam armazenados do mesmo modo como foram criados, sem interferência externa que possa comprometer, corromper ou danificar os dados. Pensando nisso, um ambiente deve adotar precauções para que nenhuma informação seja modificada sem autorização.

A disponibilidade está relacionada à acessibilidade dos dados, ou seja, se estes podem ser acessados a qualquer momento. Por essa razão, a manutenção e preservação do acesso aos dados é fundamental, deve-se manter os equipamentos (*hardware*) e *softwares* sempre ativos e assegurar que atualizações periódicas estejam instaladas.

Desse modo, configura-se um ambiente de alta segurança aquele que atende todos os requisitos de segurança, onde são aplicadas boas práticas para instalação, parametrização e uso dos dispositivos IoT, melhorias no ecossistema como um todo e configuração e segmentação de rede. Esse ambiente possui auditoria, correções, verificações de riscos e controles para manter a constância no processo de melhoria e privacidade.

O ambiente de média segurança possui os requisitos de segurança, porém estes não são atribuídos ao ambiente em sua totalidade e não passam por análise frequente, ou seja, podem até serem ambientes seguros quando configurados inicialmente, mas com o decorrer do tempo não há uma prática de checagem frequente.

Por fim, é caracterizado como baixa segurança o ecossistema que não possui nenhuma política de segurança e análise de vulnerabilidades presentes nos dispositivos e no tráfego de dados, aquele em que a única medida tomada é a inclusão de um dispositivo na rede.

## 3.1 Alta segurança

Cada dispositivo IoT conectado é um coletor de dados, consequentemente em um ambiente de alta segurança a primeira medida tomada é a alteração de nomes de usuário e senha dos dispositivos, por senhas fortes que possuam combinação de letras, números e símbolos. Além disso, são mantidos padrões de senhas distintos, que tornam mais difícil para um *hacker* ampliar sua presença na rede em caso de ataques.

Igualmente, deve ser ativado no roteador o protocolo de segurança criptografado que protege o tráfego de redes sem fio, o WPA2 (*Wi-Fi Protected Access 2*) e criadas redes separadas, sendo uma para uso pessoal, onde são realizadas compras e transações bancárias por exemplo, e outra para conectar os dispositivos inteligentes. Com isso, caso sejam identificadas vulnerabilidades a rede não possibilitará acesso a informações sensíveis.

Em um ecossistema otimista, os sistemas operacionais, *softwares* e aplicativos utilizados sempre são atualizados com as últimas versões e correções disponíveis, pois maior parte das atualizações são disponibilizadas devido a falhas de segurança encontradas e exploradas em versões anteriores. Da mesma forma, são analisadas algumas questões antes mesmo da aquisição dos dispositivos, buscando os mais atuais e que possuem melhor tecnologia, estrutura e segurança, já que dispositivos mais antigos tendem a ser mais vulneráveis.

Para manter a alta segurança, são verificadas as configurações padrão de segurança e privacidade. Em dispositivos que possuem controle por voz é feito uma análise sobre a importância do recurso, em caso de não utilização eles são desativados, impedidos que conversas sejam ouvidas e registradas. Deve-se também analisar a funcionalidade *Plug and play universal*[1] (UpnP) no dispositivo e desligar a mesma, pois é um grande risco de segurança já que isto permite que os dispositivos se identifiquem e conectem automaticamente uns aos outros.

Para impedir que usuários mal-intencionados se conectem, os dispositivos que não estão em uso, principalmente aqueles que possuem microfones e câmeras, devem ser desligados. Em alguns casos, como os termostatos

[1] *Plug and play* ("Ligar e usar") protocolo de Internet definido principalmente para redes domésticas, permitindo que dispositivos se conectem à rede automaticamente.

inteligentes, requerem conexão constante à Internet, porém outros como TVs, cafeteiras, etc., não há necessidade.

Como quase todos os dispositivos IoT são controlados por aplicativos do *smartphone*, os aparelhos se tornam alvo para entrada em casas inteligentes, portanto é importante proteger o aparelho e ler as Políticas de Privacidade dos aplicativos que controlam uma *smart home*, para identificar quais os dados este terá acesso, quais serão coletados e o que será feito com essas informações e aplicar medidas de segurança para limitar acesso a determinadas informações. Essas políticas geralmente são disponibilizadas na página de detalhes dos aplicativos, tanto na *Google Play* (para dispositivos *Android*) quanto na *APP Store* (nos dispositivos iOS).

