PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS

CENTRO DE CIÊNCIAS EXATAS, AMBIENTAIS E DE TECNOLOGIAS

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

TIAGO GUIMARÃES MONTEIRO

ANÁLISE DE REQUISITOS DE SEGURANÇA PARA UMA REDE DE IOT

CAMPINAS

2021

TIAGO GUIMARÃES MONTEIRO

ANÁLISE DE REQUISITOS DE SEGURANÇA PARA UMA REDE DE IOT

Dissertação apresentada ao Programa de Pós-Graduação *Stricto Sensu* em Engenharia Elétrica do Centro de Ciências Exatas, Ambientais e de Tecnologias, da Pontifícia Universidade Católica de Campinas, como requisito para obtenção do título de Mestre em Gestão de Redes de Telecomunicações.

Orientadora: Profª. Drª. Lia Toledo Moreira Mota

PUC-CAMPINAS

2021

Ficha catalográfica elaborada por Vanessa da Silveira CRB 8/8423
Sistema de Bibliotecas e Informação - SBI - PUC-Campinas

006.22 Monteiro, Tiago Guimarães
M775a

Análise de requisitos de segurança para uma rede de IOT / Tiago Guimarães Monteiro. - Campinas: PUC-Campinas, 2021.

85 f.: il.

Orientador: Lia Toledo Moreira Mota.

Dissertação (Mestrado em Gestão de Redes de Telecomunicações) - Programa de Pós-Graduação em Engenharia Elétrica, Centro de Ciências Exatas, Ambientais e de Tecnologia, Pontifícia Universidade Católica de Campinas, Campinas, 2021.
Inclui bibliografia.

1. Internet das coisas. 2. Redes de computação - Medidas de segurança. 3. Entropia. I. Mota, Lia Toledo Moreira. II. Pontifícia Universidade Católica de Campinas. Centro de Ciências Exatas, Ambientais e de Tecnologia. Programa de Pós-Graduação em Engenharia Elétrica. III. Título.

CDD - 23. ed. 006.22

TIAGO GUIMARÃES MONTEIRO

ANÁLISE DE REQUISITOS DE SEGURANÇA PARA UMA REDE DE IOT

Dissertação apresentada ao Programa de Pós-Graduação *Stricto Sensu* em Engenharia Elétrica do Centro de Ciências Exatas, Ambientais e de Tecnologias, da Pontifícia Universidade Católica de Campinas, como requisito para obtenção do título de Mestre em Gestão de Redes de Telecomunicações.

Orientadora: Profª. Drª. Lia Toledo Moreira Mota

Dissertação defendida e aprovada em 28 de Janeiro de 2021 pela Comissão Examinadora constituída dos seguintes professores:

Profa. Dra. Lia Toledo Moreira Mota
Orientadora da Dissertação e Presidente da Comissão Examinadora
Pontifícia Universidade Católica de Campinas

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

Prof. Dr. Takao Suguiy
Centro de Tecnologia da Informação Renato Archer - CTI

AGRADECIMENTOS

A PUC-Campinas pela infraestrutura concedida e fornecimento da Bolsa de Estudos e dos equipamentos para realização dos ensaios.

À minha orientadora Professora Dra. Lia Toledo Moreira Mota pela paciência e dedicação na condução deste trabalho.

Ao Prof. Dr David Bianchini pelas orientações iniciais e constante apoio e incentivo.

À minha banca de qualificação composta pelos professores: Prof. Dr. Frank Herman Behrens e Prof. Dr. Marcius Fabius Henriques de Carvalho pelas suas considerações que foram fundamentais ao desenvolvimento deste trabalho.

Aos colegas de Mestrado, pelas conversas, correções e companheirismo ao longo de dois anos de trabalho.

A todos os professores com os quais tive o prazer e gratidão de cruzarem o meu caminho.

Aos meus pais, Donald e Vera, que sempre me apoiaram, incentivaram e investiram em meus estudos.

À minha amada esposa, Natalícia Cristina Ostapenko Monteiro, pela paciência, apoio, companheirismo e tudo o mais. Sem você isso não seria possível.

RESUMO

MONTEIRO, Tiago Guimarães. **Análise de Requisitos de Segurança para uma Rede de IoT**. Dissertação de Mestrado. Programa de Pós-Graduação em Engenharia Elétrica, Pontifícia Universidade Católica de Campinas, Campinas, 2020.

O aumento vertiginoso da quantidade de dispositivos conectados à Internet aliado a popularização das redes IoT propiciaram o nascimento de diversos problemas para todos os usuários e empresas envolvidos com essas redes. O trafego por essas redes têm sido alvo de cobiças, com o intuito de controlar esses dispositivos e muitas vezes usar para ataques aos grandes usuários da rede. Por este motivo diversas leis de proteção de dados pessoais têm sido promulgadas para atribuir responsabilidades, determinar direitos e deveres e garantir a segurança desses dados. O presente trabalho tem como objetivo analisar os requisitos para a gestão segura das redes IoT baseado no uso de senhas seguras que garantam minimamente a segurança delas. Essas senhas deverão ser atribuídas e utilizadas nos roteadores de comunicação com a internet, nos controladores, nos sensores, nos dispositivos inteligentes e demais periféricos conectados nessas redes. Com a revisão da literatura e a realização de testes das senhas, usando aplicativos e sites conhecido de muitos usuários, foram analisados o nível de segurança com o uso de senhas seguras em roteadores. Foram feitos análise de requisitos para a escolha de senhas baseado no aspecto de segurança em sistemas criptográficos que utilizam chaves de criptografia simétricas e ou assimétricas. A heterogeneidade, limitação da capacidade de processamento e energia, diversidade de infraestrutura, integração de diversos fabricantes e alta variabilidade de protocolos faz das redes IoT únicas e por isso necessitam de um cuidado diferenciado para sua segurança. Este trabalho visa conscientizar os usuários das redes IoT da importância da segurança em suas redes de modo que os seus dispositivos não sejam usados de maneira imprópria. O uso de senhas com 20 caracteres e que usem números, letras e caracteres especiais é uma maneira de prover melhor segurança às redes IoT e devem ser usados nos roteadores e demais dispositivos da rede.

Palavras Chaves: IoT. Segurança de Rede IoT. Rede IoT. Entropia. Nível de Segurança. Nível de Força**.**

ABSTRACT

MONTEIRO, Tiago Guimarães. **Security Requirements Analysis for an IoT Network.** Masters Dissertation. Postgraduate Program in Electrical Engineering, Pontifical Catholic University of Campinas, Campinas, 2020.

.
The frantic increase in the number of internet connected devices coupled with the popularization of IoT networks has created several problems for all users and companies involved in these networks. Traffic through these networks has been the target of greed, in order to control these devices and often use them to attack large network users. For this reason, several personal data protection laws have been enacted to assign responsibilities, determine rights and duties and ensure the security of such data. This paper aims to analyze the requirements for the secure management of IoT networks based on the use of secure passwords that minimally guarantee their security. These passwords must be assigned and used on the internet communication routers, controllers, sensors, smart devices and other peripherals connected to these networks. The security level with the use of secure passwords in routers was analyzed by reviewing literature and testing these passwords using applications and websites known to many users. Requirements analysis was performed for the choice of passwords based on the security aspect of cryptographic systems that use symmetric and/or asymmetric encryption keys. The heterogeneity, limitation of the processing and energy capacity, infrastructure diversity, integration of several manufacturers and high variability of protocols make IoT networks unique, therefore needing a differentiated security care. This paper intends to make users of IoT networks aware of the importance of security on their networks so that their devices are not improperly used. The use of passwords with 20 characters and that use numbers, letters and special characters is a way to provide better security to IoT networks and should be the choice in routers and other network devices.

Descriptors: *IoT. IoT Network Security. IoT Network. Entropy, Security Level. Strength Level.*

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

2TDEA = *Two-key Triple Data Encryption Algorithm*
Algoritmo Triplo de Encriptação de Dados com chave dupla

3TDEA = *Three-key Triple Data Encryption Algorithm*
Algoritmo Triplo de Encriptação de Dados com chave tripla

AES = *Advanced Encryption Standard*
Padrão de Encriptação Avançado

ANPD = Autoridade Nacional de Proteção de Dados

API = *Application Program Interface*
Interface de Programação de Aplicações

ASCII = *American Standard Code for Information Interchange*
Código Padrão Americano para Intercâmbio de Informações

CCTA = *Center of Computer and Telecommunications Agency*

CIA = *Confidentiality, Integrity and Avaliability*
Confidencialidade, Integridade e Disponibilidade

ECDSA = *Elliptic Curve Digital Signature Algorithm*
Algoritmo de Assinatura Digital de Curvas Elípticas

GLP = Gás Liquefeito de Petróleo

GSTI = Gerenciamento de Serviço de TI

HTTP = *Hyper Text Transfer Protocol*
Protocolo de Transferência de Hipertexto

IoE = *Internet of Everything*
Internet de Todas as Coisas

IoT = *Internet of Things*
Internet das Coisa

ISO-OSI = *International organization of Standardization - System Interconnection*
Organização Internacional para Padronização - Interconexão de Sistemas Abertos

ITIL = *Information Technology Infraestructure Library*
Biblioteca para Infraestrutura de Tecnologia da Informação

LGPD = Lei Geral de Proteção de Dados Pessoais

LTE = *Long Term Evolution*

M2M = *Machine to Machine*

MIT = *Massachusetts Institute of Technology*

NIST = *National Institute of Standards and Technology*

OGC = *Office of Government Commerce*

RFID = *Radio Frequency Identification*
Identificação por Rádio Frequência

RSA = Rivest, Shamir, Adleman

SERPRO = Serviço Federal de Processamento de Dados

Shodan = *Sentient Hyper-Optimized Data Access Network*
Rede de Acesso a Dados Hiper-Otimizada Autoconsciente

TDEA = *Triple Data Encryption Algorithm*
Algoritmo Triplo de Encriptação de Dados

TI = Tecnologia da Informação

UIC = *University of Illinois Chicago*

USB = *Universal Serial Bus*
Porta Serial Universal

Wi Fi = *Wireless Fidelity*

WoT = *Web of Things*
Web das Coisas

WSN = *Wireless Sensors Network*
Redes de Sensores sem Fio (RSSF)

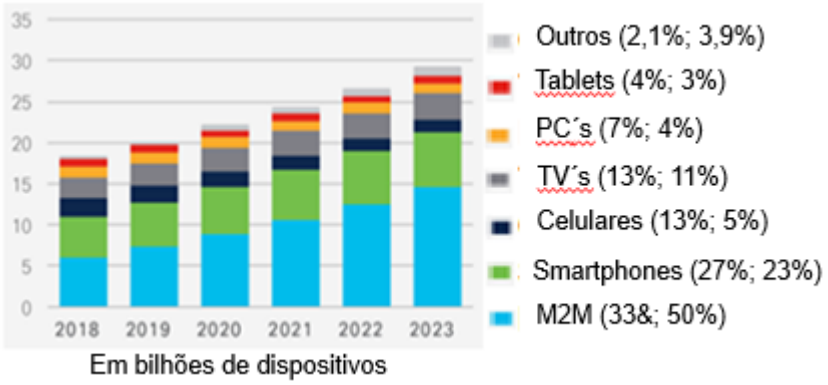
WWW = *World Wide Web*

SUMÁRIO

1 INTRODUÇÃO

A quantidade de dispositivos eletrônicos conectados à Internet tem crescido em níveis nunca vistos. Essa demanda tem feito com que a preocupação com a segurança das informações e dos dados trafegados ganhe um lugar cada vez mais importante dentro das organizações públicas e privadas, mas também para os usuários residenciais. A Figura 1 ilustra este aumento de dispositivos conectados de acordo com o relatório da Cisco Systems (CISCO, 2020).

Figura 1- Gráfico do crescimento global de dispositivos e conexões.



Fonte: Adaptado de *(CISCO, 2020, p. 6)*

O gráfico apresenta as porcentagens de cada tipo de dispositivo como: *tablets*, PC´s, TV´s,, *Smartphones* e outros. Este gráfico indica que haverá um grande aumento do segmento M2M (*Machine to Machine* – Máquina a Máquina), ou seja, na parte relacionada aos sensores, e que está diretamente ligado ao crescimento das redes de IoT (*Internet of Things* - Internet da Coisas*)*.

As redes M2M têm como principal objetivo a comunicação entre dispositivos sem a interação humana. Nestas redes os dados adquiridos são diretamente enviados a outros dispositivos e ações são tomadas de acordo com os dados lidos (WHEELER, WHEELER, & FAGBEMI, 2020).

Em 1999, o pesquisador do MIT (*Massachusetts Institute of Technology*) e pesquisador de RFID (*Radio Frequency Identification* –

Identificação por Rádio Frequência), Kevin Ashton, usou o termo IoT para definir os objetos que seriam e serão conectados à Internet para realizar tarefas sem a interferência humana. Esta definição engloba, também, o uso de dispositivos móveis, o conceito de computação na nuvem e análise de dados.

Em uma palestra na Procter & Gamble, Ashton disse:

> "Se tivéssemos computadores que soubessem tudo o que há para saber sobre coisas, usando dados colhidos sem qualquer interação humana, seríamos capazes de monitorar e mensurar tudo, reduzindo o desperdício, as perdas e o custo. Poderíamos saber quando as coisas precisarão de substituição, reparação ou atualização, e se eles estão na vanguarda ou se tornaram obsoletos" (RANGEL, 2014, p. 6).

Após o termo IoT ser popularizado, outros termos surgiram, tais como IoE (*Internet of Everything* – Internet de Todas as Coisas) e WoT (*Web of Things* – Web das Coisas). Esses termos, em vários aspectos, se sobrepõem e se fundem. Por isso, é importante que sejam definidos e sua atuação conhecida (RANGEL, 2014).

O IoE diz respeito a tudo o que pode ser conectado, não somente coisas, mas também à conexão de pessoas, dados, processos e a inteligência da comunicação de tudo (BARCELLOS, 2013).

Já o WoT é a reutilização e adaptação de aplicativos e serviços da web que permita o uso de coisas inteligentes e com isso aumentar a disponibilidade, flexibilidade e produtividade das redes de IoT (ZENG, GUO, & CHENG, 2011).

Todas as redes precisam ser protegidas do ponto de vista das informações que nelas trafegam não importa o seu tamanho. As pequenas redes domésticas e as redes de pequeno porte não contam com *softwares* aplicados à segurança quer por limitações nos equipamentos usados, quer por limitações de investimento possível. Os equipamentos usados nessas redes são eletrodomésticos inteligentes, sistemas de segurança, sistemas de ar-condicionado, controle de acesso e iluminação.

As redes internas de prédios públicos, por onde trafegam informações que, mais tarde, poderão ser usadas para a implantação de projetos de *Smart Cities* (Cidades Inteligentes) também carecem de melhorias em seus sistemas de segurança.

Somente as grandes redes corporativas já contam com sistemas de segurança de dados avançados com o uso de robôs, inteligência artificial e os mais avançados *softwares* de criptografia e detecção de invasões.

Um fato relevante no uso das redes de internet ou qualquer outro meio de comunicação que precise do uso de senhas para controle de acesso é que uma parte considerável dos usuários tem uma forte preocupação com as informações protegidas por senha (SOARES, ARAÚJO, & SOUZA, 2020).

Segundo SOARES, ARAÚJO, & SOUZA (2020) em uma pesquisa realizada por MIJUSKOVIC & FERATI (2015) com 1104 respostas houve a indicação de que 74% dos participantes se mostravam preocupados com a segurança de suas senhas e 63% com proteção a de seus gastos com cartões de crédito.

Esses valores trazem a preocupação das pessoas com essas senhas, no entanto neste mesmo artigo de SOARES, ARAÚJO, & SOUZA (2020) é afirmado que a maior parte dos usuários sequer leem os avisos de privacidade, o que se reflete também na alteração das senhas dos seus dispositivos.

Os usuários de redes residenciais ou de pequeno porte acreditam que por se tratar de redes confinadas ou de pequeno alcance não há necessidade de proteção. Uma reportagem publicada pelo site OLHAR DIGITAL (2019) relata que um grupo de *hackers* invadiu a rede de uma residência no estado americano de Wisconsin e mudou a temperatura da casa para 32°C além de colocarem músicas com palavras obscenas para os moradores ouvirem.

Nesse contexto, o presente trabalho visa analisar requisitos de segurança para as senhas de controle e acesso em redes residenciais e de pequeno porte, utilizando os equipamentos já existentes nessas redes.

1.1 Objetivos

1.1.1 Objetivo Geral

Este trabalho visa analisar os requisitos para gestão segura de uma rede de IoT residencial e de pequeno porte, por meio do uso de senhas que apresentem níveis de segurança e de força adequados, criados e testados com aplicativos de uso gratuito.

1.1.2 Objetivos Específicos

- Identificar premissas de gestão segura em redes IoT residenciais e de pequeno porte.
- Garantir que nas redes residenciais e de pequeno porte apenas os dispositivos controlados pelo administrador da rede tenham acesso à infraestrutura de Internet e aos dados compartilhados na rede.
- Especificar os requisitos de segurança das senhas para os equipamentos de roteamento, controle de redes IoT, sensores e demais periféricos visando minimizar a possibilidade de invasão das redes.
- Apresentar as definições e padrões de senhas que devem ser utilizadas nos roteadores e nos demais dispositivos em redes IoT.

1.2 Organização do trabalho

O trabalho possui 5 capítulos, estruturados da seguinte forma:

- Capítulo 2 - Revisão Bibliográfica: apresenta um estudo sobre redes IoT e as possíveis implementações de segurança para essas redes. São analisados os aspectos legais da LGPD (Lei Geral de Proteção de Dados) e do Marco Civil da Internet que influenciam no fornecimento de redes de dados por parte de pequenos e médios provedores. As características dos usuários residenciais e de redes de pequeno porte são descritas por tratar-se do objeto de estudo.
- Capítulo 3 – Metodologia: apresenta as principais etapas para a análise dos requisitos de segurança: nível de segurança e nível de força.

