UNIVERSIDADE FEDERAL DO CEARÁ

***CAMPUS* SOBRAL**

CURSO DE GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

RENATO BRITO COSTA

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS APLICADA À INTERNET DAS COISAS: UMA REVISÃO SISTEMÁTICA

SOBRAL

2022

RENATO BRITO COSTA

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS APLICADA À INTERNET DAS COISAS: UMA REVISÃO SISTEMÁTICA

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Computação da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia de Computação.

Orientador: Prof. Dr. Wendley Souza da Silva

SOBRAL

2022

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

C875l Costa, Renato Brito.
A lei geral de proteção de dados pessoais aplicada à internet das coisas: uma revisão sistemática / Renato Brito Costa. – 2022.
72 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Sobral, Curso de Engenharia da Computação, Sobral, 2022.
Orientação: Prof. Dr. Wendley Souza da Silva.

1. Internet das Coisas. 2. Lei Geral de Proteção de Dados Pessoais. 3. Proteção de Dados. 4. Segurança. I. Título.

CDD 621.39

RENATO BRITO COSTA

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS APLICADA À INTERNET DAS COISAS: UMA REVISÃO SISTEMÁTICA

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Computação da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia de Computação.

Aprovado em:

BANCA EXAMINADORA

Prof. Dr. Wendley Souza da Silva (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Me. Erick Aguiar Donato
Universidade Federal do Ceará (UFC)

Thales Guimarães Marques
Universidade Federal do Ceará (UFC)

Aos meus pais.

AGRADECIMENTOS

À minha mãe, Maria Aurilene Brito Gomes. Sem ela nada disso seria possível.

Ao meu pai, Antônio da Costa Sobrinho (*in memorian*), que sempre fez tudo pelos filhos.

Ao professor Dr. Wendley Souza da Silva pela orientação e acompanhamento.

A Michelle Pontes Fontenele por todas as vezes que me ajudou, tirou dúvidas, resolveu algum problema na coordenação do curso, meus sinceros agradecimentos.

Aos amigos que me ajudaram durante todos os anos da graduação, em especial ao grupo Talento.

"Não sei, só sei que foi assim!"

(SUASSUNA, Ariano. O Auto da Compadecida.
11ª Ed. Rio de Janeiro: Livraria AGIR, 1975.)

RESUMO

No presente trabalho será abordado o relacionamento entre a *Internet* das Coisas (IoT), uma inovação tecnológica presente no dia a dia das pessoas, seja no transporte, em residências, saúde, indústria, etc, e a Lei Geral de Proteção de Dados Pessoais (LGPD), uma legislação específica sobre como deverá ser realizado o manuseio das informações produzidas ou capturadas no território nacional. O objetivo principal deste trabalho é realizar um alinhamento daquilo que já existe na IoT com o que é cobrado na LGPD. Para tanto, uma revisão bibliográfica acerca desses assuntos foi realizada. Os resultados dessa revisão citam modelos de referência a serem adotados na IoT, os autores desses modelos se preocuparam em conhecer as tecnologias e entender seu funcionamento, além disso não houve a proposta de mudanças na tecnologia em si, houve a sugestão de uma solução adequando-se ao que já é utilizado. Assim, na problemática da IoT, primeiramente é realizado um diagnóstico local e após essa análise buscar uma solução mais adequada a sua realidade. Já sobre LGPD, ficou evidente a necessidade do entendimento da Lei e a adoção de medidas técnicas e administravas no meio corporativo para adequação à norma.

Palavras-chave: *Internet* das Coisas. Lei Geral de Proteção de Dados Pessoais. Proteção de Dados. Segurança.

ABSTRACT

This work will aproach the relationship between the Internet of Things (IoT), a technological innovation present in people's daily lives, whether in transport, in homes, health care, industry, etc, and the General Law for the Protection of Personal Data (LGPD), specific legislation on how to handle information produced or captured in the national territory. The main objective of this work is to align what already exists in the IoT with what is charged in the LGPD. Therefore, a literature review on these subjects was carried out. The results of this review cite reference models to be adopted in the IoT, the authors of these models were concerned with knowing the technologies and understanding their operation, in addition there was no proposal for changes in the technology itself, there was a suggestion of a solution adapting to what is already used. So, in the IoT problem, a local diagnosis is carried out and after this analysis seek a solution that is more appropriate to your reality. Regarding LGPD, it was evident the need to understand the Law and the adoption of technical and administrative measures in the corporate environment to adapt to the standard.

Keywords: Internet of Things. General Personal Data Protection Law. Data Protection. Security.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AHP	*Analytic Hierarchy Process*
ANPD	Autoridade Nacional de Proteção de Dados
CoAP	*Constrained Application Protocol*
COBIT	*Control Objectives for Information and Related Tecnology*
DoS	*Denial of Service*
DPO	*Data Protection Officer*
DTLS	*Datagram Transport Layer Security*
GD	Governança de Dados
GDPR	*General Data Protection Regulation*
IBM	*International Business Machines*
IEEE	*Institute of Electrical and Electronic Engineers*
IoT	*Internet of Things*
IP	*Internet Protocol*
ISACA	*Information Systems Audit and Control Association*
ISM	*Industrial, Scientific and Medical*
ISO	*International Standards Organization*
ITIL	*Information Technology Infrasructure Library*
ITU	*International Telecommunication Union*
LGPD	Lei Geral de Proteção de Dados Pessoais
LoRaWAN	*Long Range Wide Area Network*
MAPE-K	*Monitor-Analyze-Plan-Execute plus Knowledge*
ML	*Machine Learning*
MQTT	*Message Queuing Telemetry Transport*
NFC	*Near Field Communication*
OSI	*Open System Interconnection*
RBS	Revisão Bibliográfica Sistemática
RFID	*Radio-Frequency IDentification*
SDN	*Software-Defined Network*
SERPRO	Serviço Federal de Processamento de Dados
SGSI	Sistema de Gestão de Segurança da Informação
SI	Segurança da Informação

SSL	*Secure Sockets Layer*
TCP	*Transmission Control Protocol*
TI	Tecnologia da Informação
UNB	*Ultra Narrow Band*
URL	*Uniform Resource Locator*
Wi-Fi	*wireless fidelity*
WLAN	*Wireless Local Area Network*
WoT	*Web of Things*

SUMÁRIO

1 INTRODUÇÃO

A globalização é um importante processo no desenvolvimento de novas tecnologias, e recentemente a chamada indústria 4.0 ganhou mais destaque no que se refere às tecnologias emergentes. Esse desenvolvimento tecnológico a certo ponto é favorável para a sociedade, porque traz ao seu cotidiano um grau de controle mais elevado sobre seus afazeres. Outro setor que recebeu bem esse desenvolvimento foi o industrial, pois a automatização de processos reduz custos e otimiza a produção.

A *Internet* das coisas (IoT) tem recebido bastante atenção tanto da academia quanto da indústria devido ao seu potencial de uso nas mais diversas áreas das atividades humanas. A utilização dos objetos inteligentes, definidos mais à frente, é fundamental para impulsionar esse avanço tecnológico, isto porque tais objetos possuem capacidade de comunicação e processamento associados a sensores, os quais transformam a utilidade desses objetos (SANTOS *et al.*, 2016, p. 3).