## 3.2 Média segurança

Diferente de um ambiente altamente seguro, em uma casa conectada com média segurança os dispositivos muitas vezes são configurados com novos nomes de usuário e senha, com a intenção de aumentar a segurança, porém para todos são mantidos os mesmos padrões. Dessa forma, caso um ataque seja realizado, todos os dispositivos serão acessados.

Os dispositivos são conectados a uma única rede, onde ficam conectados os demais equipamentos e o acesso de visitantes é permitido. Estas atitudes, no entanto, não são apropriadas, pois muitos dispositivos têm pontos de acesso completamente abertos, permitindo que qualquer pessoa com acesso à rede *wi-fi* tenha controle de dispositivos vulneráveis, aumentando a possibilidade de ataques e a captura de dados trafegados na rede.

Em câmeras de segurança, as ameaças são ainda maiores, pois implica na captura de imagens geradas e transmitidas pela Internet.

Um ambiente realista que possui média segurança, não possui atualizações constantes, isto é, muitas vezes os dispositivos e *softwares* vão ficando obsoletos e não passam por atualizações, isso porque geralmente não há uma análise periódica dos dispositivos e *firmwares* e não existe um planejamento para a aquisição de novos dispositivos mais modernos e seguros.

Como há vulnerabilidades nos ambientes inteligentes e muitas possibilidades de acesso, junto a todo cuidado relacionado a rede são necessários

cuidados ao acessar os dispositivos remotamente através do *smartphone*, não utilizando conexões *wi-fi* que não sejam protegidas por senha e verificando se o ambiente digital é seguro.

## 3.3 Baixa segurança

Na contramão de um ambiente seguro, existem os casos em que nenhuma ação de segurança é tomada. Nesses ecossistemas de baixa segurança os dispositivos geralmente são conectados a uma rede *wi-fi* que não passou por nenhuma configuração de segurança e muitas vezes os IoT's são reconhecidos e conectados diretamente através do protocolo *Plug and play universa*l, sem que sejam feitas as devidas validações e atualizações de segurança.

Outra ação, muito necessária, mas geralmente não realizada em ambientes pessimistas são as atualizações dos dispositivos. Muitos aparelhos inteligentes fazem atualizações automaticamente, enquanto outros necessitam que o usuário se certifique e os mantenha atualizados.

Mesmo em ambientes de baixa segurança é fundamental manter a preocupação com o acesso remoto e utilizar somente aplicativos legítimos de dispositivos inteligentes, além de revisar as permissões antes de instalá-los no *smartphone*, isso porque com aplicativos seguros é possível impedir que aplicativos ou códigos maliciosos sejam executados.

# 4 Conclusão

Neste trabalho, foram identificadas e analisadas vulnerabilidades em dispositivos IoT utilizados em casas inteligentes, que estão sujeitas a múltiplas ameaças devido ao seu ecossistema. Essas ameaças, podem encontrar brechas nos dispositivos conectados e comprometer toda a segurança, colocando em risco não somente os dados pessoais do usuário, mas também sua habitação.

Por mais que pequenas ações de segurança sejam tomadas em um ambiente conectado, estas ainda não são suficientes para torná-lo altamente seguro, principalmente quando muitos dispositivos são conectados a uma rede padrão.

Através da análise do ambiente de uma *smart home*, foram atribuídos níveis de segurança baseados em diversas medidas e padrões que devem ser seguidos e revisados constantemente para que o ecossistema esteja sempre protegido e atualizado.

Após o estudo, pode-se afirmar que muitas falhas vêm sendo identificadas e corrigidas através de atualizações e melhorias dos dispositivos, no entanto, ainda existem vulnerabilidades que podem ser corrigidas por fabricantes antes mesmo de serem adquiridos pelos consumidores e é fundamental que os usuários tomem ações para tornar a casa inteligente ainda mais segura.