- Capítulo 4 – Resultados: os resultados dos testes das senhas e as características com melhor desempenho são apresentados.
- Capítulo 5 – Conclusão: apresenta a conclusão e a contribuição do trabalho, bem como sugestões para trabalhos futuros.

2 REVISÃO BIBLIOGRÁFICA

2.1 Internet das Coisas (IoT)

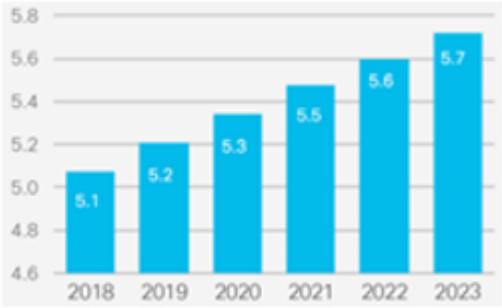
O surgimento das redes de Internet da Coisas (IoT – *Internet of Things*) e a popularização da Internet pelo uso de aplicativos em *smartphones* fizeram com que a quantidade de dispositivos crescesse exponencialmente (PALANZA, 2016).

Por conta dessa popularização, a Internet das Coisas outros conceitos e tecnologias também foram popularizados, tais como: comunicação M2M (*Machine to Machine* – Máquina a Máquina), Redes de Sensores sem Fio (WSN - *Wireless Sensors Network*) e *Smart Cities* (Cidades Inteligentes) (CARRION & QUARESMA, 2019).

Nos dias de hoje, vários tipos de dispositivos são conectados à Internet e, através dela, têm acesso a dados e informações que antes só seriam possíveis em bibliotecas e redes privadas de comunicação.

O crescimento do número de *smartphones* conectados às redes 3G e 4G já desponta como um fator de inclusão social e de acesso ao conhecimento. No relatório anual da Cisco Systems Inc., de 2018 a 2023, este crescimento é mostrado na Figura 2:

Figura 2 – Gráfico do crescimento global de usuários de dispositivos móveis.



Fonte: Adaptado de *(CISCO, 2020, p. 5)*

A Figura 2 mostra que haverá um crescimento de 200 milhões no acesso móvel, entre os anos de 2020 e 2021, e um aumento de 100 milhões nos

dois anos seguintes. Isso fará com que a quantidade de dados e informações que trafegam pelas redes aumente proporcionalmente.

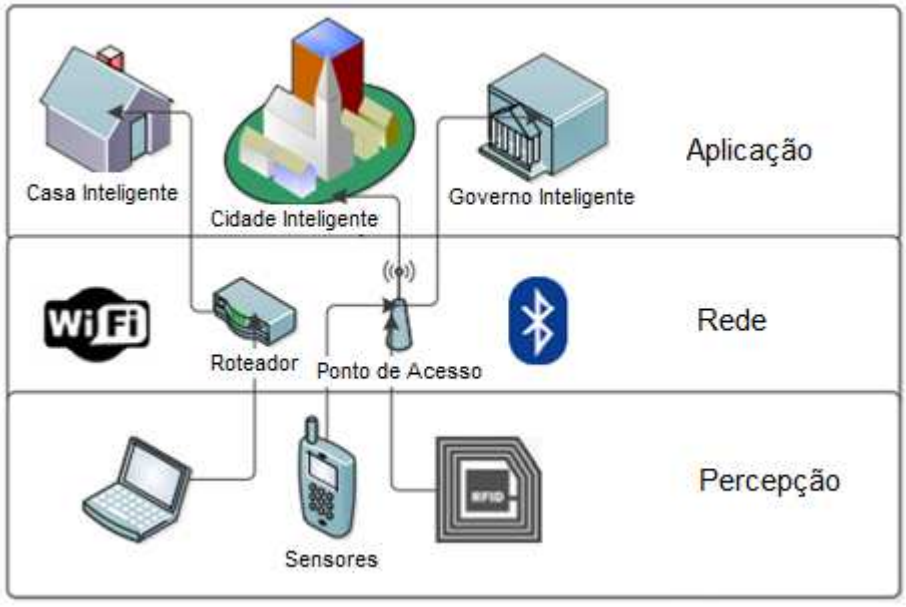
Por conta da Pandemia da COVID-19 (Sars-Cov-2) no ano de 2020 houve um aumento considerável no uso de dispositivos móveis, seja para acesso pessoal, bem com profissional e educacional. Segundo reportagem de (LAVADO, 2020) houve aumento em torno de 50% no uso das redes de dados.

Nas redes IoT são conectados diversos tipos de equipamentos como: câmeras, sensores diversos, dispositivos de armazenamento, controle de acesso e controles de iluminação e temperatura.

Essa incrível gama de dispositivos e de fabricantes faz com que as redes IoT sejam muito diferentes umas das outras. Assim, a implementação e padronização de qualquer aspecto será muito difícil.

As redes IoT foram definidas com três camadas conforme a Figura 3:

Figura 3 – As três camadas das redes IoT.



Fonte: Adaptado de (MAHMOUD, YOUSUF, *et al., 20*15, p. 3)

As três camadas e suas atribuições são:

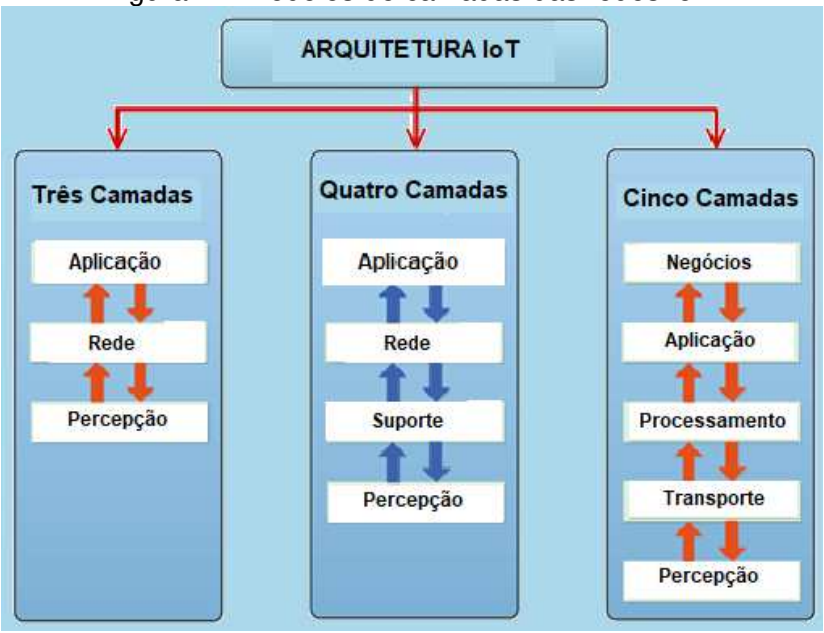
- Camada de Percepção: é a camada responsável pela detecção, coleta e processamento da informação. Comumente, esta camada utiliza WSN (*Wireless Sensors Network* – Rede de Sensores Sem fio – RSSF);

- Camada de Rede: é nesta camada que as rotas e endereçamentos dos dados são realizadas. A comunicação é realizada com uso das tecnologias mais novas de transmissão como Redes sem fio (*Wireless*), *Bluetooth*, LTE (*Long Term Evolution*), 3G, ZigBee, entre outras;
- Camada de Aplicação: nesta camada estão os aplicativos nos quais os dados e informações coletados são usados e ficam à mostra. É nessa camada que se tem a aplicação dos protocolos de segurança para as redes IoT.

A falta de capacidade de processamento e disponibilidade de energia são as maiores deficiências dos dispositivos IoT no que diz respeito à segurança. Como as redes IoT têm, principalmente, essas duas deficiências na sua parte de segurança, elas acabam se tornando alvos fáceis para ataques. Por esse motivo ainda é muito discutido em qual camada devem ser implantados os protocolos de segurança (MACEDO, *et al.,* 2019; WHEELER, WHEELER e FAGBEMI, 2020).

Por conta desta discussão da implantação dos protocolos de segurança, vários modelos de estruturas de camadas para as redes IoT foram apresentados conforme a Figura 4::

Figura 4 – Modelos de camadas das redes IoT.



Fonte: Adaptado de (BURHAN, REHMAN, *et al.,* 2018, p. 10)

Pode-se notar que, no primeiro quadro, é apresentado o modelo mais comum das redes IoT que o define com três camadas. Este modelo é o mais defendido por aqueles que desejam que a IoT continue a ser uma rede que preserve suas características principais.

Nos outros quadros, estão os exemplos de outros modelos, com quatro e cinco camadas. Mas já existem modelos de até sete camadas como o proposto pela Cisco Systems (MOSENIA e JHA, 2017).

Existem aqueles que defendem que a segurança nas redes IoT deva ser implementada em uma das camadas existentes. No entanto, há aqueles que demonstram ser melhor uma nova camada somente para a segurança e, outros, que defendem uma maior aproximação ao modelo ISO-OSI de sete camadas (MOSENIA e JHA, 2017).

2.1.1 Funcionamento da Rede IoT

Uma rede IoT é uma extensão de uma rede de dispositivos que utilizam a Internet como base para sua comunicação. A diferença entre as redes IoT e as demais redes de dispositivos que estão conectadas à Internet é que as redes IoT são capazes de fazer a medição, coleta e análise de dados dos ambientes aos quais estão integradas, contribuindo, assim, para a segurança, economia e bem-estar daqueles que frequentam aquele ambiente. A Figura 5 ilustra quatro diferentes áreas em uma rede IoT: Dispositivos Inteligentes (como *SmarTV´s*, Cafeteiras, Geladeiras, etc), Conforto Térmico/Iluminação/Sensores (Lâmpadas, Sensores de Gás, Sensores GLP, Ar Condicionado, etc), Controle de Acesso/Segurança (RFID, Câmeras, Acesso de Veículos, etc) e Comunicação (*Notebooks*, *Tablets*, *Smartphones* e *Smart Watches*).

Figura 5 - Diagrama de Rede IoT.

Fonte: Do próprio autor, 2021

Desse modo, em uma rede IoT, mostrada na Figura 5, têm-se diversos dispositivos como:

a) Câmeras: dispositivos de captura de imagens. Podem ser colocados no interior de residências ou nas áreas externas.

b) Smartphones: dispositivos móveis conectados à rede 3G/4G de telefonia celular ou então por conexão Wi-Fi à rede de Internet. São utilizados para os mais variados fins, acesso a e-mails, servidores de imagem, bancos, aplicativos variados e serviços de comunicação.

c) Impressoras: impressoras que podem ser conectadas à rede via cabo USB (*Universal Serial Bus* – Porta Serial Universal), *Wi Fi* ou cabo Ethernet.

d) *Storage*: equipamento de armazenamento de dados e imagens de um sistema. Pode ser um equipamento conectado à própria rede ou um serviço de armazenagem em Cloud.

e) Home Media: parte de entretenimento de uma casa, que pode incluir desde um Set Top Box (receptor) de uma TV por

Assinatura, projetor multimídia, sistema de Home Theater, Smart TV´s, entre outros.

f) Eletrodomésticos conectados: atualmente vários eletrodomésticos são automatizados, como geladeiras que conseguem identificar os produtos que estão faltando, cafeteiras que preparam o café em horário pré-determinado e lavadoras de roupa programáveis para a roupa estar lavada ao final do dia.

g) Sensores: garantem a aquisição de dados de temperatura interna e externa, luminosidade, umidade relativa do ar de modo a garantir o conforto térmico e luminoso dos ambientes.

h) Controladora de sensores: é um equipamento que tem como função medir, coletar e efetuar uma análise primária destes valores para então transmiti-los a um outro computador a fim de realizar análises mais detalhadas;

i) Controladora de câmeras: um dos dispositivos mais utilizados em redes IoT são câmeras e dispositivos de controle de acesso. Este equipamento tem por função carregar as imagens, armazená-las em um servidor de imagens (*Storage* - Armazenagem) e realizar primariamente a análise dessas imagens de modo a utilizá-las para a segurança e o controle de acesso dos ambientes onde estão localizadas.

j) Controladora I/O: é uma controladora para qualquer tipo de dispositivo em que seja necessário seu acionamento elétrico do tipo liga e desliga, como por exemplo: motores, iluminação, ventilação, acionamento de tomadas, etc (AL-FUQAHA, *et al.,* 2015).

Uma rede IoT não possui requisitos de segurança definidos e robustos (BASTA, BASTA e BROWN, 2014). Por essa razão o uso de senhas confiáveis, robustas e de difícil identificação pode garantir uma proteção aos usuários dessas redes.

2.1.2 Modelo OSI

Este modelo foi desenvolvido e criado em 1971, mas só foi publicado em 1983 pelo ISO (*International Standards Organization* – Organização de Padronização Internacional) (TANENBAUM, 2003). Foi a primeira tentativa no sentido de desenvolver um modelo para padronizar as conexões entre redes de computadores pelo sistema de divisão em camadas.

O modelo de referência OSI (*Open Systems Interconnection* – Interconexão de Sistemas Abertos) possui 7 camadas, de acordo com a Figura 6:

Figura 6- Modelo OSI.

Fonte: *(PPLWARE, 2010)*

As atribuições de cada camada devem ser bem definidas e não deve haver sobreposição de atribuições. As funções de cada camada são informadas pelo modelo OSI, entretanto os protocolos e serviços não são o objetivo do modelo. Sendo assim, apresentam-se, a seguir, algumas características de cada camada:

- Camada 1 - Física: transmissão dos bits propriamente ditos através de sinais elétricos. São definidas nesta camada as interfaces mecânicas, elétricas e de sincronismo com as demais camadas;
- Camada 2 – Ligação (Enlace) de Dados: aqui são definidos os endereçamentos e a transmissão. Garante a transmissão dos pacotes

de um nó a outro através do endereço de cada estação (Transmissora e Receptora);

- Camada 3 – Rede: estabelecimento das rotas dos envios dos pacotes. É nessa camada que a definição das rotas determina o tipo de rede que será utilizado: LAN´s (*Local Area Network* – Redes Locais) e WAN´s (*Wide Area Network* – Redes de Grandes Áreas);
- Camada 4 – Transporte: aceita todos os pacotes vindos da camada acima dela e divide-os de acordo com o necessário para garantir a transmissão e recepção corretas e íntegras de todos os pacotes de dados;
- Camada 5 – Sessão: a comunicação entre transmissor e receptor é estabelecida nesta camada. É aqui que os pedidos de conexão são gerados e as respostas recebidas para estabelecer uma conexão. O controle das sequências de comandos garante a transmissão total dos pacotes;
- Camada 6 – Apresentação: primeira camada que trabalha com estrutura de dados abstratas. Gerenciamento de segurança com a criptografia e também faz as conversões entre as diferentes estruturas de dados intercambiadas;
- Camada 7 – Aplicação: esta camada controla e aplica os protocolos de comunicação para envio de e-mails, transferências de arquivos e conexões servidor/cliente. O protocolo mais utilizado é o HTTP (*Hyper Text Transfer Protocol* – Protocolo de Transferência de Hipertexto) que é a base de comunicação da internet (TANENBAUM, 2003).

2.1.3 Outros Modelos de Camadas para redes IoT

Com a enorme quantidade de fabricantes de dispositivos e como não há uma definição por parte dos organismos normativos de como deve ser uma rede de IoT, cada fabricante desenvolve seus produtos baseado na suas definições e foco de mercado.

Com isso o usuário implementa sua rede de acordo com seus conhecimentos e necessidades, com isso acabam existindo diversas configurações de segurança possíveis (MOSENIA e JHA, 2017).

Em virtude disso, e como já foi mencionado anteriormente, existem alguns outros modelos de camadas para redes de IoT, conforme Figura 7:

Figura 7 – Modelos de camadas das redes IoT com modelos de 5 e 7 camadas.

Fonte: Adaptado de *(MOSENIA* e JHA*, 2017, p. 3)*

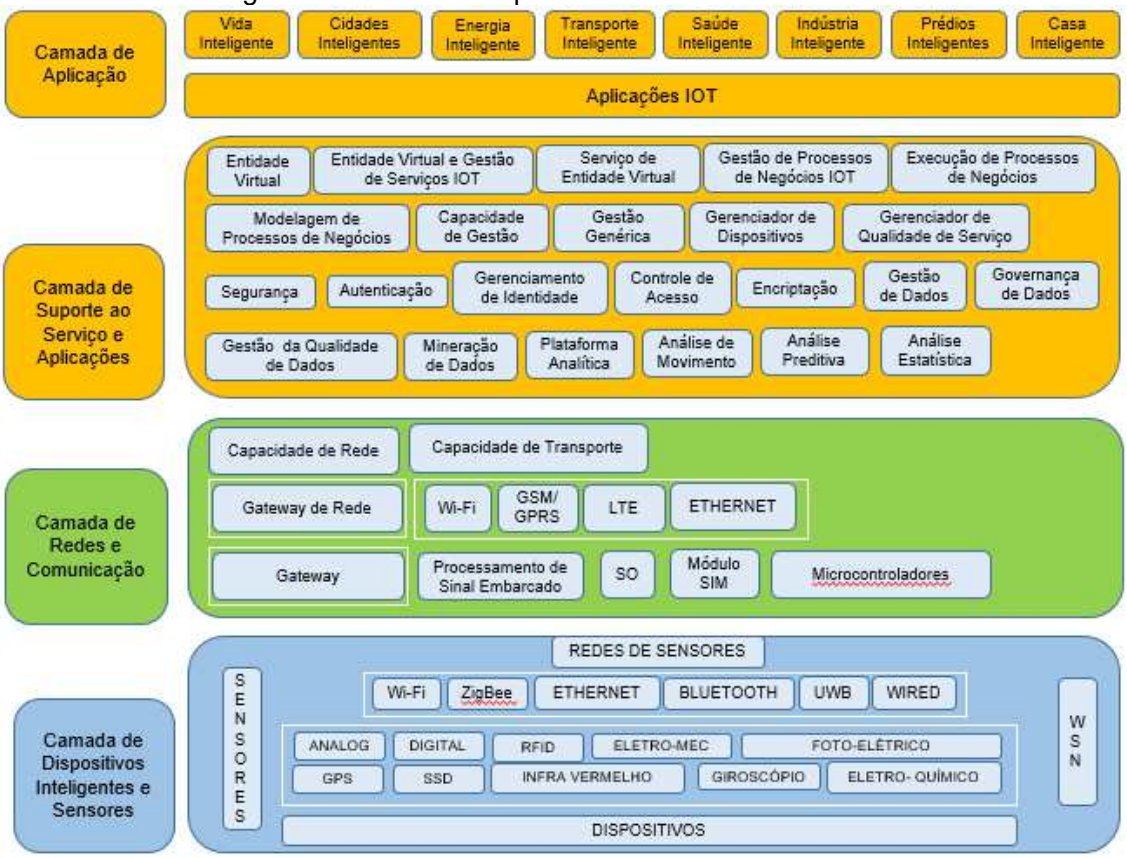
A Figura 7 apresenta proposições onde observam-se 3, 5 e 7 camadas. O modelo de 3 camadas é o modelo usado atualmente nas redes IoT onde as implementações de segurança não estão bem definidas e normalmente são incluídas na camada 2.