Ainda de acordo com (SANTOS *et al.*, 2016, p. 3) o emprego dos recursos dos objetos inteligentes é capaz de detectar o contexto sobre o qual está inserido, além de controlá-lo, viabilizar troca de informações uns com os outros, acessar serviços da *Internet* e interagir com pessoas. Deste modo, uma gama de novas possibilidades de aplicações surgem, como, por exemplo, aplicações na saúde (*Healthcare*), nas cidades inteligentes (*Smart Cities*) e as casas inteligentes (*Smart Home*). Não obstante, surgem também desafios relacionados a regulamentação, segurança e padronização dessas tecnologias.

Questionamentos sobre a segurança das informações corporativas, dados pessoais e governamentais levaram as empresas e até o Estado a implementar novas medidas de segurança e de fiscalização para o tratamento de dados no Brasil. No dia 14 de agosto de 2018 foi criada a Lei nº 13.709, a Lei Geral de Proteção de Dados Pessoais (LGPD) que dispõe de medidas preventivas, proativas na manutenção e privacidade das informações de terceiros.

(RAPÔSO *et al.*, 2019, p. 59) evidenciam a vulnerabilidade a espionagem ou a ataques de *Hackers* nos setores públicos e privados. Assim, justifica-se o aumento de investimento nos setores de Tecnologia da Informação (TI), que tenham por objetivo implementar ações para que problemas como vazamento de dados, ou com informações de terceiros não prosperem.

Em janeiro de 2021 um vazamento de grandes proporções de dados veio a conhecimento público, dentre as informações vazadas estavam: dados de falecidos, cadastro de pessoa física, nome, sexo, data de nascimento, além de uma tabela com registros de veículos e uma

lista com cadastros nacionais de pessoas jurídicas (G1, 2021). Essas informações são de caráter pessoal e se utilizadas de forma indevida podem prejudicar os donos de direito.

Este trabalho apresenta uma revisão bibliográfica sobre IoT, LGPD e Segurança da Informação (SI), apresentando os conceitos e esclarecendo o modo de operação para o tratamento de informações e como isso afetará o desenvolvimento de tecnologias emergentes, em especial as relacionadas à IoT.

1.1 Motivação

O presente estudo iniciou-se após a observação do aumento progressivo na utilização de tecnologias relacionadas à IoT, sendo ela uma das tendências tecnológicas mais proeminentes dos últimos anos (MARR, 2020, p. 1). Ademais, observa-se também as vulnerabilidades nos protocolos de comunicação entre dispositivos IoT que podem gerar prejuízos aos usuários desses aparelhos durante o tratamento dos dados coletados. Através deste estudo, será possível categorizar possíveis falhas e, por último, apontar meios para corrigi-las em concordância à LGPD, considerando que essa é a legislação brasileira no que se relaciona ao tratamento de dados.

2 OBJETIVOS

2.1 Objetivos gerais

O objetivo principal deste trabalho é realizar uma análise da infraestrutura relacionada à IoT com o intuito de mapear suas vulnerabilidades, assim, técnicas de SI, Governança de Dados (GD) e boas práticas poderão ser adotadas visando conformidade à LGPD.

2.2 Objetivos específicos

- Analisar a LGPD;
- Analisar os conceitos da IoT;
- Compreender as dificuldades da IoT quanto aos padrões e regulamentações;
- Analisar os protocolos de comunicação utilizados em IoT;
- Analisar as possíveis vulnerabilidades nos protocolos estudados;
- Analisar requisitos de segurança;
- Comparar soluções propostas.

3 FUNDAMENTAÇÃO TEÓRICA

3.1 Internet das coisas

A IoT é um termo que trata da conexão de objetos "comuns"à *internet*. (SANTOS *et al.*, 2016, p. 2) descrevem a IoT sendo uma extensão da *Internet* atual, que proporciona aos objetos do dia a dia, mas com capacidade computacional e de comunicação, se conectarem à *Internet*. A *International Telecommunication Union* (ITU) apresentou a IoT como "uma infraestrutura global para a sociedade da informação, permitindo serviços avançados interconectando coisas (físicas e virtuais) com base em tecnologias de informação e comunicação interoperáveis, existentes e em evolução"(ITU-T, 2012b).

Com o avanço tecnológico atual, muitos dispositivos estão usando sensores, atuadores, computação embarcada e computação em nuvem. Essas mudanças possibilitaram que a comunicação entre dispositivos fosse se tornando mais acessível. Assim, a interação entre dispositivos os permite coordenar uns aos outros, sem que haja interferência humana na execução de tarefas diárias (VASHI *et al.*, 2017, p. 492).

Ainda de acordo com (VASHI *et al.*, 2017, p. 492), os serviços tornarem-se mais fluidos, descentralizados, complexos e, consequentemente, a barreira de segurança na IoT ficou mais "estreita". Portanto, há uma necessidade de padronizá-la para garantir que a privacidade do usuário não seja violada.

3.1.1 Arquitetura básica dos dispositivos inteligentes

(RUIZ *et al.*, 2004, p. 2) listam os componentes básicos de um "nó sensor"em 4 unidades, sendo elas: Unidade de processamento/memória, unidade comunicação, fonte de energia e sensores/atuadores. "Aos dispositivos com essas qualidades é dado o nome de objetos inteligentes"(SANTOS *et al.*, 2016, p. 3). As unidades são descritas a seguir:

- Unidade de processamento/memória: composta de uma memória interna para armazenamento de dados e programas;
- Unidade de comunicação: consiste no canal de comunicação utilizado, pode ser com ou sem fio;
- Fonte de energia: responsável por fornecer energia aos componentes do objeto;
- Sensores/Atuadores: os sensores capturam informação do ambiente em que o objeto se encontra, os atuadores realizam alguma ação em posse dessas informações.

3.1.2 Blocos básicos de construção IoT

Para (SANTOS *et al.*, 2016, p. 5): "A IoT pode ser vista como a combinação de diversas tecnologias, as quais são complementares no sentido de viabilizar a integração dos objetos no ambiente físico ao mundo virtual". Em vista disso pode-se definir um conjunto de partes básicas para a IoT englobando diferentes conceitos para um fim comum. Os blocos básicos de construção IoT são:

- Identificação: identificar objetos unicamente para conectá-los à *internet*;
- Sensores/Atuadores: os sensores coletam informações sobre o contexto em que os objetos se encontram, já os atuadores podem manipular o ambiente ou reagir de acordo com os valores lidos;
- Comunicação: relaciona-se às técnicas utilizadas para a comunicação entre objetos inteligentes;
- Computação: envolve a unidade de processamento dos objetos inteligentes, essa sendo responsável pela execução local de algoritmos;
- Serviços: serviços de identificação (mapear entidades físicas em entidades virtuais), serviços de agregação de dados (coletar e sumarizar dados homogêneos/heterogêneos obtidos dos objetos inteligentes), serviços de colaboração e inteligência (tomar decisões e reagir de modo adequado a um determinado cenário), serviços de ubiquidade (prover serviços de colaboração e inteligência em qualquer momento e qualquer lugar em que eles sejam necessários);
- Semântica: refere-se à habilidade de extração de conhecimento dos objetos na IoT.