**Referências**

ACCARDI, Adonis. DODONOV, Eugeni. Automação residencial: elementos básicos, arquiteturas, setores, aplicações e protocolos. **Revista T.I.S. - Tecnologias, Infraestrutura e Software**, São Carlos, v. 1, n. 2, p. 156-166, nov. 2012. Disponível em: http://professor.pucgoias.edu.br/SiteDocente/admin/arquivosUpload/17829/material/ARTIGO02.pdf. Acesso em: 07 mar. 2022.

ACOHIDO, Byron. **Ataques a dispositivos inteligentes (IoT) registram alta com a Covid-19**. Avast, fev. 2021. Disponível em: https://blog.avast.com/pt-br/iot-attacks-intensified-by-covid-19-avast. Acesso em: 12 out. 2022.

AON. The One Brief. **Equilibrando risco e benefício:** O Surgimento de Cidades Inteligentes. Disponível em: https://theonebrief.com/latam/portugues/post/equilibrando-risco-e-beneficio-o-surgimento-de-cidades-inteligentes/. Acesso em: 14 out. 2022.

ASHTON, Kevin. **That 'Internet Of Things' Thing.** RFID Journal, 2009. Disponível em: http://www.rfidjournal.com/articles/view?4986. Acesso em: 29 abr. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. **NBR/ISO/IEC 27002:** Tecnologia da informação - Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2007.

BARROS, Emerson. **Estudo de vulnerabilidades em dispositivos IoT TCP/IP**. 2021. 60f. Trabalho de Conclusão de Curso - Universidade Federal do Rio Grande do Sul, Porto Alegre, 2021. Disponível em: https://www.lume.ufrgs.br/bitstream/handle/10183/222479/001126492.pdf?sequence=1. Acesso em: 07 mar. 2022.

BOLZANI, Caio Augusto. M. **Residências Inteligentes**. [S.l.]: Livraria da Física, 2004.

CISCO. **Cisco Annual Internet Report (2018–2023) White Paper**. Disponível em: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. Acesso em: 23 maio. 2022.

Cisco Systems. **The Internet of Everything Cisco IoE Value Index Study**. 2013. Disponível em: https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-index-faq.pdf. Acesso em: 21 maio. 2022.

COSTA, Luís Carlos G. **Vulnerabilidades em Dispositivos IoT para Ambiente Smart Home**. 2018. 175f. Dissertação de Mestrado em Engenharia de Segurança Informática - Escola Superior de Tecnologia e Gestão. 2018. Disponível em: https://repositorio.ipbeja.pt/bitstream/20.500.12207/4827/1/Dissertacao_Luis_Costa_PDFA.pdf. Acesso em: 07 mar. 2022.

FERREIRA, André Luiz**. Proposta de modelo de gestão para implantação de casas inteligentes com foco nos eixos da indústria 4.0**. 66f. Trabalho de Conclusão de Curso - Faculdade de Tecnologia e Ciências Sociais Aplicadas – Centro Universitário de Brasília. Brasília, 2020. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/prefix/15109/1/Andr%c3%a9%20Ferreira%20-TCC%20VF.pdf. Acesso em: 14 out. 2022.

FERREIRA, F.N.F; ARAÚJO, M. T. **Políticas de Segurança da Informação – Guia prático para elaboração e Implementação**.2 ed. Rio de Janeiro: Ciência Moderna, 2008.

FONTES, Edison. **Segurança da Informação:** O usuário faz a diferença. São Paulo: Saraiva, 2010.

FREITAS, Claudio; MESQUITA, Brehme de; PEREIRA, Carlos; FARIAS, Valcir. **Automação residencial – uma abordagem em relação as atuais tecnologias e perspectivas para o futuro**. Nov. 2010. 8f. V Congresso Norte-Nordeste de Pesquisa e Inovação. Disponível em: https://www.researchgate.net/publication/236679669. Acesso em: 04 maio 2022.

FUKUDA, Leonardo Massami. **Segurança da Informação em IoT**. 41f. Monografia MBA em Gestão da Tecnologia da Informação e Comunicação - UTFPR. Curitiba, 2019. Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/19442/2/CT_GETIC_VIII_2019_05.pdf. Acesso em: 08 mar. 2022.

GARTNER. **Gartner Glossary.** [S.l.: s.n.], 2021. Disponível em: https://www.gartner.com/en/information-technology/glossary/Internet-of-things. Acesso em: 03 maio 2022.