No modelo de 5 camadas, as implementações de segurança seriam realizadas nas camadas 3 e 4, que tratam do gerenciamento e composição da rede IoT.

Já no modelo de 7 camadas as implementações de segurança seguirão o mesmo padrão do modelo ISO-OSI que prevê aplicativos de segurança nas camadas 6 e 7 mas, também, métodos de controle de conexão de *hardware* nas camadas 2 a 4 (BUFFENOIR, 1988).

No modelo apresentado na Figura 8, as redes IoT foram definidas com quatro camadas e pode-se notar que a primeira e a segunda camadas, neste modelo, são muito semelhantes à primeira camada do modelo IoT tradicional (3 camadas). Já a terceira camada, onde estão localizadas as interfaces de segurança, é uma nova camada incluída neste modelo (PATEL, 2016).

Figura 8 – Modelo de quatro camadas das redes IoT.



Fonte: Adaptado de (PATEL, 2016, p. 5)

Na figura 08 nota-se a inclusão da camada de Suporte ao Serviço e Aplicações mostra que nesta camada diversos aspectos de segurança já existentes no modelo OSI são implementados, como:

- Autenticação;
- Gerenciamento de Identidade;
- Controle de Acesso;

- Encriptação;
- Governança de Dados.

Outro problema relacionado à segurança em redes IoT é a existência de diversas placas de prototipagem como o Arduino e Raspberry Pi, que atuam como controladoras dos sistemas e podem ou não estarem conectadas à Internet (STEVAN JUNIOR, 2018).

Essas placas de prototipagem não possuem processamento adequado para uso de aplicativos de segurança nem tão pouco de *firewall* ou antivírus e por isso se constituem um ponto fraco para ataques nas redes IoT (MONK, 2014).

2.2 Segurança em redes

No âmbito da segurança da informação, alguns requisitos de segurança são aplicáveis a qualquer tipo de rede, e eles são (MOSENIA e JHA, 2017):

- Confidencialidade: garantir que somente as pessoas autorizadas possuem acesso à informação;
- Integridade: garantir a integridade e a precisão da manipulação não autorizadas de dados;
- Disponibilidade: garantir que toda a informação esteja disponível aos usuários autorizados;
- Responsabilidade: responsabilizar o usuário por qualquer ação tomada com a informação a qual ele teve acesso;
- Auditabilidade: monitorar todas as ações para prevenir acessos indesejados;
- Confiabilidade: verificação de identidade e acesso de terceiros autorizados;
- Não Repúdio: confirmação ou não de uma ocorrência dentro dos sistemas;

- Privacidade: permitir que os usuários controlem suas informações pessoais e obedeçam às políticas de privacidade.

Estes aspectos de segurança são importantes e imprescindíveis em qualquer tipo de rede por onde trafeguem informações e dados. Segundo (MOSENIA e JHA, 2017), os aspectos mais importantes são conhecidos como Tríade da Segurança da Informação, ou pelas iniciais CIA (*Confidentiality, Integrity and Avaliability* – Confidencialidade, Integridade e Disponibilidade).

Quando as questões de segurança são tratadas no âmbito de uma rede construída com base no modelo OSI, os aplicativos de segurança estarão em diversas camadas. A implementação em determinada camada está diretamente ligada aos tipos de ataques que cada camada poderá sofrer (TANENBAUM, 2003).

No modelo OSI, a lista de possíveis ataques são:

- Mascaramento: é quando um invasor se faz passar por um usuário autorizado a acessar a rede (DE LUCCA, 1995);
- Associação Ilegal: ocorre quando o invasor se associa a outros para cometer crimes;
- Acesso não autorizado: ocorre quando um acesso sem autorização é tentado;
- Negação de serviço (*Denial of Service*): impede que um recurso/dispositivo seja utilizado pelos demais integrantes da rede através da inserção de um grande número de pacotes enviados ao receptor (KUROSE e ROSS, 2013);
- Repúdio: é quando o remetente da mensagem envia algum pacote de confirmação que é confirmado por um invasor como tendo recebido a mensagem e com isso estabelece a comunicação. Pode acontecer quando o destinatário da mensagem recebe um pacote do invasor quando está esperando um pacote do remetente confiável (BUFFENOIR, 1988);
- Vazamento de informação: quando a senha ou alguma política de segurança é divulgada com ou sem intenção;

- Análise de tráfico: através de um dispositivo os pacotes são capturados e depois analisados;
- Sequenciamento de mensagens indevido: ao enviar as mensagens de conexão à rede uma delas é trocada de ordem pode ocasionar problemas na conexão;
- Modificação ou destruição de dados: os dados que trafegam pela rede são modificados de modo a garantir a captura dos demais pacotes existentes;
- Ataques de inferência de informação;
- Modificações ilegais em programas: conhecidos em diferentes formas como: Vírus, Cavalo de Tróia e *Worms* (PATEL, 1994).

Essas ameaças são as mais comuns em termos de redes de dados. Para garantir-se a segurança da informação e dos dados que trafegam pelas redes IoT é necessário o uso de alguns tipos de contramedidas.

Os tipos mais comuns e eficientes de contramedidas são (BUFFENOIR, 1988):

- Uso de algoritmos de codificação da rede no acesso e permissão de uso dela;
- Gestão de Autenticação: garantir que o usuário ou dispositivo seja autenticado antes de conectar-se à rede e transmitir pacotes;
- Gestão do Controle de Acesso: garantir que o acesso à rede seja controlado através de senhas e códigos gerados aleatoriamente;
- Gestão de Chave de Acesso: prover chaves de acesso com criptografia adequada ao nível de segurança de rede pretendido;
- Auditoria de segurança e manipulação de eventos: promover uma garantia de auditoria nos sistemas e adequação ao uso (BUFFENOIR, 1988).

Essas contramedidas podem ser usadas, em conjunto, quando apresentam maior eficiência, ou individualmente, para garantir que a proteção seja focada no ataque sofrido.

2.3 ITIL

O ITIL (*Information Technology Infrastructure Library* ou Biblioteca de Infraestrutura de Tecnologia da Informação) foi criado, em 1989, no Reino Unido, pelo CCTA (*Center of Computer and Telecommunications Agency* – Agência Central de Computação e Telecomunicações) mas, em 2000, passou a ser gerenciado pela Secretaria de Comércio Britânica (OGC - *Office of Government Commerce*).

O ITIL é um conjunto de boas práticas aplicada a serviços de TI, ou seja, um *framework* que trata do gerenciamento de serviços em TI. Atualmente, é constituído de 5 livros sobre o ciclo de vida do serviço em TI (ALMEIDA JÚNIOR, 2019).

Este *framework* leva em conta cinco aspectos necessários a uma gestão de redes de TI, elencados como os mais importantes com foco nos serviços:

- Estratégia;
- *Design*;
- Transição;
- Operação;
- Continuidade.

O ITIL busca estabelecer uma uniformidade na sua infraestrutura e nos sistemas de *software* utilizados, de modo a garantir o funcionamento ininterrupto dos serviços de TI (SANTOS, 2017).

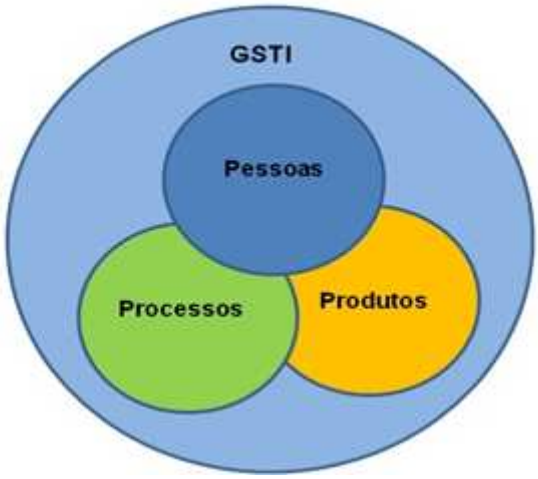
Segundo MORIKANE (2008) o Gerenciamento de Serviço de TI (GSTI) especificado no ITIL pode ser dividido em várias áreas como:

- Gerenciamento de níveis de serviço;
- Gerenciamento de finanças;
- Gerenciamento de capacidade;
- Gerenciamento de continuidade;
- Gerenciamento de disponibilidade;

- Gerenciamento de configurações;
- Gerenciamento de mudanças;
- Gerenciamento de liberação;
- Gerenciamento de incidentes;
- Gerenciamento de problemas;
- Service desk (Help Desk).

O GSTI trata da interação entre pessoas, processos e produtos já que todos eles se beneficiam das melhores práticas existentes no ITIL, conforme a Figura 9:

Figura 9 – Atuação do GSTI segundo o ITIL



Fonte: (FABICIACK, 2009, p. 2)

É esse gerenciamento nessas áreas que garante a correta entrega dos serviços previstos no ITIL, possibilitando a eficiência e a disponibilidade acordados entre fornecedores e clientes.

Guardadas as devidas proporções, de acordo com o tamanho da infraestrutura, pode-se fazer um paralelo do Gerenciamento de Serviço de TI (GSTI) do ITIL com a implantação de uma rede IoT em uma residência, por um estudante, ou então, em uma pequena empresa pelos proprietários, mesmo que não tenham experiência em TI (LYRA e DUQUE, 2011).

A parte especificada no GSTI como TI (Tecnologia da Informação) pode ser entendida, no âmbito das redes IoT, como implantar uma rede de dispositivos conectados, o conhecimento sobre os dispositivos e a capacidade de aprender sozinha.

As pessoas envolvidas no uso das redes de TI e de IoT são todas aquelas que integram aqueles ambientes, quer sejam moradores ou funcionários, pois estes serão impactados pelo controle e sensoriamento dos dispositivos instalados na rede IoT (LYRA e DUQUE, 2011).

Os processos podem ser flexibilizados e incluídos aos processos de acesso, gravação de imagem, dados dos sensores e aplicação dos dados capturados.

Não existe uma certificação em ITIL dadas às empresas que o utilizam pois para o ITIL cada empresa é única e suas configurações devem ser individualizadas para que possa garantir a implementação correta.

A segurança da informação no ITIL é tratada como um aspecto muito importante. Como o ITIL trata de processos e pessoas, um dos processos onde as pessoas têm maior interferência é na escolha da arquitetura da rede. Essa rede por sua vez possui dispositivos com senhas e limitações de acessos. (FABICIACK, 2009)

Por este motivo torna-se importante que a escolha dessas senhas, que são o primeiro passo de configuração de uma rede de internet, seja feita levando-se em conta os aspectos de segurança como nível de segurança e nível de força dessas senhas.

2.4 Segurança em redes IoT

Foi possível verificar que a questão da segurança, embora primordial e de muita relevância para qualquer tipo de dispositivo que acesse a Internet, não conta com uma variedade e quantidade necessárias de referências para balizar a implementação de uma metodologia de segurança aplicável às redes IoT

Essa conclusão foi possível através da análise de artigos, livros e normas no âmbito das redes IoT pesquisados neste trabalho. (EGIDIO & UKEI, 2015; FRUSTACI, *et al.,* 2018).

Com base no que foi pesquisa foi feito um levantamento dos tipos de ataques mais sofridos pelas redes IoT, que é um dos temas mais frequentes, bem como algumas contramedidas que podem ser utilizadas (SWAMY, JADHAY e KULKARNI 2017; MAHMOUD, *et al.*, 2015).

Segundo RAMAKRISHNA, *et al.* (2018), IoT é a interconexão de muitos tipos de dispositivos que podem ser desde máquinas de lavar roupas, refrigeradores e televisores (*SmartTV* – Televisão Inteligente), além dos mais comuns como *smartphones*, câmera e *notebook*s, é um problema quanto à padronização de segurança para redes IoT, por conta das conhecidas limitações dessas redes: Privacidade, Segurança, e Compatibilidade em dispositivos.

Estes dispositivos, por conta desta variedade, apresentam um elevado grau de possibilidades de ataques. Esses ataques são muito variados, (RAMAKRISHNA *et al.*, 2018), mas os principais são:

- Ataques físicos: adulteração de componentes de hardware da rede. São os mais caros de serem executados pois dependem de técnicas mais elaboradas;
- Ataque de canal lateral: são realizados para detectar o tipo de criptografia usado na rede;
- Ataques de criptoanálise: são tentativas de capturar os arquivos de criptografia e convertê-los em textos;
- Ataques de *software*: são os mais comuns em qualquer sistema que envolve redes. Podem ser feitos através de infecção por programas Cavalo de Tróia, Worms ou Vírus. *Software* é o maior alvo dos ataques realizados às redes IoT;
- Ataques à rede: as redes *wireless* consistem em um ponto fraco dos sistemas. Ataques aos nós de conexão através de interrupção, mau funcionamento e captura do nó.

Muitas das contramedidas utilizadas, como o uso de chaves criptográficas e *firewalls*, precisariam de um poder de processamento muito superior aos disponíveis em dispositivos e redes IoT (MOSENIA e JHA, 2017).

As características fundamentais das redes e dispositivos IoT são: interconectividade, serviços, heterogeneidade, alterações dinâmicas e larga

escala. A consideração dessas características na análise de requisitos para uma gestão segura de redes IoT se configura como um grande desafio, já que, na literatura, há alterações dessas características (PATEL, *et al.,* 2016).

Por serem redes que atendem às mais diversas finalidades suas caraterísticas fundamentais tendem a sofrer mudanças de acordo com as preferências do administrador da rede.

Tratando somente das redes residenciais e de pequeno porte há uma gama infinita de possibilidades de configuração dessa rede e também uma quantidade muito grande de dispositivos que à ela possam ser conectados.

Um exemplo possível dessas alterações é o uso de um *Firewall* nas redes IoT. Todo e qualquer *Firewall* possui necessidade de uma alta capacidade de processamento e disponibilidade de energia para funcionar corretamente e atingir seus objetivos de proteção configurando um desafio para implementação em redes IoT (SHIRALI-SHAHREZA e GANJALI, 2018).

Exatamente por ser uma rede heterogênea, onde os ativos computacionais não estão sob controle do usuário e, por isso, não podem implementar os aspectos de segurança que julguem adequados, é que se faz necessário um meio de certificar e autenticar os dispositivos conectados e os que se desejam conectar com um controle para prover melhor segurança.

As redes de sensores sem fio (RSSF ou *Wireless Sensors Network* - WSN), que são parte muito importante das redes IoT, também carecem de uma implementação de segurança para que possam garantir a segurança dos dados que estão sendo coletados e a confidencialidade desses dados (JESUS JUNIOR e MORENO, 2015).

Segundo DIAS (2016), as questões de segurança mais importantes para as redes e dispositivos IoT são:

- Uso de redes não confiáveis;
- Maior parte dos acessos é por meio remoto;
- Falta de interfaces de atualização confiáveis;
- A criptografia de dados não é suportada por esses dispositivos.

Por isso, muitos dos artigos publicados nesse tema não conseguem estabelecer um paralelo entre manter a rede IoT heterogênea e dinâmica e garantir a segurança de dados e informações (RAMAKRISHNA, *et al.,* 2018; EGIDIO e UKEI, 2015; MAHMOUD, YOUSUF, *et al.,* 2015).

Em DIAS (2016) há várias análises sobre técnicas de segurança que podem ser usadas em redes IoT, tais como: “autenticação, garantia de saúde dos dispositivos, recuperação, proteção de dispositivos infectados, proteção de dados, segurança no *hardware* e segurança física do *hardware*”. Apesar de enumerar essas técnicas essa referência não apresenta nenhum método efetivo de proteção às redes IoT, deixando várias possibilidades em aberto.

Por serem heterogêneas e dinâmicas, as redes IoT não podem ser encaixadas em um tipo específico de sistema de gerenciamento de redes e nem em alguns métodos de boas práticas.

A segurança em redes IoT tem sido um tema bastante discutido e com várias possibilidades em estudo (CHERUVU, *et al.*, 2020). No entanto, essa dificuldade de padronizar as infraestruturas das redes IoT levou a um sério problema de aplicação das soluções encontradas.

Já nos casos das redes de dispositivos IoT, é necessária a utilização de outros tipos de aplicativos, pois a capacidade de processamento e disponibilidade de energia elétrica são fatores limitantes para o uso dos mesmos aplicativos usados em redes de computadores que seguem o modelo OSI.