3.1.3 Modelos de Comunicação para IoT

(TSCHOFENIG *et al.*, 2015) propõem 4 modelos para comunicação em redes IoT, sendo eles:

- *Device-to-Device*: neste modelo os dispositivos se comunicam diretamente;
- *Device-to-Cloud*: neste modelo o dispositivo se comunica diretamente com a *Internet*, sem um equipamento intermediário entre esta comunicação;
- *Device-to-Gateway*: neste modelo para o dispositivo ter acesso à *Internet* ele precisa se conectar a um *gateway*;
- *Back-End Data Sharing*: neste modelo, dá-se sentido a uma grande quantidade de dados

de diferentes fontes, assim, o resultado será uma informação mais útil ao usuário;

3.1.4 Arquitetura da IoT

De acordo com (BURHAN *et al.*, 2018, p. 6) não existe um acordo único e geral sobre a arquitetura da IoT que seja convencionado no mundo inteiro e também pelos pesquisadores. Muitas arquiteturas acabaram sendo propostas por pesquisadores da área, há quem defenda um modelo de 3 camadas, mas também há aqueles que defendem modelos com 4 ou 5 camadas.

Essa discussão da quantidade de camadas na arquitetura IoT está relacionada à segurança da rede. Na maioria dos casos, os desafios dos objetos inteligentes são a capacidade de processamento reduzida e a sua fonte de alimentação, isso traz a esses dispositivos fragilidades que podem ser exploradas por invasores da rede. Desse modo, acaba sendo discutido recorrentemente questões de segurança da rede como, por exemplo, em qual camada devem ser executados os protocolos de segurança, e se existe a necessidade de uma camada específica para realizar essas operações.

3.1.4.1 Arquitetura de 3 camadas

Apesar de ser uma arquitetura básica, este modelo cumpre a ideia essencial da IoT. As 3 camadas deste modelo são: camada de percepção, camada de rede e camada de aplicação. Detalhadas abaixo.

- Camada de percepção: tem a responsabilidade de identificar objetos e coletar as informações dos sensores;
- Camada de rede: é nesta camada que as informações coletadas são transmitidas para os seus devidos fins;
- Camada de aplicação: esta camada garante a autenticidade, integridade e confidencialidade dos dados;

3.1.4.2 Arquitetura de 4 camadas

O motivo para a inclusão de uma quarta camada é a segurança na arquitetura IoT. Assim como no modelo anterior, neste modelo estão presentes as camadas de aplicação, rede e percepção. A nova camada adotada, camada de suporte, é responsável por prover medidas de segurança para tornar a arquitetura mais segura.

3.1.4.3 Arquitetura de 5 camadas

Apesar do modelo de 4 camadas ter apresentado meios de melhorar a segurança na IoT, ainda existiam problemas de armazenamento e questões de segurança não abordados. O modelo de 5 camadas foi proposto para solucionar essa situação, nele estão presentes 3 camadas já conhecidas dos modelos anteriores (camada de percepção, camada de transporte e a camada de aplicação) e as camadas de processamento, onde ocorre a coleta e processamento das informações, e a camada de negócios, cuja responsabilidade é gerenciar e controlar aplicações.

3.1.4.4 Modelo OSI

O OSI foi criado em 1971, mas formalizado apenas em 1983 pela *International Standards Organization* (ISO). "Foi a primeira tentativa no sentido de desenvolver um modelo para padronizar as conexões entre redes de computadores pelo sistema de divisão em camadas"(MONTEIRO *et al.*, 2021, p. 23).

(FOROUZAN, 2009, p. 29) destaca que esse modelo é uma estrutura em camadas para o projeto de sistemas de redes que permitem a comunicação entre todos os tipos de sistemas de computadores. O modelo OSI possui 7 camadas, sendo elas expostas na Tabela 1.

Tabela 1 – Camadas do modelo OSI

Camada	Atribuição
Camada 1 - física	Movimentação de bits individuais de um *hop* para o seguinte.
Camada 2 - enlace de dados	Transferência de frames de um *hop* para o seguinte.
Camada 3 - rede	Entrega de pacotes individuais desde o *host* de origem até o *host* de destino.
Camada 4 - transporte	Entrega de uma mensagem, de um processo a outro.
Camada 5 - sessão	Controle de diálogo e sincronização.
Camada 6 - apresentação	Tradução, compressão e criptografia.
camada 7 - aplicação	Prover serviços ao usuário.

Fonte: Adaptado de (FOROUZAN, 2009, p. 33 a 41)

3.1.5 Tecnologias de comunicação na IoT

São abordadas nesta seção as principais tecnologias de comunicação IoT.

3.1.5.1 Ethernet

A *Ethernet* é um padrão de camada física e camada de enlace que consiste de três elementos: o meio físico, as regras de controle de acesso ao meio e o quadro *Ethernet*. Nesse padrão as topologias suportadas são: barramento, estrela e árvore. Ademais, O modo de transmissão também é uma característica importante da *Ethernet*, podendo ser:

- *Simplex*: durante todo o tempo apenas uma estação transmite, a transmissão é feita unilateralmente;
- *Half-duplex*: cada estação transmite ou recebe informações, não acontecendo transmissão simultânea;
- *Full-duplex*: cada estação transmite e/ou recebe, podendo ocorrer transmissões simultâneas.

O uso do padrão *Ethernet* é sugerido para dispositivos fixos, sem mobilidade, o que pode ser inadequado para algumas aplicações. Logo, o uso desse padrão fica sujeito à conexão ponto a ponto de dispositivos, dependendo da situação esta pode ser a melhor configuração para que haja comunicação.

3.1.5.2 wireless fidelity

O *wireless fidelity* (Wi-Fi) é um conjunto de especificações técnicas para redes locais sem fio (*Wireless Local Area Network* (WLAN)) baseado no padrão *Institute of Electrical and Electronic Engineers* (IEEE) 802.11. Nas redes *Wireless* a transmissão ocorre por sinais de radiofrequência que se propagam pelo ar.

Esse protocolo atua em faixas de frequência de 2,4 Ghz ou 5 Ghz; salientando que quanto maior a frequência, maior será a taxa de transferência, entretanto o alcance do sinal será menor. Por estar no segmento de frequências que podem ser usados sem necessidade de aprovação direta de entidades reguladoras (Frequência *Industrial, Scientific and Medical* (ISM)), as redes sem fio que utilizam esse protocolo podem ser implementadas sem licença para instalação e operação.

Se comparado ao padrão *Ethernet* o *Wi-Fi* terá algumas vantagens como, por exem-

plo, maior velocidade de transmissão e não é mais necessário a utilização de cabos para a comunicação, todavia, o sinal da rede é curto alcance.

3.1.5.3 ZigBee

O Protocolo *ZigBee* (IEEE 802.15.4) foi desenvolvido pela *ZigBee Alliance*, projetado para oferecer flexibilidade aos tipos de dispositivos que ele pode controlar. Ele abrange as camadas referentes a *internet*, ou inter-redes, transporte e de aplicação do modelo TCP/IP.

O *ZigBee* permite comunicações robustas e opera na frequência ISM 868 MHz (1 canal), 915 MHz (10 canais) e 2,4 GHz (16 canais). Este protocolo oferece uma boa imunidade contra interferências, capacidade de hospedar milhares de dispositivos em uma rede, com taxas de transferências de dados variando entre 20 kbps a 250 kbps (LUGLI; SOBRINHO, 2012, p. 4).

3.1.5.4 Bluetooth

É um protocolo de comunicação sem fio projetado originalmente para curto alcance e baixo consumo de energia, ele permite dois dispositivos trocar informações entre si.

Seu funcionamento se dá pela utilização de ondas de rádio, isso faz com que os dispositivos não precisam estar no alcance de visão um do outro, mas precisam respeitar uma distância específica (GOGONI, 2019).