IDC. IDC Media Center. **Previsões da IDC para 2022 apontam crescimento de 8,2% para o mercado de TIC no Brasil**. Fev. 2022. Disponível em: https://www.idc.com/getdoc.jsp?containerId=prLA49041022. Acesso em: 12 out. 2022.

MCAFEE**. Proteção de dispositivos IoT como defesa contra ataques – Resumo de solução**. Abr. 2017. Disponível em: https://www.mcafee.com/enterprise/pt-br/assets/solution-briefs/sb-quarterly-threats-mar-2017-1.pdf. Acesso em: 12 out. 2022.

NOZOMI NETWORKS. **Relatório de segurança OT/IoT**. O que precisa de saber para combater o ransomware e as vulnerabilidades da IoT. Jul. 2021. Disponível em: https://www.nozominetworks.com/downloads/PT/NN-OT-IoT-Security-Report-2021-1H-ES-PT.pdf. Acesso em: 14 out. 2022.

NSFOCUS. **Cybersecurity Insights.** 2020. Disponível em: https://nsfocusglobal.com/wp-content/uploads/2021/06/2020-NSFOCUS-Cybersecurity-Insights.pdf. Acesso em: 25 out. 2022.

OWASP. **Internet of Things - Top 10.** 2018. Disponível em: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf. Acesso em: 25 out. 2022.

RAZZAQ, Mirza A., GILL, Sajid H., QURESHI, Muhammad A., ULLAH, Saleem. Security Issues in the Internet of Things (IoT): A Comprehensive Study, **International Journal of Advanced Computer Science and Applications**, Vol. 8, No. 6, p. 383 a 388, 2017. Disponível em: https://thesai.org/Downloads/Volume8No6/Paper_50-Security_Issues_in_the_Internet_of_Things.pdf. Acesso em: 22 out. 2022.

REBOUÇAS, Eduardo P., **Análise do Mercado de Casas Inteligentes no Brasil:** Uma Pesquisa Exploratória por meio de Surveys. Dissertação de Mestrado em Gestão e Tecnologia Industrial. Centro Universitário SENAI CIMATEC. 2020. Disponível em: http://repositoriosenaiba.fieb.org.br/bitstream/fieb/1099/1/TCCP_GETEC_Eduardo%20Pimentel%20Rebou%C3%A7as.pdf. Acesso em: 07 mar. 2022.

RUSSEL, S., NORVIG, P. **Inteligência Artificial**. Segunda edição. 2 ed. Elsevier, 2003.

SANTOS, Bruno P.; SILVA, Lucas A. M.; CELES, Clayson S. F. S.; BORGES, João B.; PERES, Bruna S.; VIEIRA, Marcos A. M.; VIEIRA, Luiz F. M.; GOUSSEVSKAIA, Olga N.; LOUREIRO, Antonio A. F. **Internet das Coisas:** da Teoria à Prática**.** Minas Gerais: Departamento de Ciência da Computação, 2016. Disponível em: Https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/Internet-das-coisas.pdf. Acesso em: 08 mar. 2022.

SÊMOLA, Marcos. **Gestão da segurança da informação:** uma visão executiva. - 2. ed. - Rio de Janeiro: Elsevier, 2014.

SILVA, Cleber J. R. da; MUSSOLINE, Michel**. Implementação da tecnologia Internet das coisas na iluminação pública**. 2019. 24f. Trabalho de Conclusão de Curso - Centro Universitário Uniamérica. Foz do Iguaçu, 2019. Disponível em: https://pleiade.uniamerica.br/index.php/bibliotecadigital/article/download/558/667. Acesso em: 21 maio. 2022.

SONICWALL. **Cyber Threat Report**. Mid-Year Update, 2022. Disponível em: https://www.sonicwall.com/2022-cyber-threat-report/. Acesso em: 25 out. 2022.

Telecommunication Standardization Sector (ITU-T). ITU-T Y.2060: **Overview of the Internet of things.** [S.l: s.n.]. Disponível em: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559. Acesso em: 28 abr. 2022.

ZANI, Bruno. **As vulnerabilidades e necessidades de segurança em IoT**. Set.2016. Disponível em: https://www.securityreport.com.br/overview/mercado/vulnerabilidades-necessidades-seguranca-iot/#.Y0S3F3bMLIV. Acesso em: 10 out. 2022