Os dispositivos IoT são instalados muitas vezes na periferia das redes e nesses casos não possuem conexão direta com a rede de energia elétrica. Por isso é muito comum que usem baterias que não garantem autonomia perene à esses dispositivos.

Com essa disponibilidade de energia tão pequena os processadores e as memórias dos dispositivos IoT devem ser projetados para não consumir muita potência e por esse motivo não se pode contar com processadores com uma alta capacidade de processamento por estes dependerem de alta disponibilidade de energia.

Os diferentes aplicativos devem garantir os seguintes aspectos de segurança (ALCÂNTARA, 2017; ETTER, 2017):

- Usar somente dispositivos e *softwares* originais, autorizados e licenciados;
- Uso de processo de autenticação cada vez que um novo dispositivo desejar conectar a uma rede. Esse processo deve ser realizado antes do novo dispositivo enviar e coletar dados;
- Um outro dispositivo deve ser o responsável pela execução de um *Firewall* já que os dispositivos IoT têm processamento, memória e energia muito limitados;
- Evitar consumo excessivo de banda da conexão de Internet para implantação e/ou atualização dos aplicativos de segurança.

A melhor configuração de segurança para uma rede IoT deve resguardar as principais características desse tipo de rede, como (MAHMOUD, *et al.,* 2015):

- O dinamismo e heterogeneidade das redes IoT;
- Sua configuração e infraestrutura foge dos padrões dos modelos tradicionais;
- Os tipos de ataques e ameaças são otimizados, alterados e estão em constante evolução;
- A integração de produtos de diversos fabricantes;
- A alta variabilidade dos protocolos existentes nessas redes.

Em virtude do cenário descrito, diversas pesquisas têm sido realizadas com o intuito de criar um conjunto de requisitos de segurança facilmente adaptável às redes IoT. Nessas pesquisas, demonstra-se que os principais assuntos relacionados à segurança são (DIAS, 2016):

- Garantir que os ataques na camada de percepção, onde estão localizados os sensores, sejam minimizados. É apresentada a possibilidade de um protocolo de segurança nos sensores implantado pelos fabricantes;

- Garantir que outros dispositivos de redes IoT sejam capazes de suportar ataques de intrusão;
- Identificar as contramedidas já existentes para outras redes, mas que não prejudiquem a comunicação, velocidade e agilidade das redes IoT (MOSENIA e JHA 2017).

Por conta disso, o método mais próximo encontrado para o gerenciamento das redes IoT é o *framework* ITIL, pois este é adaptável às necessidades da organização, ao investimento disponível e aos conhecimentos do proprietário da rede (ALMEIDA JÚNIOR, 2019).

Como não há um método específico para redes IoT e que atenda às particularidades de cada tipo de rede IoT existente utilizou-se o ITIL que também prevê um modelo de gestão de segurança específico para cada uma das organizações que o aplicam.

2.5 Roteadores

Roteadores são dispositivos eletrônicos que no âmbito das redes IoT residenciais e de pequeno porte têm papel fundamental na comunicação entre os dispositivos de controle, sensores e outros equipamentos integrados à rede.

É o roteador que garante também a conexão daquela rede com a Internet e permite que os dispositivos sejam acionados remotamente a partir de aplicativos de controle (TANENBAUM, 2003).

Os roteadores são o ponto de conexão, entrada e saída de dados e controle da rede. É através dele que tudo se conecta à rede e, por esse motivo é imprescindível que o roteador possua uma senha de acesso para configuração segura e que suporte ataques de intrusão.

Os roteadores proveem, além da rede através de cabos, uma ou mais redes sem fio e é nessa rede sem fio que a grande maioria dos dispositivos se conectará à rede IoT.

Por isso é necessário que a senha de conexão dos roteadores tenha também uma segurança adequada e seja segura para suportar os ataques.

É nos roteadores é que as controladoras das redes IoT são conectadas e transmitem seus dados na rede e para fora dela. Os dados são obtidos dos sensores e periféricos de rede, por exemplo: sensores de temperatura e luminosidade.

Estes sensores por sua vez conectam-se aos controladores que fazem a aquisição e o tratamento desses dados indicando as ações que serão tomadas a partir dos dados dos sensores.

Os controladores comunicam-se entre si para que as ações tenham os efeitos necessários. Essa comunicação entre os controladores deve possuir segurança adequada para não serem utilizados como ponto de acesso indevido.

Em muitos casos, é interessante o uso de controladoras conforme descrito no item 2.1.1 pois os roteadores, em sua maioria, possuem uma limitação quanto ao número de dispositivos que podem conectar-se a ele. Essa limitação gira em torno de 250 dispositivos.

Outro problema na escolha de roteadores e que tem que ser levado em conta são as interferências de outros roteadores que estejam ao alcance do roteador da rede IoT. Por isso, roteadores com vários canais de transmissão sem fio são mais caros e mais úteis nas redes IoT (FERREIRA e MONTANHA, 2017).

Segundo BASTA, BASTA e BROWN (2014) não é indicado que a senha dos roteadores seja a mesma para todos os dispositivos de rede e sensores, e sim que cada dispositivo na rede possua uma senha única e exclusiva. Essa medida é capaz de dificultar a entrada de invasores e em caso de ser quebrada, será necessária a troca apenas da senha daquele equipamento e não de toda a rede.

2.6 Shodan

Existe na Internet um site que disponibiliza diversas ferramentas de análise de segurança de maneira gratuita. Esse site é o www.shodan.io.

O uso do Shodan foi definido pois é mencionado em vários sites como o “buscador dos buscadores” e apresenta diversas ferramentas de coleta de dados pré-programadas e disponíveis para uso (CARVALHO, 2018).

A denominação “Shodan” vem de (*Sentient Hyper-Optimized Data Access Network* - Rede de Acesso a Dados Hiper-Otimizada Autoconsciente) e é um poderoso buscador da Internet, criado em 2003, por John Materly (IMASTERS FÓRUM, 2014).

O site Shodan é um mecanismo de busca onde todos os dispositivos da Internet podem ser localizados (TONOBOHN, 2020). Muito utilizado para verificar o alcance de um tipo de invasor de computadores chamado *Ransonware*. Através de ferramentas disponíveis neste site, é possível verificar quantos dispositivos foram infectados.

Outro uso possível das API´s (*Application Program Interface* – Interface de Programação de Aplicações) disponíveis no site é a verificação do uso de senhas padrão pelos equipamentos. O uso de senhas padrão facilita o ataque e invasão de redes e dispositivos conectados à World Wide Web (WWW) e, com isso, gera um ponto de entrada frágil nas redes IoT (CARVALHO, 2018).

A API verificará se o dispositivo teve sua senha trocada para que ele possa ser conectado à rede. Quando o nome do dispositivo, nome de administrador e senha do administrador do dispositivo são facilmente encontrados na Internet, o usuário deverá trocar essas informações por informações únicas e exclusivas para melhorar a segurança de sua rede IoT.

2.7 Marco Civil da Internet e Lei Geral de Proteção de Dados (LGPD)

Como as informações e os dados que trafegam pelas redes de computadores, sobretudo pela Internet, tornaram-se ativos muito valiosos fez-se necessária a criação de diversas leis que garantam a confidencialidade, integridade e disponibilidade dessas informações.

Nos Estados Unidos da América (AMÉRICA, ESTADOS UNIDOS DA, 1986) e na União Europeia (JORNAL OFICIAL DA UNIÃO EUROPÉIA, 2016),

as leis que regulamentam o uso, coleta, troca e segurança de dados já entraram em vigor.

No Brasil, o Novo Marco Civil da Internet (Lei nº 12.965 de 23/04/2014) e, mais recentemente, a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709 de 14/08/18) são leis que instituem a regulamentação, diretrizes e multas para a proteção de dados pessoais (MARCACINI, 2016).

A LGPD estabelece os atores, suas funções e responsabilidades. Os quatro principais atores são: Titular, Agentes de Tratamento (Controlador e Operador), Encarregado da Proteção de Dados Pessoais e a Agência Nacional de Proteção de Dados (ANPD) (BRASIL, 2018). A Figura 10 ilustra os atores e suas funções na LGPD.

Figura 10 - Atores envolvidos na LGPD.

Fonte: (A2C BRASIL, 2019)

Os atores previstos na LGPD são:

- Titular: é aquele que tem seus dados armazenados no site e demais entes sujeitos à lei;
- Agentes de Tratamento: são de dois tipos, o Controlador é aquele que faz as regras de tratamento dos dados pessoais e o Operador é que efetivamente aplica as regras;
- Autoridade Nacional de Proteção de Dados: é um órgão público que foi criado e é o responsável pela fiscalização e implementação da LGPD;

- Encarregado de proteção dos dados pessoais: encarregado da comunicação e relacionamento entre os demais atores previstos.

A Figura 11 indica os pontos mais importantes na aplicação da LGPD com as atividades englobadas e as ações necessárias em cada um desses pontos.

Figura 11 – Aspectos mais importantes da LGPD.

Fonte: (SERPRO, 2018)

Cada um desses aspectos completa o outro, de modo que a lei garanta a privacidade e controle de seus dados pelo usuário:

- Confirmação: garante a existência do tratamento de dados;
- Acesso aos dados: o usuário pode acessar seus dados a qualquer momento;
- Correção de dados: o usuário pode corrigir seus dados sempre que julgar necessário;
- Eliminação de dados: o usuário pode apagar seus dados;
- Informação sobre compartilhamento: delimita com quem os dados serão compartilhados;

- Informação sobre o não consentimento: o usuário avisa que não permite o uso de seus dados e é informado das responsabilidades dessa ação;
- Revogação: altera os termos do consentimento de uso dos dados;
- Reclamação: o usuário poderá informar a ANPD sempre que tiver problemas com o Controlador;
- Oposição: o usuário poderá informar ao Controlador que não concorda com o tratamento dado a seus dados.

No entanto, a LGPD carece de uma legislação de apoio mais clara e definida. Os novos meios de comunicação que surgirão e os novos serviços que estão sendo propostos deverão ser incluídos na legislação de forma mais rápida, para que não haja prejuízo dos serviços, nem dos clientes (SERPRO, 2018).

A proteção de dados e a segurança de redes são aspectos importantes aos usuários da Internet, quer esses usuários sejam pessoas físicas, jurídicas ou entes governamentais.

Todas as tentativas de proteção de dados têm como principal alvo os ataques organizados por grupos de *hackers* e *crackers* que têm sido cada vez mais comuns e com um poder de penetração maior.

Muitos ataques visam, muitas vezes, apenas criar pânico, e não têm como propósito o roubo de dados e equipamentos. No entanto existem ataques mais elaborados, como os conhecidos *Ransonware*, que têm como objetivo “sequestrar” determinado dispositivo ou rede e exigir o pagamento de altas quantias, normalmente em moedas virtuais.

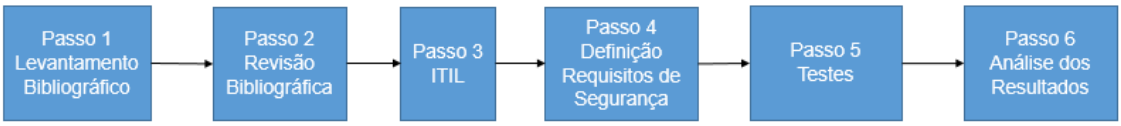
Em 20/10/2020 o Senado Federal aprovou as nomeações para a ANPD (SERPRO, 2020) e em 06/11/2020 o Diário Oficial da União trouxe os nomes dos membros do Conselho Diretor da mesma que passou a atuar conforme previsto em lei.

Doravante cabe agora à ANPD fiscalizar e aplicar sanções, mediante processo administrativo, quando o tratamento de dados ocorrer em desconformidade com a legislação de proteção de dados vigente.

3 METODOLOGIA

Este capítulo descreve a metodologia adotada neste trabalho. A figura 12 apresenta os principais passos dessa metodologia.

Figura 12 – Fluxograma da Metodologia



Fonte: Do próprio autor, 2021

Passo 1: Levantamento Bibliográfico acerca dos principais desafios relacionados aos aspectos de segurança em redes IoT e seus requisitos de implantação.

Passo 2: Revisão Bibliográfica acerca das melhores práticas de segurança de redes de maneira geral.

Passo 3: Identificou-se o ITIL como um meio de gestão de redes com características mais próximas das redes IoT.

Passo 4: Definição dos requisitos de segurança em uma rede IoT a serem analisados com base no ITIL – nível de segurança e nível de força.

Passo 5: Realização de Testes visando a análise do nível de segurança e nível de força em redes IoT.

Passo 6: Análise dos requisitos (nível de segurança e nível de força)

3.1 Descrição da Proposta

Como já foi dito os dispositivos IoT e suas redes necessitam de uma melhoria em seus aspectos de segurança, mas que não prejudiquem as qualidades e especificidades deles. Como este objetivo verificou-se que uma alternativa para melhoria da segurança seria o uso de senhas confiáveis e robustas em todos os dispositivos e redes IoT.

Sendo assim através de uma análise dos requisitos mínimos para que uma senha seja considerada forte (com elevado nível de segurança) foram criadas senhas no aplicativo gratuito *Safe in Cloud*.

Neste aplicativo é possível escolher alguns parâmetros e definições para as senhas como: quantidade de caracteres (tamanho da senha) e complexidade dos caracteres que é a possibilidade de usar-se somente números, números e letras ou números, letras e caracteres especiais.

Quando a senha é gerada, o próprio aplicativo já indica o nível de segurança, que é calculado através de um algoritmo próprio, e que indica o tempo necessário para essa senha ser quebrada.

Não se obteve acesso às equações usadas no algoritmo próprio do software, mas em testes realizados que serão descritos no capítulo 4 pode-se constatar que a equação utilizada no cálculo do nível de segurança pelo *Software Safe in Cloud* é muito similar a equação da Entropia que é um dos métodos formais usados para se determinar a força de uma senha.

A Entropia, no contexto das senhas, é usada como uma medida de quão aleatória é uma senha. Quanto maior a entropia de uma senha, mais difícil será usar a força bruta para desvendá-la. É medida em bits e a fórmula matemática para calculá-la é:

$$E = log_2 R^L \quad (1)$$

Onde:

- E é Entropia da Senha;
- R é o conjunto de possíveis símbolos* utilizáveis e
- L é quantidade de símbolos* ou a comprimento da senha.

Os testes realizados têm como objetivo verificar a nível de segurança e o nível de força das senhas geradas pelo aplicativo *Safe In Cloud*. Para isso, são utilizados outros dois softwares (ou sites) que verificam o nível de segurança (aplicativo *Kaspersky Password Checker)* e o nível de força (aplicativo *Password Strength Test* da Universidade de Illinois em Chicago).

O nível de força pode ser definido pela somatória dos aspectos positivos e negativos utilizados pelo aplicativo *Password Strenght Test* disponibilizado pela Universidade de Illinois em Chicago através do site (UIC, 2020).

Os aspectos positivos são:

1. Números de caracteres (NC);
2. Letras maiúsculas (LM);
3. Letras minúsculas (LN);
4. Números (N);
5. Símbolos (S);
6. Números e símbolos no meio da senha (NM)
7. Atendimento dos Requisitos Anteriores. (AA)

Os aspectos negativos são:

1. Somente letras (LL);
2. Somente números (NN);
3. Caracteres repetidos (CR);
4. Letras maiúsculas consecutivas (LMC);
5. Letras minúsculas consecutivas (LNC);
6. Números consecutivos (NC);
7. Letras em sequência (LS);
8. Números em sequência (NS);
9. Símbolos em sequência (SS).

Assim o nível de força (nf) de uma senha é calculado por esse aplicativo a partir das seguintes equações:

$$nf = \Sigma\,(\text{aspectos positivos}) - \Sigma\,(\text{aspectos negativos}) \quad (2)$$

$$\text{nf} = (\text{NC} + \text{LM} + \text{LN} + \text{N} + \text{S} + \text{NM} + \text{AA}) - (LL + NN + CR + LMC + LNC + NC + LS + NS + SS) \quad (3)$$

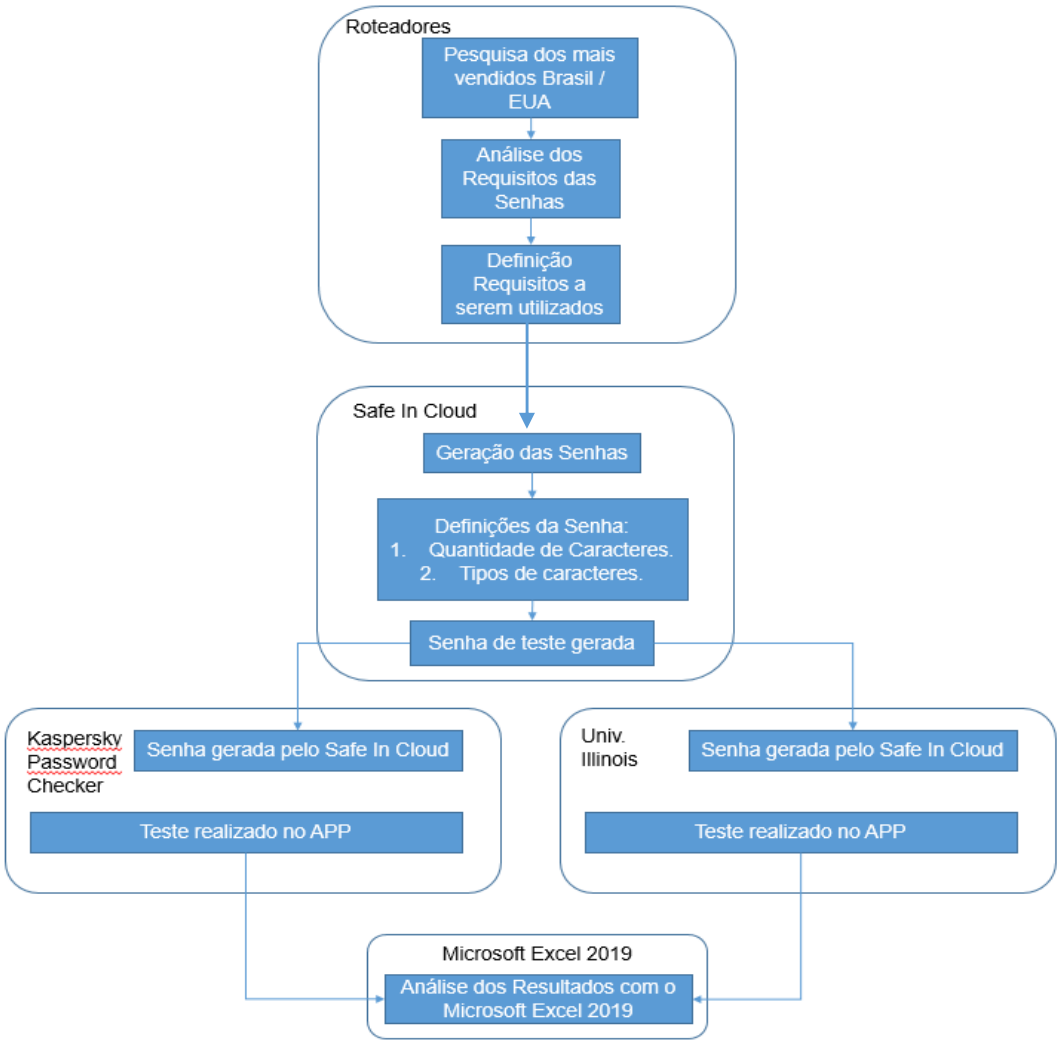
A escolha dos aplicativos foi feita com base no conhecimento do autor sobre a robustez, nível de segurança e nível de força dos aplicativos utilizados.