3.1.5.5 LoRaWAN

Mantido pela *LoRa Alliance*, o *Long Range Wide Area Network* (LoRaWAN) é um protocolo que tem por base uma rede de topologia estrela. Cada módulo *LoRa* envia e recebe dados a partir de *Gateways*, que repassam os dados via conexão *Internet Protocol* (IP) para os servidores adequados.

A especificação LoRaWAN foi projetada para criar redes de longa distância, composta de dispositivos alimentados por bateria e com capacidade de comunicação sem fio. A especificação LoRaWAN trata de requisitos presentes na IoT como comunicação segura e bidirecional, mobilidade e tratamento de serviços de localização.

O fator atrativo do LoRaWAN é o seu baixo custo de operação e a quantidade de empresas de *hardware* que o estão adotando. A LoRaWAN utiliza frequência ISM, logo não precisa de autorização prévia para operação. Os valores de frequência mais usadas nessa

tecnologia são: 109 MHz, 433 MHz, 866 MHz e 915 MHz. Já as distâncias alcançadas podem variar de 2 km a 5 km em meio urbano e 45 km no meio rural (ALLIANCE, 2021).

3.1.5.6 Sigfox

O *Sigfox* utiliza a tecnologia *Ultra Narrow Band* (UNB), que oferece uma solução de comunicação baseada em *software*. Essa tecnologia foi projetada para lidar com pequenas taxas de transferência de dados, para tanto o protocolo *Sigfox* é otimizado para mensagens pequenas. Por conta da sua abordagem em *software*, no *Sigfox* a complexidade da rede e da computação é gerenciada em nuvem e não nos dispositivos, consequentemente ocorre uma redução no consumo de energia e nos custos dos dispositivos conectados (BRASIL, 2017).

3.1.5.7 Message Queuing Telemetry Transport

O *Message Queuing Telemetry Transport* (MQTT) foi desenvolvido pela *International Business Machines* (IBM) na década de 90. Sua aplicação original era vincular sensores em *pipelines* de petróleo a satélites. Ele é um protocolo de mensagem com suporte para a comunicação assíncrona entre as partes, baseado em *Transmission Control Protocol* (TCP) com segurança *Secure Sockets Layer* (SSL) (YUAN, 2017).

O MQTT é um protocolo de rede leve que permite a implementação em *hardware* de dispositivo altamente restringido e em redes de largura da banda limitada e de alta latência, além de ser flexível, possibilitando suporte a diversos cenários de aplicativo para dispositivos e serviços de IoT. Assim, torna-se ideal para desenvolvedores.

No protocolo MQTT são definidas duas entidades na rede. A primeira é o *message broker* e a segunda os clientes. O *broker* é um servidor que recebe todas as mensagens dos clientes e, em seguida, distribui essas mensagens para os clientes de destino relevantes (YUAN, 2017).

3.1.5.8 Constrained Application Protocol

O *Constrained Application Protocol* (CoAP) foi desenvolvido pelo grupo de trabalho *Constrained Restful Environments* (CoRE) do *Internet Engineering Task Force* (IETF). Esse protocolo apresenta bom desempenho nos dispositivos com energia limitada, enlaces com baixa largura de banda, redes congestionadas ou com perdas, ou seja, ambientes com recursos limitados.

Além disso o CoAP pode ser utilizado onde o *broadcast* e *multicast* são necessários, em suma são situações cuja transmissão é feita de um emissor para vários ou todos receptores da rede (SILVA *et al.*, 2019).

Ainda de acordo com os autores o CoAP é adequado na implantação de ambientes em que o dispositivo apenas reporta dados de volta para o servidor, ou seja, em modo *report only*. já para as redes coletoras de dados de terceiros nas quais não há controle sob *firewalls* e portas bloqueadas, o CoAP pode não ser adequado. Com relação a segurança o CoAP usa o *Datagram Transport Layer Security* (DTLS)

3.1.5.9 Radio-Frequency IDentification

A tecnologia *Radio-Frequency IDentification* (RFID) permite a transferência de dados através de sinais de rádio. Essa tecnologia é capaz de identificar e rastrear objetos sem que haja contato físico entre eles, sendo então utilizada na coleta de informações de objetos em movimento, em locais insalubres ou em qualquer tipo de processo que impeça a utilização de código de barra (LOUREIRO *et al.*, 2015). Além de não precisar ter contato físico entre os objetos, essa tecnologia apresenta uma faixa de leitura com distância média de cerca de 3 a 6 m, porém, alguns tipos de *tags* podem alcançar distâncias de até 30 m dependendo da sua configuração e condições locais.

Um sistema de RFID pode ser dividido em três partes:

- Etiqueta (*tag*) ou *transponder*: dispositivo de identificação;
- Controlador (*middleware*): responsável por todo o processamento das informações;
- Leitor: dispositivo que se comunica com a etiqueta e com o controlador fornecendo e recuperando informações.

3.1.5.10 Near Field Communication

Assim como o RFID, o *Near Field Communication* (NFC) é uma tecnologia que permite a transferência de informações entre dois aparelhos sem ser necessário o contato entre os mesmos. Criado em 2003 pelas empresas pelas empresas *Sony* e *Philips*, o NFC tem por objetivo ser uma tecnologia de conexão de curta distância de forma segura (FONSECA *et al.*, 2018).

Para estabelecer conexão entre dispositivos, o NFC utiliza a tecnologia de indução magnética nos aparelhos capacitados. A transferência de dados necessita um aparelho iniciador, ou leitor, e um aparelho alvo, ambos compatíveis com a tecnologia. O iniciador gera um campo

de ondas de rádio de baixa frequência e, na existência de um alvo dentro desse campo, o circuito é ativado, configurando uma conexão entre ambos (FONSECA *et al.*, 2018).

3.1.6 Segurança em IoT

A segurança dos dados e privacidade do usuário é um dos assuntos mais importantes quando se trata de uma rede de dispositivos. Logo, é de suma importância adotar medidas de segurança e gerência dos dados que possam mitigar ataques e garantir a integridade das informações, haja vista que, dependendo do caso, dados sensíveis possam estar ali armazenados ou em trânsito.

As redes IoT são redes que atendem as mais diversas finalidades. Consequentemente, suas caraterísticas podem sofrer mudanças de acordo com a vontade do administrador ou usuários da rede, adequando-se às suas necessidades. Quando a rede em questão é uma rede residencial e de pequeno porte há uma variedade infinita de maneiras para configuração dessa rede, além de uma vasta quantidade de dispositivos que podem a ela se conectar.

O uso de um *firewall* nas redes IoT é um exemplo de alteração que pode ser feita pelo administrador da rede. O *firewall* possui alta necessidade de processamento e disponibilidade de energia para funcionar corretamente e alcançar seu objetivo de proteção da rede, assim, verifica-se um desafio para implementação em redes IoT, pois os recursos de processamento e energia, geralmente, são limitados nos dispositivos inteligentes (MONTEIRO *et al.*, 2021, p. 35).

(MONTEIRO *et al.*, 2021, p. 35) ressalta que por se tratar de redes heterogêneas e dinâmicas, onde os ativos computacionais não estão sob controle do usuário e, consequentemente, não ser possível implementar todos os aspectos de segurança que se julguem adequados, é que se faz necessário um meio de certificar e autenticar os dispositivos conectados à rede, além dos que se desejam conectar com um controle para prover melhor segurança. Além disso, 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.