Os testes foram realizados em quatro etapas:

- Etapa 01: pesquisa dos roteadores e definição dos requisitos das senhas.
- Etapa 02: as senhas foram geradas pelo aplicativo *Safe In Cloud* com a definição da quantidade de caracteres e tipos de caracteres que podem ser usados;
- Etapa 03: realização dos testes usando os aplicativos disponíveis no site da Kaspersky e Universidade de Illinois (KASPERSKY, 2020; UIC, 2020);
- Etapa 04: uso do Microsoft Excel para cálculo da equação 3 (Entropia) e análise dos resultados obtidos com base nos resultados dos aplicativos e de itens pesquisados na literatura.

O fluxograma da Figura 13 mostra a sequência de etapas que foram realizadas:

Figura 13 – Fluxograma das Etapas dos testes.



Fonte: Do próprio autor, 2021

O *software* Microsoft Excel foi usado para o cálculo das equações (1), (2) e (3). Através dos resultados obtidos nele foram feitas as análises de nível de segurança e nível de força.

3.1.1 Testes de Senhas

Para garantir a segurança em dois dos principais pontos de ataque, roteadores e dispositivos periféricos, foram geradas senhas seguindo alguns requisitos:

- Quantidade de caracteres possíveis: 8, 12, 20, 26 e 32. Os valores mínimo e máximo foram escolhidos de acordo com os números

mínimo e máximo existentes nas configurações dos roteadores pesquisados e utilizados nos testes (CONSULTECHRS, 2020; PC MAGAZINE, 2020).

- As possibilidades de uso de caracteres definidos como números, letras maiúsculas e minúsculas e os caracteres especiais foram escolhidas de acordo com as mesmas possibilidades encontradas nos roteadores pesquisados (CONSULTECHRS, 2020; PC MAGAZINE, 2020).

As senhas foram escolhidas utilizando o aplicativo *Safe in Cloud* desenvolvido por SHCHERBAKOV (2020). Este aplicativo está disponível para download de forma gratuita ou paga. O *software* utilizado, neste trabalho, foi a versão gratuita para Windows 7 (v20.4.0) que apresenta a possibilidade de predefinir alguns aspectos das senhas como:

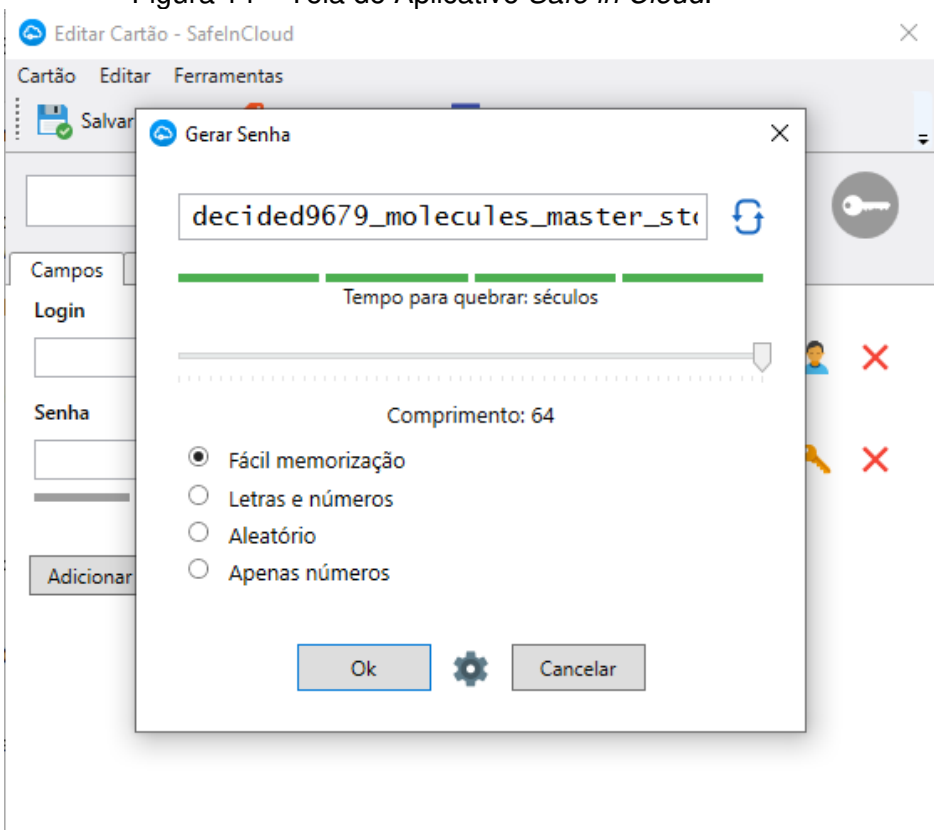
- Quantidade de caracteres possíveis: até 64 caracteres;
- Tipo de memorização: fácil memorização, letras e números, aleatório e apenas números.

O aplicativo *Safe in Cloud* para *smartphones* Android e IOS não foi usado pois a limitação de quantidade de caracteres para as senhas é de 31 caracteres.

Existe, ainda, a versão PRO (20.2.0) para *smartphones* que conta com a possibilidade de compartilhamento para até 6 pessoas poderem consultar as mesmas senhas.

Os cenários dos testes das senhas foram definidos de acordo com o tipo de memorização disponibilizada pelo aplicativo gerador de senhas. A figura 14 mostra a tela do aplicativo com a configuração de 64 caracteres de fácil memorização:

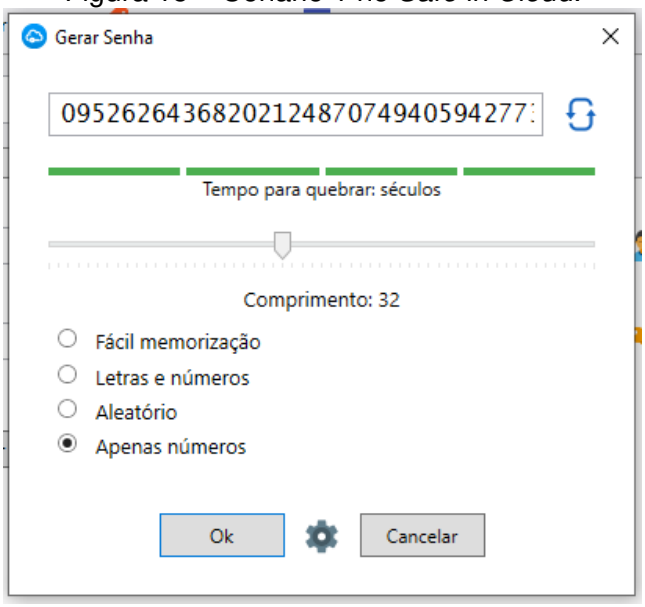
Figura 14 – Tela do Aplicativo *Safe in Cloud*.



Fonte: (SHCHERBAKOV, 2020)

Os cenários foram, então, definidos usando as possiblidades dadas pelo aplicativo, sendo o cenário 1 com apenas números conforme a figura 15:

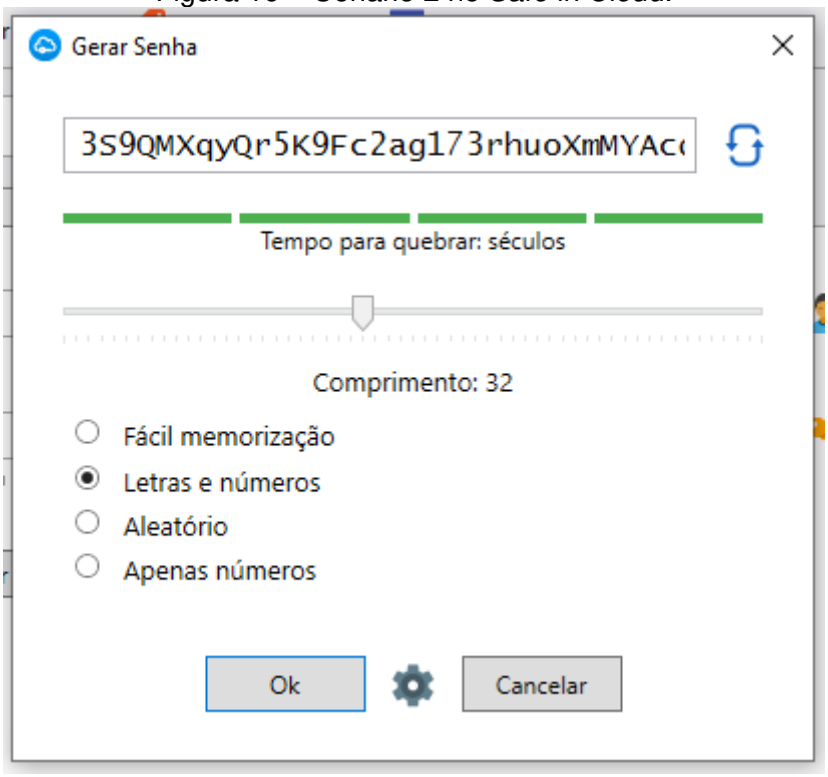
Figura 15 – Cenário 1 no *Safe in Cloud*.



Fonte: (SHCHERBAKOV, 2020)

O cenário 2 com números e letras, conforme na figura 16:

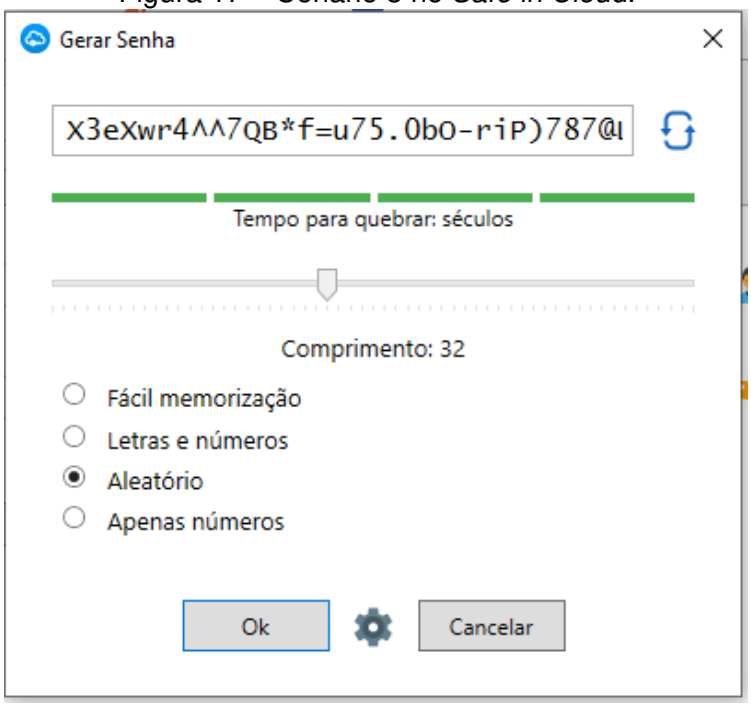
Figura 16 – Cenário 2 no *Safe in Cloud.*



Fonte: (SHCHERBAKOV, 2020)

Já o cenário 3 foi usado na opção Aleatório como pode-se observar na figura 17:

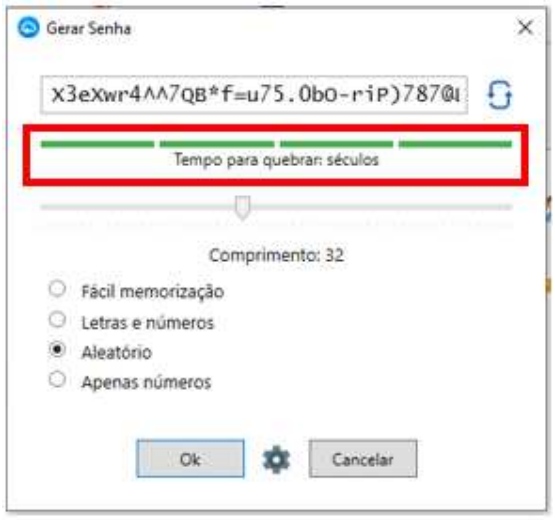
Figura 17 – Cenário 3 no *Safe in Cloud.*



Fonte: (SHCHERBAKOV, 2020)

Com a definição das senhas, passou-se a análise dos requisitos de segurança disponíveis no aplicativo. Na parte destacada na figura 18, o aplicativo disponibiliza o tempo necessário para a quebra da senha de acordo com seus parâmetros de teste que não são divulgados pelo desenvolvedor:

Figura 18 – Parâmetro de quebra de senhas no *Safe in Cloud*.

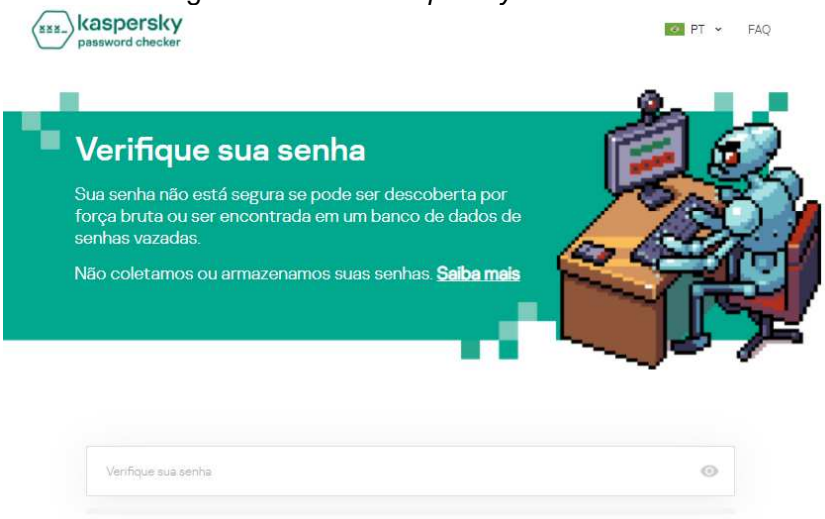


Fonte: (SHCHERBAKOV, 2020)

3.1.2 Aplicativos e Testes Realizados

Outro aplicativo foi usado para uma segunda análise dos parâmetros de quebra de senha. O site *Kaspersky Password Checker*, apresentado na figura 19, também foi usado para classificar o tempo de quebra das senhas geradas pelo aplicativo *Safe in Cloud* (KASPERSKY, 2020).

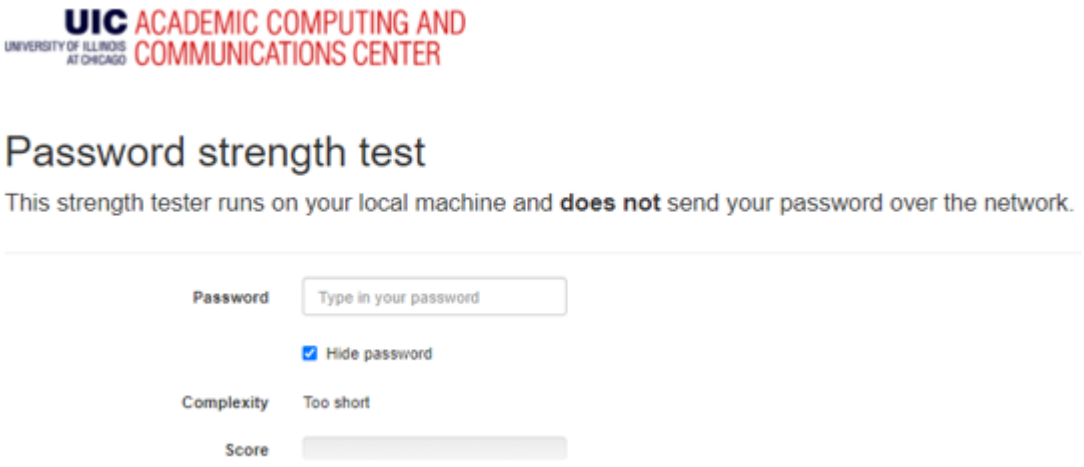
Figura 19 – Site *Kaspersky Password Checker*



Fonte: (KASPERSKY, 2020)

Foi utilizado, também, o site da Universidade de Illinois em Chicago que analisa diversos aspectos positivos e negativos das senhas (forças das senhas) ali inseridas, conforme ilustrado na figura 20:

Figura 20 – *Password Strength Test* da Universidade de Illinois



Fonte: (UIC), 2020)

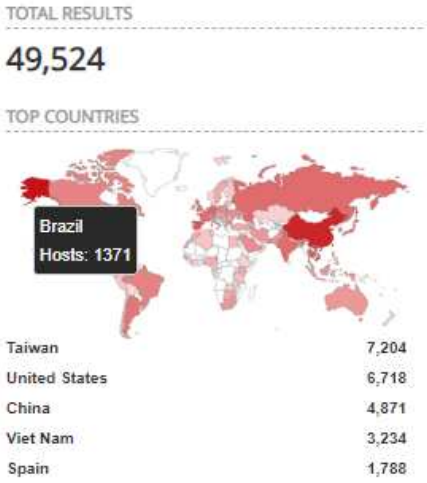
O detalhamento dos aspectos positivos e negativos utilizados pelo site da Universidade de Illinois está no capítulo 4 “Resultados” deste trabalho.