Também vale salientar que as diferentes placas de prototipagem utilizadas em IoT, como o *Arduino* e *Raspberry Pi*, podem apresentar problemas associados à segurança nas redes em que são utilizados. Visto que essas placas não possuem todo o *hardware* e *softwares* necessários para realizar o processamento adequado e seguro da informação ali armazenada, como *firewall* ou antivírus, por isso podem ser considerados um ponto fraco para ataques nas redes IoT (MONTEIRO *et al.*, 2021, p. 27).

Segundo (YOUSUF *et al.*, 2015, p. 2), alguns requisitos para que a estrutura de comunicação esteja protegida são:

- Confidencialidade: garantir que os dados estejam seguros e acessíveis apenas àqueles que possuam autorização;
- Integridade: garantir a precisão dos dados, bem como assegurar que os dados não sejam adulterados durante o processo de transmissão;
- Disponibilidade: dispositivos e serviços devem estar acessíveis e disponíveis quando necessário e em tempo hábil;
- Autenticação: cada objeto na IoT deve ser capaz de identificar e autenticar outros objetos;
- Soluções leves: recursos de segurança que podem ser aplicados mesmo diante das limitações de *hardware* e *software* dos dispositivos envolvidos na IoT;
- Heterogeneidade: capacidade de dispositivos e protocolos se comunicarem entre si, mesmo sendo de fontes diferentes;
- Políticas: são as políticas e padrões para garantir que os dados serão gerenciados, protegidos e transmitidos de forma eficiente;
- Sistemas de gerenciamento de chave de criptografia: na IoT ocorre a troca de informações de criptografia entre dispositivos para garantir a confidencialidade dos dados. Assim, faz-se necessário mecanismos para realizar a gerência das chaves, de modo a garantir a segurança do sistema;

Indivíduos mal-intencionados aproveitam das características das redes IoT para explorar suas vulnerabilidades e aplicar ataques visando algum ganho sob aquilo que foi "recuperado". A falta de comunicação entre os protocolos, dependência energética dos dispositivos, baixo poder de processamento, pouca memória, a larga escala de uso são características de dispositivos inteligentes que, infelizmente, facilitam a execução de ataques à rede.

Há uma elevada variedade de ataques que podem ser realizados nos dispositivos inteligentes. Segundo (RAMAKRISHNA *et al.*, 2018, p. 145), os principais ataques que podem ocorrer são:

- Ataques físicos: Esse tipo de ataque é mais caro para ser executado, pois consiste na modificação de componentes do *hardware*, sendo então mais difíceis para realizar;
- Ataque de canal lateral: detectam o tipo de criptografia usado na rede. Dispositivos de criptografia produzem informações que podem ser mensuradas, a exemplo o tempo e estatísticas de consumo. Neste ataque essas informações são coletadas, tratadas e utilizadas

para recuperar a chave de criptografia do dispositivo;

- Ataques de criptoanálise: ataques focados no texto cifrado e na tentativa de quebrar a criptografia utilizada;
- Ataques de *software*: este tipo de ataque é a principal vulnerabilidade de segurança em qualquer sistema. Esse ataque inclui a exploração de estouros de *buffer* e uso de programas de cavalos de Troia, *worms* ou vírus para injetar código malicioso no sistema. O *Software* acaba sendo o maior alvo dos ataques realizados às redes IoT;
- Ataques à rede: neste ataque são exploradas as vulnerabilidades da rede, em especial as redes *wireless*, pois elas consistem em um ponto fraco dos sistemas. São exemplos de ataques desse tipo a espionagem da rede, captura de pacotes, análise de tráfego, etc;

3.2 A Lei Geral de Proteção dos Dados Pessoais (LGPD) - Lei 13.709/18

A lei 13.709/18, conhecida como LGPD, é a legislação brasileira que ordena as atividades de tratamento de dados no Brasil, sejam elas em meios físicos ou digitais. Ela tem por objetivo garantir os direitos fundamentais de liberdade e de privacidade (TEMER *et al.*, 2018, p. 59).

Esse é um assunto recente no Brasil, o texto da lei teve sua aprovação em agosto de 2018, entrando em vigor em setembro de 2020, já as sanções, para quem descumprir as regras, serão aplicadas a partir de agosto de 2021. (LORENZON, 2021, p. 42) destacam que essa temática é extremamente passível e urgente de ser estudada .

A LGPD não é a primeira regulamentação a tratar questões virtuais. O Código de Defesa do Consumidor, a Lei de Acesso à Informação, o Marco Civil da Internet possuem textos que tratam do assunto (SEBRAE, 2020, p. 4).

Mesmo sendo por uma boa causa a implementação da LGPD no funcionamento das empresas, órgãos públicos e demais prestadores de serviços que coletam e utilizam dados alheios, essa mudança causará impacto e poderá contribuir para o aumento do chamado "custo Brasil", no qual empresas menores, *startups* e o setor público serão mais afetados (PINHEIRO, 2020).

A fim de compreender mais a Lei as seguintes subseções explicarão alguns dos seus aspectos fundamentais, bem como: Tipos de dados, quando a Lei é aplicada, seus princípios norteadores, como e quando deve ocorrer o tratamento de dados, direitos do titular, os agentes envolvidos no tratamento das informações, sanções, responsabilidades e demais questões pertinentes ao estudo.

3.2.1 Tipos de dados

No Art. 5º da Lei Nº 13.709/18 os dados são classificados em 3 grupos. Apresentados abaixo.

- Dado pessoal: é a informação relacionada a pessoa natural identificada ou identificável;
- Dado pessoal sensível: é a informação a respeito de uma pessoa que possa levá-la a sofrer discriminação dependendo da forma como for tratada;
- Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Feita a distinção dos dados, pode-se perceber que os dados pessoais sensíveis precisam de uma maior atenção, como proteção especial e sigilo. Desse modo, a coleta e utilização desses dados somente ocorrerá em momentos específicos como, por exemplo, quando há consentimento explícito do titular. Demais situações para o tratamento de dados sensíveis são abordadas no Art. 11º da Lei.

3.2.2 Aplicações da lei 13.709/18

A LGPD é aplicada a qualquer operação de tratamento de dados realizada por pessoa natural ou por pessoa jurídica, independente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada em território nacional e tenha por objetivo a oferta de serviços, além dos dados terem sido coletados em território nacional.

Entretanto há algumas exceções como, por exemplo, a Lei não se aplica ao tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos, questões de segurança pública, defesa nacional, tratamento de dados para fins jornalísticos e artísticos, fins acadêmicos. Outras exceções, bem como maiores descrições, encontram-se nos Arts. 3º e 4º da Lei.

3.2.3 Princípios norteadores

O princípio fundamental da LGPD é a boa-fé (TEMER *et al.*, 2018, p. 60), então, para que o tratamento dos dados ocorra da maneira correta a Lei prevê em seu Art. 6º os seguintes princípios:

I. Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados

ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II. Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III. Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV. livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V. Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI. Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII. Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII. Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX. Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X. Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

A manutenção desses princípios visa garantir o respeito aos direitos dos titulares. Além disso, também serve para criar diretrizes a serem seguidas pelos agentes de tratamento, haja vista as bases legais da lei, como o consentimento do titular e o legítimo interesse.

3.2.4 O tratamento de dados

A Lei considera tratamento de dados toda operação realizada com dados pessoais, como as que se relacionam a coleta, utilização, reprodução, transmissão, distribuição, processamento, armazenamento, eliminação, transferência e demais operações (TEMER *et al.*, 2018, p. 60). A Tabela 2 abaixo traz uma síntese das fases do ciclo de tratamento e das operações envolvidas.