4 RESULTADOS

Segundo o site SHODAN.IO (2020), existe uma quantidade considerável de dispositivos que não tiveram sua senha de acesso de configuração alterada pelo usuário.

Em uma busca pelos assuntos mais acessados neste site, verificou-se algumas informações muito interessantes sobre segurança de redes. O primeiro assunto é relacionado ao uso de Senha de Fábrica em roteadores. Nessa pesquisa, foram encontrados 49.524 equipamentos, em todo o mundo, que não tiveram sua senha alterada, conforme pode-se verificar na Figura 21.

Figura 21 - Busca por Senhas Padrão.



Fonte: (SHODAN.IO, 2020)

Também é possível verificar os dispositivos que utilizam como senha de configuração a palavra “Admin”, compartilhando uma senha amplamente divulgada pelos fabricantes com inúmeros outros dispositivos, o que torna a segurança desses dispositivos bastante frágil. A Figura 22 ilustra os países no mundo onde essa senha é mais utilizada.

Figura 22 - Busca por senha “Admin”.

Fonte: (SHODAN.IO, 2020)

Conforme pode-se observar na Figura 22, o Brasil é o líder no uso de senha “ADMIN”. Com isso, diversas redes brasileiras têm esta fragilidade que é amplamente usada para ataques de intrusão.

Segundo a referência (TELECO , 2019), existiam, em 2018, cerca de 32,6 milhões de conexões de Banda Larga no Brasil e 116,46 milhões nos Estados Unidos. Se for feita uma análise das redes com os problemas mais comuns identificados pelo Shodan.io (uso de senha padrão do fabricante e senha “Admin”), têm-se os seguintes dados:

Tabela 1 - Comparativo de Redes Brasil x EUA

Comparativo de Redes	**BRASIL**	**EUA**
Número de Redes com problemas (Shodan.io)	17889	10946
Quantidade de conexões de Banda Larga (2018)	31200000	116467000
Porcentagem (%)	0,057%	0,009%

Fonte: Do próprio autor com dados do site (TELECO , 2019)

A partir da análise da Tabela 1, pode-se concluir que as redes brasileiras apresentam seis vezes mais problemas que as redes dos Estados Unidos o que torna os usuários brasileiros alvos mais fáceis de ataques.

Exatamente por entender-se que o uso de uma senha diferente do padrão, personalizada e exclusiva é de extrema importância na segurança das

redes IoT, foi realizada uma pesquisa a respeito dos roteadores mais vendidos no Brasil e nos Estados Unidos.

Os roteadores constituem-se em um ponto extremamente vulnerável do ponto de vista da segurança de redes, mas muitas vezes os usuários acabam entendendo que como o acesso físico não pode ser realizado, não há motivos para preocupação. Desse modo, acabam relaxando e deixam a senha padrão ativa. Os resultados com relação aos roteadores são apresentados no item que se segue.

4.1 Roteadores Analisados

Os resultados conseguidos pela análise de artigos sobre criptografia e sobre configurações dos roteadores mais vendidos no Brasil e nos Estados Unidos, mostram que somente o uso de senhas onde a escolha da senha seja realizada apenas por uma escolha livre do usuário não é suficiente para garantir a segurança das pequenas e médias redes de IoT (SOARES, ARAÚJO, & SOUZA, 2020).

Segundo FERNÁNDES-CARAMÉS e FRAGA-LAMAS (2020), nos mais populares sistemas de criptografia, há diferentes níveis de segurança entre as duas chaves simétricas e assimétricas atualmente usadas. As chaves simétricas recebem esse nome pois a mesma chave secreta é usada no processo de encriptação e decriptação da mensagem. As chaves assimétricas possuem duas chaves diferentes, uma privada (usada no processo de encriptação) e outra pública (usada no processo de decriptação), portanto requerem maior tempo para serem processadas.

Um fator que influencia na decisão do nível de segurança a ser usado nas redes é o tipo de chave que será usado. Na Tabela 2, percebe-se que o nível de segurança mais elevado depende de uma quantidade grande de bits de

criptografia para cada chave. No entanto quanto maior o número de bits da chave de segurança, maior a capacidade de processamento e consumo de energia para processá-la, o que pode se configurar como um problema no caso das redes IoT.

Tabela 2 - Nível de segurança de referência para criptossistemas populares simétricos e assimétricos

Nível de Segurança	Quantidade de operações para encontrar a chave	TIPO DE CHAVE		
		PRIVADA	PÚBLICA	
		Tamanho da Chave Simétrica Criptografada	Tamanho da Chave RSA	Tamanho da Chave Elíptica ECDSA
80	1,21E+24	2TDEA (112 bits)	1024 bits	prime192v1 (192 bits)
112	5,19E+33	3TDEA (168 bits)	2048 bits	secp224r1 (224 bits)
128	3,40E+38	AES-128 (128 bits)	3072 bits	secp256r1 (256 bits)
192	6,28E+57	AES-192 (192 bits)	7680 bits	secp384r1 (384 bits)

Fonte: (FERNÁNDES-CARAMÉS e FRAGA-LAMAS, 2020)

Os tipos de chaves que são mostradas na Tabela 2 são:

- TDEA (*Triple Data Encryption Algorithm* – Algoritmo Triplo de Encriptação de Dados): é um tipo de chave simétrica que criptografa os dados por três vezes usando um algoritmo de 56 bits.
    - 2TDEA (*Two-key Triple Data Encryption Algorithm* - Algoritmo Triplo de Encriptação de Dados com chave dupla): utiliza duas chaves de encriptação em cada transmissão.
    - 3TDEA (*Three-key Triple Data Encryption Algorithm* - Algoritmo Triplo de Encriptação de Dados com chave tripla): utiliza três chaves de encriptação em cada transmissão.
- AES (*Advanced Encryption Standard* – Padrão de Encriptação Avançado): padronizada pelo NIST (*National Institute of Standards and Technology* – Instituto Nacional de Padrões e Tecnologia) como uma das mais seguras chaves simétricas usadas. O número que a acompanha está relacionado ao nível de segurança e a quantidade de bits que a compõe (NIST, 2016).
- RSA (Rivest, Shamir, Adleman): é um sistema de criptografia assimétrico onde a chave usada para encriptar os dados é pública

e a chave usada para decriptação é privada. Leva os nomes dos seus criadores: Ron Rivest, Adi Shamir e Leonard Adleman (AUFA, ENDROYONO e AFFANDI, 2018).

- ECDSA (*Elliptic Curve Digital Signature Algorithm* - Algoritmo de Assinatura Digital de Curvas Elípticas): usa equações baseadas em curvas elípticas pré-definidas onde os valores das chaves usados são definidos por uma equação e as chaves usadas no processo de encriptação e decriptação são as variáveis da equação (NIST, 2013).

Outras vantagens e desvantagens do uso das chaves simétrica e assimétrica são mostradas na tabela 3:

Tabela 3 **-** Vantagens e Desvantagens em Encriptação Simétrica e Assimétrica.

TIPOS	VANTAGENS	DESVANTAGENS
SIMÉTRICA	Segurança Forte	Troca de Chaves Segura
	Desempenho Mais Rápido	Gerente de Chaves
	Menos Recursos de Computação	
ASSIMÉTRICA	Usos Múltiplos (Autenticação, Controle de Acesso, Confidencialidade e Privacidade, Integridade de Dados e Não-Repúdio)	Requer Chaves Maiores para Segurança Equivalente a Simétrica
	Altamente Escalável	Desempenho Mais Lento
	Sem Gerenciamento de Chaves	Computacionalmente Intensivo

Fonte: (MILLER, 2016)

A vantagem mais importante para o uso de chaves simétricas para as pequenas redes de IoT está no fato de que é possível transmiti-las em um mesmo canal que a informação criptografada e que por ter um desempenho mais lento necessita de menor capacidade de processamento, pois são chaves menos complexas do que as chaves assimétricas.

Como as chaves simétricas são as mais indicadas para uso em redes IoT, verificando os tipos de chave simétricas apresentados na Tabela 2 e que de acordo com NIST (2016) podem ser usadas definiu-se que o tipo de chave que será usado como parâmetro para os testes realizados neste trabalho será o AES-128bits, que possui Q_{op}= 3,40*e^{+38}.

Através de pesquisas em sites de lojas, revistas da área de informática e sites com comparativos de roteadores, foram encontrados os modelos mais vendidos no Brasil e nos Estados Unidos da América (ZOOM, 2020; CONSULTECHRS, 2020; MELHOR DO LAR, 2020; PC MAGAZINE, 2020; TECHRADAR, 2020; WESTOVER, 2020).

Esses roteadores foram comparados de acordo com o tipo de segurança existente nas suas configurações de redes sem-fio (*Wireless*), a quantidade de caracteres da senha e a quantidade de possíveis caracteres que podem ser usados nas senhas de cada um deles, conforme apresentado nas Tabelas 4 e 5.

Conforme pode-se observar nessas tabelas, somente um dentre os roteadores mais vendidos (ASUS RT AC68-U) não apresenta o tamanho máximo da senha com 63 caracteres. Outro fato importante é que todos eles aceitam o uso de caracteres especiais e os modelos vendidos no Brasil, do fabricante TP-Link, aceitam, ainda, 120 caracteres da tabela ASCII (*American Standard Code for Information Interchange* - Código Padrão Americano para Intercâmbio de Informações).

Tabela 4 - Roteadores mais vendidos no Brasil em 2019.

BRASIL	Tipos de Protocolos de Segurança	Tamanho da Senha (quantidade de caracteres)		Tipos de Caracteres Permitidos na Senha	Caracteres possíveis
		Mínimo	Máximo		
D-Link DIR-615	WPA2 / WPA2-PSK / WPA / WPA-PSK	8	63	Números, Letras, Caracteres Especiais, Espaço	90
TP-Link Archer C60	WPA2-PSK / WPA-PSK	8	63	ASCII	120
Asus RT-AC68U	WPA / WPA2 PERSONAL / WPA AUTO-PERSONAL / WPA ENTERPRISE / WPA2 ENTERPRISE / WPA AUTO-ENTERPRISE / RADIUS WITH 802.1X	8	32	Números, Letras, Caracteres Especiais, Espaço	90
TP-Link Archer C6	WPA-PERSONAL / WPA-3-PERSONAL / WPA-PERSONAL	8	63	ASCII	120
D-Link DIR 822	WPA2 / WPA2-PSK / WPA / WPA-PSK	8	63	Números, Letras, Caracteres Especiais, Espaço	90
TP-Link Archer C50	WPA-PERSONAL / WPA-3-PERSONAL / WPA-PERSONAL	8	63	ASCII	120
D-Link DIR-819	WPA2 / WPA2-PSK / WPA / WPA-PSK	8	63	Números, Letras, Caracteres Especiais, Espaço	90

Fonte: Do próprio autor, 2021

Tabela 5. Roteadores mais vendidos nos Estados Unidos em 2019.

ESTADOS UNIDOS	Tipos de Protocolos de Segurança	Tamanho da Senha (Quantidade de caracteres)		Tipos de Caracteres Permitidos na Senha	Caracteres Possíveis
		Mínimo	Máximo		
Google Nest Wi-fi	WPA2 / WPA2-PSK / WPA / WPA-PSK	8	63	Números, Letras, Caracteres Especiais, Espaço	90
TP-Link Archer C5400 v2	WPA2 / WPA2-PSK / WPA / WPA-PSK	8	63	Números, Letras, Caracteres Especiais, Espaço	90
TP Link Archer A7	WPA2 / WPA2-PSK / WPA / WPA-PSK	8	63	Números, Letras, Caracteres Especiais, Espaço	90
Eero Home Wi-Fi System	WPA2 PSK	8	63	Números, Letras, Caracteres Especiais, Espaço	90

Fonte: Do próprio autor, 2021

Os testes que foram realizados são descritos no Item 3.1 do Capítulo “Metodologia”, onde foram explicitados os requisitos usados para a definição das senhas que foram usadas nos testes.

Essa informação da quantidade de caracteres de cada roteador foi usada na geração das senhas de testes. Como um dos roteadores pesquisados apresenta 32 caracteres como quantidade máxima de caracteres, este foi o valor máximo escolhido. Desse modo, foram escolhidos outros valores abaixo do máximo (32 caracteres), que representam o que normalmente é usado, além do mínimo valor presente em todos os roteadores (8 caracteres).

Por esse motivo, os tamanhos das senhas foram definidos em: 32, 26, 20, 12 e 8 caracteres. As senhas usadas nos testes foram geradas através do aplicativo *Safe In Cloud* (versão 20.4.0) para Windows 7 (SHCHERBAKOV, 2020).

Outro fator determinante para a geração das senhas de teste foi quais os caracteres que podem ser usados. Assim, foram definidos três grupos:

1. Cenário 1: Somente Números: de 0 a 9 – totalizando dez possibilidades;
2. Cenário 2: Números e Letras: de 0 a 9, letras maiúsculas e minúsculas de A a Z (no alfabeto em português) + K, Y e W (maiúsculos e minúsculos) – totalizando 62 possibilidades;
3. Cenário 3: Números, Letras e Caracteres especiais: igual ao anterior mais os seguintes caracteres: “, !, @, #, $, %, &, *, (,), _, -, +, =, ?, /, \, ‘ , <, > , [,], {, }, . , |, § , ;, : - totalizando 90 possibilidades.

Com base nos cenários descritos anteriormente, obteve-se as seguintes senhas, apresentadas na Tabela 6.

A partir das senhas definidas na Tabela 6, foram realizados testes no aplicativo gerador de senhas *Safe in Cloud* (SHCHERBAKOV, 2020) e no site da empresa Kaspersky (KASPERSKY, 2020) para verificar qual a resposta dada

pelo algoritmo desses sites na questão da segurança e complexidade (força) de cada senha.

A Tabela 7 apresenta o resultado do teste de segurança das senhas geradas nos aplicativos *Safe In Cloud e Kaspersky.*

Tabela 6 - Senhas Geradas para Testes no Aplicativo *Safe In Cloud*.

Tamanho da senha (quantidade de caracteres)	**8**	**12**	**20**	**26**	**32**
Cenário 1	59622044	398976147931	31018636571252948676	600192395884184641167080l5	150202813172894964859666l9056002
Cenário 2	kr7aghZo	qLQG94E54MWK	M2EJ8K7sgUHyXhFp56yd	LhTyye6Fr4G83L37u63SV33g4Y	Up25Q738YHnJS4M6iPjE289jkWN7s7fH
Cenário 3	-Zt?$nx6	.&\YKj_LV5X&	A{PUek]_s*Y?9SxBGyPS	ar<(J7*nHQ/<KP?M(E4SDb[e5c	/44>C>6dpdB8X5mqL}332tS64(d:Fv6y

Fonte: Do próprio autor, 2021

Tabela 7 - Resultado do teste de nível de segurança das senhas geradas no Aplicativo *Safe In Cloud e* Kaspersky

Cenários	**Tamanho da senha (quantidade de caracteres)**	**8**	**12**	**20**	**26**	**32**
Cenário 1	Tempo para encontrar a senha - Safe in Cloud	2h	2 meses	Séculos	Séculos	Séculos
	Tempo para encontrar a senha - Kaspersky	10h	2 séculos	+10000 séculos	+10000 séculos	+10000 séculos
Cenário 2	Tempo para encontrar a senha - Safe in Cloud	9 anos	Séculos	Séculos	Séculos	Séculos
	Tempo para encontrar a senha - Kaspersky	12 dias	4 séculos	+10000 séculos	+10000 séculos	+10000 séculos
Cenário 3	Tempo para encontrar a senha - Safe in Cloud	Séculos	Séculos	Séculos	Séculos	Séculos
	Tempo para encontrar a senha - Kaspersky	12 dias	4 séculos	+10000 séculos	+10000 séculos	+10000 séculos

Fonte: Do próprio autor, 2021

Se for utilizada a informação de tempo necessário para encontrar cada chave (Tabela 7) para definição do nível de segurança das senhas geradas para teste, tem-se a quantidade de operações necessárias para encontrar cada senha.

Esses valores foram determinados pela equação:

$$Q_{op} = R^L \qquad (4)$$

Onde:

- Q_{op} é a quantidade de operações ou quantidade de senhas possíveis;
- R é o conjunto de possíveis símbolos (pode ser o conjunto de caracteres alfa numérico e caracteres especiais) utilizáveis e

- L é quantidade de símbolos* ou a comprimento da senha.

Aplicando a Eq. (4), que calcula a quantidade de operações necessárias para a quebra de uma senha, para todos os cenários e senhas definidos anteriormente tem-se os valores apresentados na Tabela 08.