Tabela 2 – Tratamento de dados pessoais

Fase do ciclo de Tratamento	Operações de Tratamento
Coleta	Coleta, produção, recepção
Retenção	Arquivamento, armazenamento
Processamento	Classificação, utilização, reprodução, processamento, avaliação, extração, modificação
Compartilhamento	Transmissão, distribuição, comunicação, transferência, difusão
Eliminação	Eliminação

Fonte: Adaptado de CONBCON 2020

Contudo, para que o tratamento dos dados seja realizado é necessário que ele ocorra em situações específicas, seja para dados pessoais, dados pessoais sensíveis, dados de crianças e adolescentes. Esse processamento será para fins específicos, legítimos, explícitos e comunicados entre os envolvidos. As situações para que possa ocorrer o tratamento dos dados são descritas com mais detalhes nos Art. 7º, 11º e 12º da Lei.

3.2.5 Direitos do titular

É estabelecido pela Lei que o titular dos dados deverá ter acesso facilitado às informações sobre o tratamento de seus dados, sendo elas de forma clara e adequada. Ademais, são garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade.

Quanto ao tratamento dos dados, os titulares mediante requisição podem: ter acesso aos seus dados; confirmar existência do tratamento; solicitar correção de dados incompletos ou desatualizados; solicitar anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o previsto na Lei e acesso à informação das entidades com as quais o controlador realizou uso compartilhado de dados.

3.2.6 Agentes no tratamento

A LGPD em seu Art. 5º define a figura do controlador e do operador como os agentes de tratamento. Além deles, ainda há a figura do encarregado pelo tratamento de dados, conhecido como *Data Protection Officer* (DPO) na *General Data Protection Regulation* (GDPR).

O controlador é aquele a quem competem as decisões referentes ao tratamento de dados pessoais. Portanto, é o principal responsável pelas decisões que envolvam os dados pessoais coletados. Já o operador é aquele que realiza o tratamento de dados pessoais em nome do controlador. Percebe-se então o grau de hierarquia entre essas figuras, sendo o controlador (grau mais alto) aquele que define a ação a ser realizada e o operador (grau mais baixo) aquele que obedece essa escolha. As bases legais da LGPD concedem atribuições e limites a cada um dos agentes de tratamento, em especial nos artigos 7º e 11º da Lei pode-se notar requisitos para o tratamento de dados.

Por sua vez, o encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

3.2.7 Segurança, sigilo de dados e governança

A segurança da informação não é somente uma preocupação das empresas que coletam e processam os dados, os titulares também estão mais atentos a isso, considerando que são suas informações na posse de outros e que isso pode afetá-lo posteriormente.

Em seu texto a LGPD deixa evidente as responsabilidades dos agentes de tratamento, eles devem adotar medidas técnicas e administrativas de segurança para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, além disso também devem garantir a segurança da informação mesmo após o fim do tratamento realizado (TEMER *et al.*, 2018, p. 61).

Nos casos de incidentes de segurança que possam causar risco ou dano relevante aos titulares, o operador deverá comunicar imediatamente à ANPD a ocorrência. Nessa comunicação deverá conter a descrição dos fatos ocorridos, informações dos titulares afetados, riscos relacionados ao incidente e as medidas que serão adotadas para reverter os efeitos do prejuízo (TEMER *et al.*, 2018, p. 63).

3.2.8 Sanções

A LGPD não é uma legislação proibitiva, ou seja, em seu texto ela não proíbe o tratamento de dados, seja ele para fins comerciais, econômicos, financeiros, acadêmicos, entre outros. Sua real função é determinar métricas para que essas operações ocorram de maneira segura e sem prejudicar os titulares. Além disso, também dá uma maior segurança aos titulares no que se refere ao controle das suas informações, a exemplo disso temos os princípios da lei (Incisos I ao X do art. 6º).

Então, no caso de vazamento de dados em uma empresa, por exemplo, a LGPD atuará diretamente sobre à segurança que a empresa empregava ao manter aquela informação em seus bancos de dados. (SANTINI *et al.*, 2019, p. 24) destacam que as empresas devem adaptar-se às novas disposições legais, indiferente ao tipo de documento, seja ele físico ou virtual. As penalidades, caso ocorra violação à lei, são tratadas no art. 52º da referida lei.

As sanções são rigorosas, tendo em vista que os prejuízos que a empresa pode ter não são somente monetários, mas a sua imagem também é afetada devido a divulgação da infração cometida, ação prevista no inciso IV do artigo 52 da lei. Todavia, para que as sanções possam

ser aplicadas é necessário antes a execução de procedimento administrativo que possibilite a oportunidade da ampla defesa. Ao fim do procedimento administrativo, respeitando seus critérios, as sanções da LGPD podem ser executadas.

(SANTINI *et al.*, 2019, p. 25) destacam o impacto das sanções em empresas de pequeno e médio porte, em especial as *startups*, pois a suspensão das suas atividades e as sanções aplicadas podem resultar um grande prejuízo. Desse modo, a aplicação de medidas de segurança como boas práticas e gestão de dados podem garantir o cumprimento mínimo dos requisitos exigidos pela Lei.

3.2.9 Atribuições e composição da Autoridade Nacional de Proteção de Dados (ANPD)

A ANPD é o órgão do governo ligado à Presidência da República responsável por fiscalizar e aplicar a LGPD. Em suma, esse órgão é o responsável por regulamentar as operações de tratamento de dados, fiscalizar e aplicar as penalidades àqueles que descumprirem a Lei. Além disso, a ANPD também tem a função de informar ao público as políticas no tratamento de dados, os direitos envolvidos e fomentar boas práticas as empresas que utilizam dados pessoais de terceiros, considerando que essas empresas poderão ser auditadas nos casos de discordância à Lei.

3.3 Segurança e governança de dados

O ciclo de vida da informação é composto de 7 camadas, sendo elas: identificação das necessidades e requisitos; obtenção das informações; tratamento da informação; distribuição da informação; uso; armazenamento e descarte (ARMSTRONG *et al.*, 2019, p. 590). Logo, é necessário definir requisitos para que ocorra o tratamento adequado dos dados desde o momento que eles são obtidos até o seu descarte. Uma fase importante nesse processo é a definição de condições mínimas de segurança durante todo o processamento. Assim, nesta seção serão tratadas estratégias para gerência da informação, tal como a SI, GD e a utilização dos *frameworks* *Information Technology Infrasructure Library* (ITIL) e *Control Objectives for Information and Related Tecnology* (COBIT).

3.3.1 Segurança da informação

"A SI é a responsável por salvaguardar a informação. Esta deve garantir a continuidade das atividades, a integridade da informação e a disponibilidade da informação e dos serviços da organização", (OLIVEIRA *et al.*, 2016, p. 39). Ou seja, a SI busca proteger um grupo de informações que possuem valor para uma pessoa ou organização (NOBRE *et al.*, 2019, p. 3).

(HINTZBERGEN *et al.*, 2018, p. 12) definem alguns conceitos fundamentais para a SI, dentre eles:

- Autenticidade: uma entidade ser o que afirma que é;
- Confiabilidade: consistência dos comportamentos e resultados desejados;
- Confidencialidade: a informação não é divulgada àqueles não autorizados;
- Disponibilidade: ser acessível e utilizável sob demanda por aquele que é autorizado;
- Integridade: garantir que a informação esteja correta ao ser acessada;
- Não repúdio: habilidade de provar a ocorrência de um suposto evento ou ação em suas entidades de origem.