Tabela 8 – Números de Senhas Possíveis para os cenários de teste.

Tamanho da Senha (quantidade de caracteres)	**Q_{op} para o Cenário 1**	**Q_{op} para o Cenário 2**	**Q_{op} para o Cenário 3**
8	1,00E+08	2,18E+14	4,30E+15
12	1,00E+12	3,23E+21	2,82E+23
20	1,00E+20	7,04E+35	1,22E+39
26	1,00E+26	4,00E+46	6,46E+50
32	1,00E+32	2,27E+57	3,43E+62

Fonte: Do próprio autor, 2021

Como o valor mínimo definido anteriormente no item 4.1 e com base na Tabela 2, como requisito mínimo é Q_{op}= 3,40*e^{+38}, então os valores acima desse valor indicarão as senhas que poderão ser utilizadas.

Por exemplo: na Tabela 2, o nível de segurança 80 (ns = 80) necessita de 1,21*e^{+24} operações para ser quebrado com isso pode-se concluir, com a Tabela 8, que as senhas que apresentarem valores menores que esse tem nível de segurança inferior a 80.

Todas as correlações entre os níveis de segurança da Tabela 2 e os valores de Q_{op} da Tabela 8 são apresentados na Tabela 9.

Tabela 9 – Correlação entre Níveis de Segurança e Quantidade de Operações necessárias para “quebrar” a senha (correlação entre as Tabelas 2 e 8)

Qop		Nível de Segurança
Valor Mínimo	Valor Máximo	
0	1,21 e+24	ns < 80
1,22 e+24	5,19 e+33	80<ns<112
5,19 e+33	3,40 e+38	112<ns<128
3,40 e+38	6,28 e+57	128<ns<192
acima de 6,28 e+57		ns>192

Fonte: Do próprio autor, 2021

Com base nessa correlação, pode-se considerar que as senhas têm os seguintes níveis de segurança, conforme a Tabela 10.

Tabela 10 - Classificação quanto aos níveis de segurança (ns) das senhas de teste.

Tamanho da Senha (quantidade de caracteres)	**Cenário 1**	**Cenário 2**	**Cenário 3**
8	ns<80	ns<80	ns<80
12	ns <80	ns<80	ns<80
20	ns <80	112 <ns <128	128 < ns < <192
26	80<ns <112	128 < ns <192	128 < ns < <192
32	80<ns <112	128< ns <192	ns >192

Fonte: Do próprio autor, 2021

As células dessa tabela destacadas em amarelo correspondem a um nível de segurança (ns) maior que 128 (ns > 128). Esse valor foi escolhido como limite mínimo de nível de segurança pois é o nível de segurança das chaves criptografadas com protocolo AES-128 que foi criado pelo NIST dos Estados Unidos em 1977 (NIST, 2016) e que possuem nível de segurança aceitáveis para uso em redes.

Com base na Eq. (1) que define a Entropia, verificou-se, também os valores de Entropia das senhas. Os valores das entropias das senhas são apresentados na Tabela 11:

Tabela 11 – Entropia das Senhas

Tamanho da Senha (quantidade de Caracteres)	Entropia para o Cenário 1 (bits)	Entropia para o Cenário 2 (bits)	Entropia para o Cenário 3 (bits)
8	26,5754248	47,63357	51,93482
12	39,8631371	71,45036	77,90224
20	66,4385619	119,0839	129,8371
26	86,3701305	154,8091	168,7882
32	106,301699	190,5343	207,7393

Fonte: Do próprio autor, 2021

Os valores mostrados na Tabela 11 e marcados em amarelo, indicam as senhas que possuem Entropia, conforme calculado pela Eq. (1), superior ao valor da Entropia de uma chave simétrica AES-128 que é 43,8301, demonstrado abaixo:

$$E = log_2 R^L = L * log_2 R = 128 * log_2 2 = 43{,}8301 \qquad (5)$$

Onde:

- R = 2: o conjunto de possíveis símbolos da chave AES-128 (cada bit pode ser “0”(nível lógico baixo) e “1” (nível lógico alto));
- L = 128: quantidade de bits na chave AES-128.

Considerando, agora, os resultados dos testes para a determinação do nível de força (nf) a partir do testador da Universidade de Illinois. A partir da Eq. (2) pode-se determinar o nível de força das senhas conforme apresentado na Tabela 12.

Pode-se concluir que a menor senha que apresenta os parâmetros mínimos de segurança é uma senha com 20 caracteres e que possa usar 90 caracteres diferentes (Cenário 3) pois das senhas que satisfazem aos três testes realizados é aquela que possui menor quantidade de caracteres e, portanto, é mais fácil de ser memorizada.

Desse modo pode-se concluir também, que o nível de força mínimo aceitável para uma senha segura é de 171 pontos (nf = 170). Na Tabela 12, os valores destacados em amarelo correspondem a níveis de força maiores ou iguais ao mínimo (nf ≥ 170).

Tabela 12 - Resultado do *Password strenght test*.

Resultado UIC	**Cenário 1**					**Cenário 2**					**Cenário 3**				
Tamanho da Senha (Quantidade de Caracteres)	8	12	20	26	32	8	12	20	26	32	8	12	20	26	32
Nível de Força	19	32	52	74	82	58	99	157	237	277	90	123	171	261	333

Fonte: (UIC, 2020)

Utilizando os dados obtidos no testador da Universidade de Illinois (Tabela 12) junto aos dados obtidos na Tabela 8, tem-se os resultados a seguir, na Tabela 13:

Tabela 13 - Qualificação das Senhas de Teste.

Tamanho da Senha (Quantidade de Caracteres	**Cenário 1**	**Cenário 2**	**Cenário 3**	**Nível de Segurança / Entropia / Nível de Força**
8	<80	<80	<80	Nivel de Segurança (Qop)
	26,57542476	47,63357048	51,93482477	Entropia
	19	58	90	Nível de Força
12	<80	<80	<80	Nivel de Segurança (Qop)
	39,86313714	71,45035572	77,90223716	Entropia
	32	99	123	Nível de Força
20	<80	>112 / <128	>128 / <192	Nivel de Segurança (Qop)
	66,4385619	119,0839262	129,8370619	Entropia
	52	157	171	Nível de Força
26	>80 / <112	>128 / <192	>128 / <192	Nivel de Segurança (Qop)
	86,37013047	154,8091041	168,7881805	Entropia
	74	237	261	Nível de Força
32	>80 / <112	>128 / <192	>192	Nivel de Segurança (Qop)
	106,301699	190,5342819	207,7392991	Entropia
	82	277	333	Nível de Força

Fonte: Do próprio autor, 2021

Na Tabela 13 as células marcadas em azul indicam para cada um dos cenários as senhas que foram aprovadas em cada teste realizado individualmente.

Tabela 14 – Senhas qualificadas em todos os testes simultaneamente

Tamanho da Senha (Quantidade de Caracteres	**Cenário 1**	**Cenário 2**	**Cenário 3**	**Nível de Segurança / Entropia / Nível de Força**
8	<80	<80	<80	Nivel de Segurança (Qop)
	26,57542476	47,63357048	51,93482477	Entropia
	19	58	90	Nível de Força
12	<80	<80	<80	Nivel de Segurança (Qop)
	39,86313714	71,45035572	77,90223716	Entropia
	32	99	123	Nível de Força
20	<80	>112 / <128	>128 / <192	Nivel de Segurança (Qop)
	66,4385619	119,0839262	129,8370619	Entropia
	52	157	171	Nível de Força
26	>80 / <112	>128 / <192	>128 / <192	Nivel de Segurança (Qop)
	86,37013047	154,8091041	168,7881805	Entropia
	74	237	261	Nível de Força
32	>80 / <112	>128 / <192	>192	Nivel de Segurança (Qop)
	106,301699	190,5342819	207,7392991	Entropia
	82	277	333	Nível de Força

Fonte: Do próprio autor, 2021

As células na Tabela 14 marcadas em amarelo indicam as senhas que satisfazem aos três testes realizados simultaneamente:

1. Nível de Segurança: através da Tabela 2, definido o padrão da chave de criptografia aceitável como AES-128 que apresenta $Q_{op} = 3{,}40*e^{+38}$ e os demais a partir do Q_{op} calculados pela Eq. 4 e que apresenta os resultados na Tabela 08.
2. Entropia: a Entropia calculada pela Eq. (1) mostra que a chave AES-128 apresenta E =43,8301bits, conforme calculado pela Eq. (5). Calculando pela mesma equação a Entropia das senhas e cenários analisados tem-se a Tabela 11.

3. Nível de Força: pela análise fornecida pelo aplicativo da Universidade de Illinois em Chicago tem-se que o nível mínimo que garanta a segurança de uma senha é 177.

As senhas aprovadas simultaneamente nos três testes realizados estão marcadas em amarelo na Tabela 15.

Tabela 15 - Senhas Geradas para Testes no Aplicativo *Safe in Cloud* que podem ser utilizadas

Tamanho da senha (quantidade de caracteres)	**8**	**12**	**20**	**26**	**32**
Cenário 1	59622044	398976147931	31018636571252948676	600192395884184641167080l5	150202813172894964859666l9056002
Cenário 2	kr7aghZo	qLQG94E54MWK	M2EJ8K7sgUHyXhFp56yd	LhTyye6Fr4G83L37u63SV33g4Y	Up25Q738YHnJS4M6iPjE289jkWN7s7fH
Cenário 3	-Zt?$nx6	.&\YKj_LV5X&	A{PUek]_s*Y?9SxBGyPS	ar<(J7*nHQ/<KP?M(E4SDb[e5c	/44>C>6dpdB8X5mqL}332tS64(d:Fv6y

Fonte: Do próprio autor, 2021

Conclui-se que a senha mais indicada é uma que possua 20 caracteres no mínimo e que use números, letras e caracteres especiais (Cenário 3) – por, primariamente, possuir a menor quantidade de caracteres dentre as senhas possíveis.

Além disso, a senha com 20 caracteres possui o nível de segurança superior a 128 de acordo com (FERNÁNDES-CARAMÉS e FRAGA-LAMAS 2020), Entropia superior a 43, 8301 bits e o nível de força é superior àquele indicado nas análises feitas por (UIC, 2020) que foi de 171 pontos.

Uma senha pode ser uma frase onde algumas letras sejam trocadas por números e caracteres especiais, tornando-a assim mais complexa de ser quebrada.

As senhas de 26 e 32 caracteres também apresentam níveis de segurança adequados e mesmo aquelas somente com números e letras (Cenário 2) poderão ser usadas conforme destacado na Tabela 15. No entanto, a quantidade de caracteres pode gerar um problema na memorização da senha, por isso optou-se pela menor quantidade de caracteres que atendam aos requisitos de segurança.

As senhas que não foram aprovadas concomitantemente nos três testes realizados e devem ser evitadas estão destacadas em amarelo na Tabela 16:

Tabela 16. Senhas Geradas para Testes no Aplicativo *Safe In Cloud* que não devem ser utilizadas.

Tamanho da senha (quantidade de caracteres)	**8**	**12**	**20**	**26**	**32**
Cenário 1	59622044	398976147931	31018636571252948676	60019239588418464116708015	150202813172894964859666190560 02
Cenário 2	kr7aghZo	qLQG94E54MWK	M2EJ8K7sgUHyXhFp56yd	LhTyye6Fr4G83L37u63SV33g4Y	Up25Q738YHnJS4M6iPjE289jkWN7s7fH
Cenário 3	-Zt?$nx6	.&\YKj_LV5X&	A{PUek]_s*Y?9SxBGyPS	ar<(J7*nHQ/<KP?M(E4SDb[e5c	/44>C>6dpdB8X5mqL}332tS64(d:Fv6y

Fonte: Do próprio autor, 2021

4.2 Dispositivos IoT

Nas pesquisas sobre a garantia de segurança para os dispositivos IoT separa-se muitas vezes os dispositivos em dois tipos: controladores e sensores (BASTA, BASTA e BROWN, 2014). Os dispositivos controladores são aqueles que recebem os dados, enviam os dados para armazenamento, determinam como os sensores e outros equipamentos atuam e se comunicam com o roteador que garante acesso à Internet.

Os sensores podem ser os mais variados e são os responsáveis pela aquisição de dados, captura de imagens, leitura de cartões e *tags (*Etiquetas que utilizam sensores RFID). A conexão do controlador com os sensores e outros dispositivos na ponta das redes deve ser realizada somente com o uso de uma senha ou então de um certificado digital (BASTA, BASTA e BROWN, 2014).

Devido a limitada capacidade de processamento e a disponibilidade de energia, o uso de certificados digitais com chaves privadas ou chaves simétricas são mais adequados por demandarem menos tempo para serem processadas.

O maior problema no compartilhamento de chave privadas é que a chave precisa ser compartilhada por um canal criptografado e a mensagem criptografada enviada por outro canal. No caso das pequenas e médias redes de IoT (escopo desse trabalho) não há esse problema, pois, a chave será conhecida do controlador e será conhecida pelo sensor já que ambos são configurados e integrados à rede pelo mesmo administrador.

O uso nos dispositivos de IoT de senhas que tenham nível de segurança mínimo de 128 poderá, também, garantir a segurança nos dispositivos em questão. Esse nível de segurança em 128 foi escolhido por tratar-se do nível de segurança da chave simétrica AES-128bits padronizada pelo NIST e classificada como aceitável quando trata-se de uma chave simétrica (NIST, 2019).

Outro fato importante de ser mencionado é que como há limitação de processamento dos dispositivos controladores de redes IoT tudo o que envolve seu uso fica mais complicado.

A plataforma mais comum de prototipagem usada no Brasil é o Arduino.

De acordo com MONK (2014) um programa de testes levou 28 segundos para ser executado em um Arduino Uno, enquanto em um MacBook PRO 2,5GHZ levou 0,068 segundos. Isso significa que o Arduino é 400 vezes mais lento que o notebook.

Conclui-se que qualquer implementação ou aplicação para rede IoT de pequeno porte tem obrigatoriamente levar em consideração a limitada capacidade de processamento.

4.3 Proposição de Requisitos de Segurança para Rede de IoT de Pequeno Porte

Em virtude do que foi obtido através dos testes e estudos realizados pode-se concluir que em uma rede IoT residencial e de pequeno porte, deve-se garantir que:

1. A senha a ser utilizada no roteador entre os dispositivos IoT e a Internet deve seguir alguns requisitos:
    a. Ter pelo menos 20 caracteres de tamanho;
    b. Utilizar números, letras e caracteres especiais;
2. A senha utilizada nos dispositivos de controle e sensores das redes IoT também deve contar com uma senha que obedeça aos mesmos critérios dos roteadores.
3. As senhas não devem ser compartilhadas com pessoas que não devem ter acesso aos dados e informações que trafegam pela rede IoT residencial ou de pequeno porte.

5 CONCLUSÕES

A análise de requisitos para uma gestão segura de uma rede IoT residencial ou de pequeno porte é muito dependente de ações do usuário para garantir sua segurança.

Dessa forma não é apenas o uso de senhas que correspondam aos requisitos analisados que farão com que a rede IoT seja segura.

Os requisitos analisados que ajudam a melhorar a segurança das redes IoT é o uso de senhas com as seguintes características:

1. Uso de senhas com pelo menos 20 caracteres;
2. Uso do conjunto de caracteres que engloba números, letras maiúsculas e minúsculas e caracteres especiais;
3. Garantir que as senhas sejam mantidas em segredo e somente os usuários autenticados possam ter acesso à rede IoT.

A segurança em redes IoT é um vasto campo de estudo, seja na análise comportamental do usuário até o desenvolvimento de softwares que necessitem de baixo processamento e disponibilidade de energia, por isso pode ser explorado em diversos aspectos. Neste sentido o usuário deve entender que, apesar de sua rede ser residencial, ela pode ser atrativa a uma invasão exatamente por não possuir uma segurança aprimorada. Essa conscientização pode levá-lo ao uso de senhas nos roteadores e dispositivos periféricos, de acordo com os requisitos propostos neste trabalho.

O uso de roteadores que possuam a possibilidade de uso das senhas acima também é um fator que contribuirá para a segurança da rede IoT. Outro aspecto que deve ser usado quando da escolha das senhas é o uso do aplicativo disponível no site Shodan.io que verifica a segurança das senhas.

Em trabalhos futuros poderão ser desenvolvidos os seguintes temas:

- Certificados digitais que usem chave simétricas transmitidas através do mesmo canal de comunicação dos dados;
- Desenvolvimento de softwares que necessitem de baixo processamento e pouca disponibilidade de energia se explorado adequadamente poderá fazer com que as redes IoT ganhem cada vez mais espaço nas residências e pequenas empresas possibilitando assim um crescimento cada vez maior em seu uso;
- Uso de ferramentas de segurança disponíveis em provedores como Amazon AWS e Microsoft Azure para garantir a segurança da rede IoT.

6 REFERÊNCIAS

A2C BRASIL. *LGPD Lei Geral de Proteção de Dados*, 25 set. 2019. Disponível em: <https://www.a2c.com.br/guias/lgpd-lei-geral-de-protecao-de-dados/>. Acesso em: 11 out. 2019.

ALCÂNTARA, L. K. *Big Data e IoT: Desafios da Privacidade e da Proteção de Dados no DireitoDigital*, ISBN: 9788593745096, São Paulo, 2017. Disponível em: <https://amazon.com/kindle>. Acesso em: 01 jun. 2018.

ALMEIDA JÚNIOR, P. O. B. *ITIL V3 Em 120 minutos e 30 segundos [E-BOOK].* 2019. Disponível em: <https://www.amazon.com.br/ITIL-EM-120-MINUTOSSEGUNDOS-ebook/dp/B07RH4FK57/ref=sr_1_fkmr0_1?__mk_pt_BR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&dchild=1&keywords=ITIL+V3+EM+120+MINUTOS+E+30+SEGUNDO&qid=1594666969&sr=8-1-fkmr0>. Acesso em: 06 maio 2020.

AL-FUQAHA, A., GUIZANI, M., MOHAMMADI, M., ALEDHARI, M. and AYYASH, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communication Surveys & Tutorials*, Nova Iorque, 2015, pp 2347 - 2376. Disponível em: <https://ieeexplore.ieee.org/document/7123563>. Acesso em: 15 jul. 2020.

AMÉRICA, ESTADOS UNIDOS DA. *Electronic Communications Privacy Act [Public Law]*, Washington, 21 out. 1986. Disponível em: <https://itsrio.org/wpcontent/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 10 ago. 2019.

AUFA, F. J. . ENDROYONO, E. and AFFANDI, A. Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm*. 2018 4th International Conference on Science and Technology (ICST)*. Yogyakarta, Indonesia, 2018, pp.1-5.

BARCELLOS, M. Internet de todas as coisas: uma 'nova' internet para uma nova era. Disponível: https://canaltech.com.br/internet/Internet-de-Todas-as-Coisas-uma-nova-internet-para-uma-nova-era/ Acesso em: 22 dez. 2020.

BASTA, A., BASTA, N. e BROWN, M. *Segurança de Computadores e Teste de Invasão*. 2a.. ed. São Paulo: Cengage Learning, 2014, ISBN-13: 9788522117994.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*, Brasília. DF, 23 Abril 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato20112014/2014/lei/l12965.htm>. Acesso em: 26 Set. 2019.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018, LGPD*. 14 Agosto 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato20152018/2018/Lei/L13709.htm>. Acesso em: 26 Set. 2019.

BUFFENOIR, T. Security in the OSI Model. *North-Holland Computer Standards & Interfaces*, Eidhoven, 1, 1988. Vol. 7(1-2), 145-150. Disponível em: < https://doi.org/10.1016/0920-5489(88)90059-1>. Acesso em: 17 set. 2019.

BURHAN, M., REHMAN, R. A., KHAN, B. and KIM, B.S. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors,* 2018, *18*(9), 2796; <https://doi.org/10.3390/s18092796> Acesso em: 23 ago. 2019.

CARRION, P.; QUARESMA, M. Internet das Coisas (IoT): Definições e aplicabilidade aos usuários finais. *Human Factors Design*, Florianópolis,SC, v. 8 (15), pp. 49-66, 2019. Acesso em: 21 maio 2020.

CARVALHO, V. M. Detecção automatizada de dispositivos Internet of Things (IOT) com credenciais de acesso padrão, utilizando shodan e python. Brasília: *Centro de Instrução de Guerra Eletrônica (CIGE)*, 2018. Disponível em: <http://www.bdex.eb.mil.br/jspui/bitstream/123456789/4205/1/2018%20CCIBEROF_TEN%20MINELLI.pdf>. Acesso em: 17 set. 2019.

CHERUVU, S. KUMAR, A., SMITH, N. and WHEELER, D. M. *Demystifying Internet of Thing Security*. 1a. ed. ed. Chandler, AZ, EUA: Apress Open, 2020, 488 páginas.

CISCO. Cisco Annual Internet Report (2018–2023) White Paper. CISCO, 09 Março 2020. Disponível em: <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html>. Acesso em: 10 Maio 2020.

CONSULTECHRS. Roteadores Wireless: os 5 mais vendidos no Brasil.*CONSULTECHRS*, 2020. Disponível em: <https://consultechrs.com.br/2020/05/02/roteadores-wireless-os-5-maisvendidos-no-brasil-em-2020/#page-content>. Acesso em: 02 Maio 2020.

DE LUCCA, J. E. Arquitetura de Segurança para Redes Aplicada a Sistema de Gerência. *Tese de Mestrado UFSC*, Florianópolis, 1995. 106 páginas. Disponível em: <https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/76231/100164.pdf?sequence=1&isAllowed=y>. Acesso em: 30 nov. 2020.

DIAS, R. R. F. *Internet das Coisas sem mistérios: Uma nova inteligência para os negócios.* São Paulo: Netpress Books, ISBN: 9788565794022, 2016.

EGIDIO, L. e UKEI, T. Internet das Coisas (IoT): Uma análise de aplicabilidade. *1º WSEE - Workshop de Sistemas Embarcados da ES670 - FEM - Unicamp*. Campinas, 2015.

ETTER, D. *IoT Security: Pratical Guide Book [E-book]*. São Paulo: [s.n.], 2017. Disponível em: <https://amazon.com/kindle>. Acesso em: 13 ago. 2018.

FABICIACK, D. 1. Introdução ao Gerenciamento de Serviços de TI (GSTI), *Governança de TI e Gerenciamento de Serviços*, 05 dez. 2009. Disponível em: <https://danielfabiciack.wordpress.com/2009/12/05/1-introducao-aogerencimento-de-servicos-de-ti-gsti/>. Acesso em: 04 dez. 2019.

FERNÁNDES-CARAMÉS, T. M. and FRAGA-LAMAS, P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access*, vol. 8, 04 fev. 2020, pp. 21091-21116. Disponível em: <https://ieeexplore-ieeeorg.ez128.periodicos.capes.gov.br/stamp/stamp.jsp?tp=&arnumber=8967098>. Acesso em: 17 out. 2020.

FERREIRA, L. e MONTANHA, G. K. Interferência do sinal Wi-Fi em função dos tipos de barreira. *Tekne e Logos*, Botucatu, v. 8 (2), pp. 73 - 81, Setembro 2017.

FRUSTACI, M., PACE, P., ALOI, G. and, FORTINO, G. Evaluating Critical Security Issues of the IoT World: Present and future Challenges. *IEEE Internet of Things Journal*, vol. 5 (4), 2018, pp. 2483-2495. Disponível em: <https://ieeexplore.ieee.org/document/8086136>. Acesso em: 16 set. 2019.

IMASTERS FÓRUM. www.imasters.com.br. *iMasters*, 09 abr. 2014. Disponível em: <https://imasters.com.br/devsecops/shodan-o-buscador-mais-perigosomundo>. Acesso em: 02 nov. 2020.

JESUS JUNIOR, A. A. e MORENO, E. D. Segurança em Infraestrutura para Internet das Coisas, *Revista Gestão.Org*, v. 13, Edição Especial, 2015, pp. 370-380 2015. Disponível em: <https://doaj.org/article/c89df05024004589997e01f06df279c8>. Acesso em: 06 abr. 2019.

JORNAL OFICIAL DA UNIÃO EUROPÉIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Genebra, Suiça, 2016.

KASPERSKY. Kaspersky Password Checker, 2020. Disponível em: <https://password.kaspersky.com/>. Acesso em: 27 out. 2020.

KUROSE, J. F. e ROSS, K. W. Redes de Computadores e a Internet**:** Uma abordagem top-down. 6º. ed. São Paulo: Pearson Universidades, 2013. 656 páginas.

LAVADO, T. Com maior uso da internet durante a pandemia número de reclamações aumenta. *G1 Economia*, 2020. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/06/11/com-maior-

usoda-internet-durante-pandemia-numero-de-reclamacoes-aumenta-especialistasapontam-problemas-mais-comuns.ghtml>. Acesso em: 13 dez. 2020.

LYRA, M. R. e DUQUE, C. G. Uma proposta de posicionamento da arquitetura da informação no gerenciamento de serviços de TI. *Brazilian Journal of Information Service*, Marília, vol. 5, 2011, pp. 50-55. Disponível em: <http://www2.marilia.Unesp.br/revistas/index.php/bjis/index>. Acesso em: 16 maio 2020.

MACEDO, E. L. C., OLIVEIRA, E. A. R., SILVA, F. H., MELLO Jr, R. R., FRANÇA, F. M. G., DELICATO, F. C., REZENDE, J. F. and MORAES, L. F. M. On the Security Aspects of Internet of Things: A Systematic Literature Review. *JOURNAL OF COMMUNICATIONS AND NETWORKS*, vol. 21(5), out. 2019, pp. 444-457. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8854272>. Acesso em: 05 Abr. 2020

MAHMOUD, R., YOUSUF, T., ALOUL, F. and ZUALKERNAN, I. Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures**.** 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)**,** pp. 336 - 341, 2015. Disponível em:<https://www.researchgate.net/publication/307945826_Internet_of_Things_IoT_ Security_Current_Status_Challenges_and_Countermeasures>. Acesso em: 17 set.2019

MARCACINI, A. T. R. *Aspectos Fundamentais do Marco Civil da Internet: Lei nº 12.965/2014*. São Paulo, ISBN-13: 978-1541333031, 2016. Disponível em: <https://amazon.com/kindle>. Acesso em: 03 set. 2019.

MELHOR DO LAR. MELHOR DO LAR, 2020. Disponivel em: <https://melhordolar.com.br/melhor-roteador-wifi/>. Acesso em: 03 Maio 2020.

MIJUSKOVIC, A.; FERATI, M. User awareness of existing privacy and security risks when storing data in the cloud. *International Conference on eLearning and the Knowledge Society*, European Commission, 2015, pp. 268-273.

MILLER, L. *IOT Security for Dummies: Inside Secure Edition.* 1a edição. ed. Londres: John Wiley & Sons, 2016.

MONK, S. *Programação com Arduino II: Passos Avançados com Sketches.* Tradução de A. LASCHUK. 1a edição. ed. São Paulo: Editora Bookman, 2014. 260páginas.

MORIKANE, C. K. *O Gerenciamento de Serviços de Tecnologia da Informação (TI) em uma Instituição Pública: aplicabilidade da Norma ISO20000 em uma instituição pública de ensino.* Tese de Mestrado, Universidade de Taubaté, 2008, 118 páginas. Disponível em: <http://ppga.com.br/mestrado/2008/morikane-carlos_koji.pdf>. Acesso em: 06 Maio 2020.

MOSENIA, A. and JHA, N. K. A Comprehensive Study of Security of Internet-of-Things. *IEEE Transactions on Emerging Topics in Computing*, Princeton, NJ, 06 Dezembro 2017. Disponível em: <https://ieeexplore-ieee-org.ez128.periodicos.capes.gov.br/document/7562568>. Acesso em: 26 Abr. 2019.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Signature Standard (DSS)*. Gaithersburg:, v. 1, 2013, 128 páginas. Disponível em: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>. Acesso em: 22 Out. 2020.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST Special Publication 800-57 Part 1 Revision 4: Recommendation for Key Management, *Part 1: General. 4a. revisão. ed. Gaithersburg*, v. 1, 2016, 160 páginas. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.80057pt1r4.pdf >. Acesso em: 08 Out. 2020.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST Special Publication 800-131A Revision 2: Transitioning the Use of Cryptographic Algorithms and Key Lengths. *1a. ed. Gaithersburg*: v. 1, 2019, 33 páginas. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800131Ar2.pdf> . Acesso em: 08 Out. 2020.

OLHAR DIGITAL. Hackers invadem sistema de casa e infernizam moradores. *OLHAR DIGITAL*, 2019. Disponível em: <https://olhardigital.com.br/2019/09/24/seguranca/hackers-invadem-sistema-de-casa-e-infernizam-moradores/>. Acesso em: 01 Dez. 2020.

PALANZA, S. Internet of things, big data e privacy: la tríade del futuro. *Documenti Istituto Affari Internazionali*, Roma, 2016. Disponível em: <http:// www.iai.it/ en/ pubblicazioni/ internet-things-big-data-e-privacy>. Acesso em: 05 Jul. 2018.

PATEL, A. Security Management for OSI networks. *Computer Communications*, Dublin, 17, n. 7, 07 jul. 1994, pp. 544-553. Disponível em:

<https://www.sciencedirect.com/science/article/abs/pii/0140366494901090>. Acesso em: 20 Abr. 2019.

PATEL, K., PATEL, S., SCHOLAR, P. G., and SALAZAR, C. Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. *International Journal of Engineerging Science and Computing*, vol. 6 (5), Maio 2016. Disponível em: <http://ijesc.org/upload/8e9af2eca2e1119b895544fd60c3b857>. Acesso em: 23 Set. 2019.

PC MAGAZINE. The best wireless routers. *PC Magazine*, 2020. Disponível em:<https://www.pcmag.com/picks/the-best-

wirelessrouters?test_uuid=01jrZgWNXhmA3ocG7ZHXevj&test_variant=b>. Acesso em: 29 Out. 2020.

PPLWARE. Redes – Sabe o que é o modelo OSI? *PPLWARE*, 15 set. 2010. Disponível em: <https://pplware.sapo.pt/tutoriais/networking/redes-sabe-o-quee-o-modelo-osi/>. Acesso em: 05 Fev. 2020.

RAMAKRISHNA, C., KUMAR, G. K., REDDY, A. M. and RAVI, P. A Survey on varios IoT Attacks and its Countermeasures. *International Journal of Engineering Reasearch in Computer Science and Engineering (IJERCSE)*, vol. 5 (4), 2018, pp.143-150. Disponível em: < http://ijercse.com/specissue/april-2018/27.pdf >. Acesso em: 09 Set. 2019. ISSN 2394-2320.

RANGEL, R. Internet das Coisas: nova revolução da conectividade. Entrevista com Kevin Ashton, *Revista Inovação em Pauta*, RJ, v. 1, n. 18, pp. 4-7, 2014. Disponível em: <http://finep.gov.br/images/revista/revista18/index.html#p=7> Acesso em: 05 Maio 2020.

SANTOS, R. L. A. IoT Como Framework para a Gestão e Governança de TI,

Modelo ITIL V3. *Revista Interdisciplinar de Tecnologia e Educação*, Boituva, 02 jun. 2017. Disponível em: <http://rinte.ifsp.edu.br/index.php/RInTE/article/view/350/pdf_97>. Acesso em: 01 Jun. 2020.

SERPRO - SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. *Quais são seus direitos?*, 2018. Disponível em: <https://www.serpro.gov.br/lgpd/cidadao/quais-sao-os-seus-direitos-lgpd>. Acesso em: 04 Abr. 2019.

SERPRO - SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. *Senado aprova nomes para a primeira diretoria da ANPD*, Brasília, 23 out. 2020. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/2020/senado-aprovanomes-para-primeira-diretoria-da-anpd>. Acesso em: 03 Nov. 2020.

SHCHERBAKOV, A. SAFE IN CLOUD. *SAFE IN CLOUD*, 2020. Disponível em: <https://www.safe-in-cloud.com/en/>. Acesso em: 27 Out. 2020.

SHIRALI-SHAHREZA, S. and GANJALI, Y. Protecting Home User Devices with an SDN-Based Firewall. *IEEE Transactions on Consumer Eletronics*, vol. 64 (01), fev. 2018, pp.92-100. Disponível em: <https://ieeexplore-ieeeorg.ez128.periodicos.capes.gov.br/document/8307429>. Acesso em: 07 Jun. 2020.

SHODAN.IO. SHODAN.IO. *SHODAN.IO*, 07 jun. 2020. Disponível em: <https://www.shodan.io/search?query=%22default+password%22>. Acesso em: 07 Jun. 2020.

SOARES, H. J.; ARAÚJO, N. V. D. S.; SOUZA, P. C. Privacidade e Segurança Digital: um estudo sobre a percepção e o comportamento dos usuários sob a

perspectiva do paradoxo da privacidade. *Workshop sobre as implicações da computação na sociedade (WICS)*. Cuiabá, MT: [s.n.]. 2020.

STEVAN JUNIOR, S. L. *Internet das coisas: fundamentos e aplicações em arduino e NodeMCU*. São Paulo: Editora Érica, 2018, 224 páginas.

SWAMY, S., JADHAY, D. and KULKARNI, N. Security Threats in the Application layer in IOT Applications. *International Conference of I-SMAC*, 2017.

TANENBAUM, A. S. *Redes de Computadores*. Rio de Janeiro: Elsevier Editora Ltda, 2003.

TECHRADAR. Top Wireless Routers on Test. *TECHRADAR*, 2020. Disponível em: <https://www.techradar.com/news/networking/routers-storage/best-router-9top-wireless-routers-on-test-1090523>. Acesso em: 27 Out. 2020.

TELECO. Teleco Inteligência em Telecomunicações. *Teleco.com*, 2019. Disponivel em: <https://www.teleco.com.br/pais/us.asp>. Acesso em: 03 Nov. 2020.

TONOBOHN, G. Shodan: conheça o buscador mais perigoso da internet. *Canal Tech*, 04 maio 2020. Disponível em: <https://canaltech.com.br/seguranca/Shodan-conheca-o-buscador-maisperigoso-da-internet/>. Acesso em: 01 Jun. 2020.

UIC - UNIVERSIDADE DE ILLINOIS. UIC Academic Computing and Communications Center. *Password strength test*, 2020. Disponível em: <https://www.uic.edu/apps/strong-password/>. Acesso em: 28 Out. 2020.

WESTOVER, B. *Best Wi-Fi routers for 2020.* TOM´S GUIDE, 2020. Disponível em: <https://www.tomsguide.com/us/best-wifi-routers,review-2498.html>. Acesso em: 27 Out. 2020.

WHEELER, D. M.; WHEELER, J. C. and FAGBEMI, D. D. *The IoT Architect´s Guide to Attainable Security & Privacy*. 1a. Ed. ed. Boca Raton, FL: CRC Press, 2020.

ZENG, D., GUO, S., & CHENG, Z. (07 de 2011). The Web of Things: A Survey. Journal of Communications, vol. 6, nº 6, 424-438. doi:10.4304/jcm.6.6.439-459 Disponível em: https://www.researchgate.net/publication/220520321_The_Web_of_Things_A_Survey_Invited_Paper. Acesso em: 21 Dez. 2020.

ZOOM. *ZOOM*, 2020. Disponivel em: <https://www.zoom.com.br/modem-eroteador/deumzoom/melhor-roteador-wi-fi-2020>. Acesso em: 07 out. 2020.