(OLIVEIRA *et al.*, 2016, p. 39) realçam o aumento do nível de preocupação com a SI desde a popularização da *Internet* e o crescimento dos crimes no ambiente tecnológico. Tamanha preocupação instigou governos a criarem normas e padrões no intuito de organizar a segurança e proteger as organizações.

Um dos padrões de segurança mais utilizados mundo afora é o conjunto de normas da família ISO 27000, que, por sua vez, traz diversos conceitos a fim de se obter uma maior segurança das informações através de um Sistema de Gestão de Segurança da Informação (SGSI) para uma organização. Esse conjunto de normas fornece boas práticas, diretrizes para o desenvolvimento de métricas para realizar avaliação da eficácia de SGSI, dos controles implementados, diretrizes para o processo de gestão de riscos de SI, entre outros. (OLIVEIRA *et al.*, 2016; NOBRE *et al.*, 2019).

3.3.2 Governança de dados

Conforme (SANTOS, 2010, p. 19) a GD tem por finalidade tratar dados como algo valioso nas organizações, ou seja, como ativos. Para tanto, a GD dispõem de processos, políticas, padronização e tecnologias que buscam tratar e garantir a disponibilidade, acessibilidade,

qualidade, consistência e segurança dos dados.

A utilização de um *framework* de GD pode ajudar as organizações a utilizarem os dados com mais eficiência. Para (SANTOS, 2010, p. 20) esse *framework* deve prover definições consistentes, estabelecer uma administração de dados na organização e ser capaz de mensurar e rastrear a qualidade dos dados.

Posto isso, ao adotar a GD no tratamento de informações, é possível planejar e implementar diretrizes, bem como padronizações que permitam a manipulação dos dados. Além disso, as boas práticas na GD asseguram a qualidade dos dados, sua segurança, consistência e disponibilidade de acesso (ESPÍNDOLA *et al.*, 2018).

3.3.2.1 ITIL

O ITIL é um conjunto de boas práticas a serem adotadas em serviços de TI, ou seja, um *framework* para o gerenciamento de serviços em TI. (OSTEC, 2016) destaca alguns dos objetivos chave do *itil*, dentre eles: influenciar nos resultados do negócio, auxiliar no processo de mudança do negócio, gestão de risco de acordo com as necessidades do negócio, otimizar a experiência dos consumidores, mostrar valor e possibilitar melhoria continua.

Algumas práticas gerais de gerenciamento do ITIL são: gerenciamento de arquitetura, gerenciamento de riscos, gerenciamento de segurança da informação, gerenciamento de Projetos, gerenciamento de fornecedores, melhoria contínua e medição e relatórios,

3.3.2.2 COBIT

O COBIT é um *framework* de governança da TI desenvolvido pela *Information Systems Audit and Control Association* (ISACA). Ele auxilia as organizações a obterem êxito em seus objetivos de governança e gestão da TI abarcando todas as áreas de negócio da organização (PEREIRA; FERREIRA, 2015, p. 23).

Um característica importante do COBIT é o valor posto às informações das organizações, daí a necessidade de ter um bom projeto de gerência desses dados. Resumidamente, no COBIT os recursos de TI precisam ser gerenciados por um conjunto de processos agrupados corretamente (MOMO; LIMA, 2021, p. 56).

Segundo (MOMO; LIMA, 2021, p. 56), a fim de alcançar os resultados esperados, o *framework* faz: *link* entre a TI e o negócio, organiza os processos e atividades de TI em um modelo mundialmente aceito, identifica os maiores recursos de TI a serem gerenciados e define

os objetivos de controle a serem implementados.

4 METODOLOGIA

4.1 Tipo de estudo

O presente trabalho vale-se de uma Revisão Bibliográfica Sistemática (RBS). A RBS é um instrumento para mapear trabalhos publicados no tema de pesquisa, assim o pesquisador é capaz de elaborar uma síntese atualizada do conhecimento existente sobre o assunto (BIOLCHINI *et al.*, 2007, p.135).

O modelo de RBS adotado neste trabalho é uma adaptação da proposta de (LEVY; ELLIS, 2006, p. 182) que definem o processo de revisão de literatura como um conjunto de etapas sequenciais para coletar, conhecer, compreender, aplicar, analisar, sintetizar e avaliar a literatura de qualidade a fim de fornecer uma base sólida para um tópico e método de pesquisa. A Figura 1 ilustra o modelo de (LEVY; ELLIS, 2006, p. 2).

(LEVY; ELLIS, 2006, p. 182) propõem 3 etapas principais para realizar uma RBS de qualidade, sendo elas: Entrada, processamento e saída. Na primeira etapa, a entrada, é onde está localizada a informação a ser trabalhada, seja ela por meio de artigos clássicos na área de estudo, livros-texto que reúnem conhecimentos na área, artigos de referência indicados por especialistas. Nessa etapa também inclui o planejamento para a condução da RBS, ou seja, o protocolo a ser adotado na pesquisa. Trata-se de um documento que descreve o processo, técnicas e ferramentas que serão utilizadas durante a segunda etapa, etapa de processamento, que por fim irá gerar as saídas (terceira etapa), relatórios, síntese dos resultados (CONFORTO *et al.*, 2011, p.4).

Figura 1 – Etapas de um revisão bibliográfica.

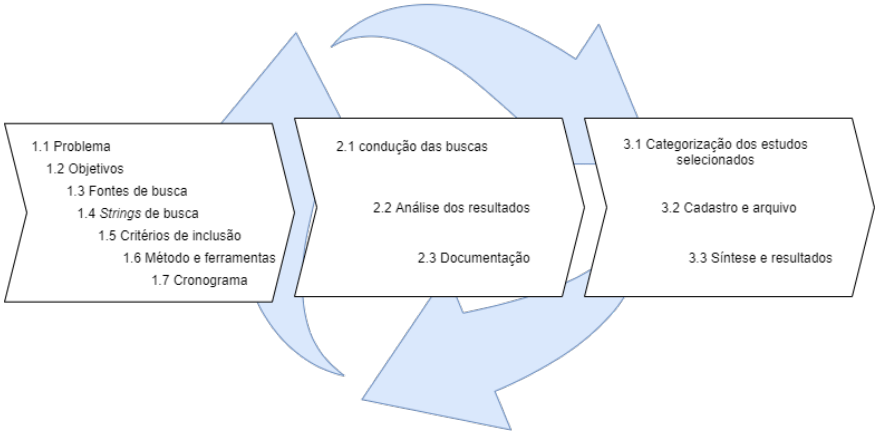
Fonte: Adaptado de (LEVY; ELLIS, 2006, p. 182).

4.2 Etapas da revisão

Para a condução efetiva da RBS disposta neste trabalho, o roteiro, ou protocolo, adotado é uma adaptação do roteiro RBS *Roadmap* desenvolvido por (CONFORTO *et al.*, 2011, p. 5).

A adaptação do RBS *Roadmap* está dividida em 3 etapas, sendo elas as mesmas definidas por (LEVY; ELLIS, 2006, p. 182), por sua vez essas etapas estão divididas em 13 fases, conforme a Figura 2 abaixo.

Figura 2 – Modelo para condução da RBS *Roadmap* adaptado.



Fonte: Adaptado de (CONFORTO *et al.*, 2011, p. 7)

4.2.1 Primeira etapa: Entrada

Nesta etapa são definidos os conceitos iniciais para a realização do estudo como. A etapa é dividida em 7 fases, sendo essas: Problema, objetivos, fontes de busca, *strings* de busca, critérios de inclusão, método e ferramentas, cronograma. Abordadas abaixo.

4.2.1.1 Fase 1: Problema

A definição do problema é o ponto de partida da RBS (CONFORTO *et al.*, 2011, p. 6). A partir da identificação do problema é possível definir uma pergunta norteadora para o tema de estudo, essa por sua vez determina quais serão os estudos incluídos e os meios adotados para identificação de cada estudo selecionado (SOUZA *et al.*, 2010, p. 104).

O tema de estudo foi delimitado diante do contexto atual, a LGPD já está em vigor e suas sanções passarão a valer a partir de agosto de 2021, logo, identificou-se a seguinte pergunta norteadora: como empresas de tecnologia, em especial as mantenedoras de protocolos

de comunicação, irão adequar-se à LGPD.

4.2.1.2 Fase 2: Objetivos

Os objetivos da RBS devem estar bem definidos e alinhados com os objetivos do projeto de pesquisa. (CONFORTO *et al.*, 2011, p. 6) salientam a importância de estabelecer critérios e segui-los à risca na definição dos objetivos, considerando que eles serão a base para a análise dos artigos encontrados. A partir dos objetivos da RBS é possível estabelecer os métodos para inclusão dos artigos na pesquisa.

4.2.1.3 Fase 3: Fontes de busca

Para o presente estudo a base de dados utilizada foi o *Google Scholar*.

4.2.1.4 Fase 4: Strings de busca

As *strings* de busca, ou descritores, são palavras-chave referentes ao tema de estudo. Na sua criação é necessário identificar as palavras e termos pertinentes ao estudo. Isso pode ser feito a partir de uma análise introdutória das fontes e também por consulta a especialistas e pesquisadores (CONFORTO *et al.*, 2011, p. 7).

Os descritores “LGPD”, “IoT”, “ITIL”, "COBIT", “segurança", "governança de dados", "segurança da informação”, “protocolos de segurança IoT” e suas combinações foram utilizados na base de busca com a utilização das aspas duplas, pois elas forçam o mecanismo de pesquisa a retornar valores com o mesmo nome presente entre as mesmas. Além disso, o operador booleano *AND* também foi utilizado, ele, por sua vez, restringe e retorna os documentos existentes na base que mostram os descritores usados.

4.2.1.5 Fase 5: Critérios de inclusão

Esta fase compreende a adoção de critérios para inclusão e exclusão dos trabalhos mapeados. Para a definição coesa desses critérios é preciso levar em consideração os objetivos da pesquisa (CONFORTO *et al.*, 2011, p. 7).

No caso deste trabalho em específico, a RBS pretende identificar casos de aplicação de práticas de gestão de dados nos protocolos IoT em conformidade à LGPD, sendo assim os artigos analisados necessariamente deverão conter estudos de caso ou pesquisa-ação da temática,

todavia, se os artigos não apresentem essas informações serão excluídos ao término da análise pelos filtros de busca (Figura 3).

Isto posto, foram definidos os seguintes critérios de inclusão para dar início à pesquisa: (1) artigos completos; (2) material de livre acesso; (3) idioma português ou inglês; (4) ano de publicação e (5) tema em concordância ao foco do presente estudo.

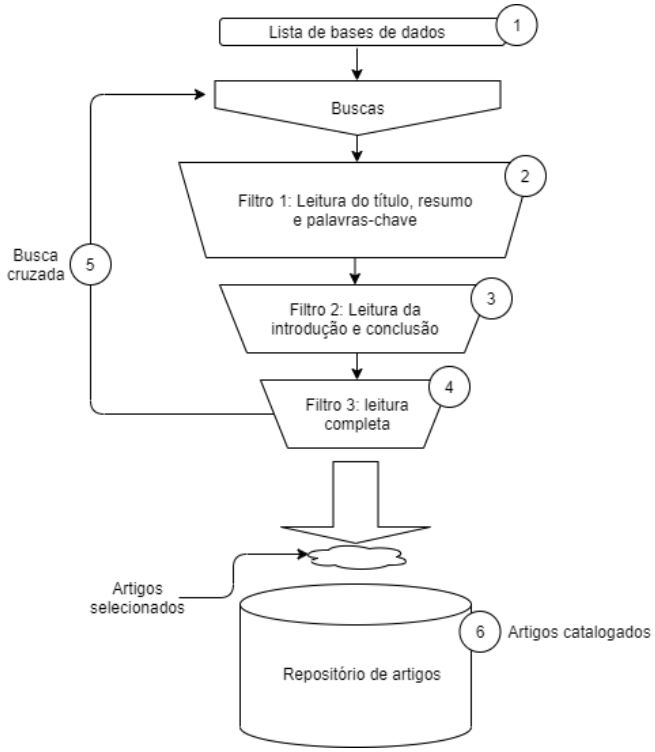
Os critérios de exclusão definidos foram: (1) artigo sem livre acesso; (2) estudo que foge do escopo da pesquisa; (3) material que apresente duplicidade nas bases de dados e (4) artigo em discordância ao foco do presente estudo.

4.2.1.6 Fase 6: Método e ferramentas

Nesta fase são definidos as etapas para a condução das pesquisas, definição de filtros de busca, como a pesquisa será realizada nas bases de dados e como os resultados serão armazenados (CONFORTO *et al.*, 2011, p. 7).

A Figura 3 é uma adaptação do método proposto por (CONFORTO *et al.*, 2011, p. 5). Além disso, de acordo com os autores o método proposto é iterativo, ou seja, ele contempla ciclos que favorecem o aprendizado, refinamento da busca, e buscas cruzadas, a partir de referências citadas nos artigos encontrados.

Figura 3 – Procedimento iterativo da etapa de processamento.



Fonte: Adaptado de (CONFORTO *et al.*, 2011, p. 8).

4.2.1.7 Fase 7: Cronograma

Fase de definição do cronograma para conclusão da RBS.

4.2.2 Segunda etapa: Processamento

Nesta etapa será realizado o processamento dos dados obtidos. Dividida em 3 fases: condução das buscas; análise dos resultados; documentação.

As buscas (Figura 2 - fase 2.1) realizadas correspondem aos passos 1 e 5 do método utilizado (Figura 3). É feita a consulta na base de dados utilizando os descritores e suas combinações, mencionados na seção 4.2.1.4. Terminada a busca, é iniciada a análise (Figura 2 - fase 2.2) dos itens encontrados, são aplicados os filtros (passos 2, 3, 4 e 5 da Figura 3) e, por conseguinte, os resultados são armazenados e documentados (passo 6 da Figura 3).

Na fase 2.3 (Documentação) as informações catalogadas são: quantidade de citações, origem do trabalho; autores; ano de publicação; *Uniform Resource Locator (URL)* do artigo; o padrão de cores correspondente aos critérios de inclusão e exclusão, etc. Segundo (CONFORTO *et al.*, 2011, p. 8): “esses dados serão uteis para argumentação teórica e embasamento da síntese da teoria sobre o assunto pesquisado”.

O primeiro passo da pesquisa é a busca na base de dados, os resultados dessa pesquisa foram armazenados no Apêndice A. Na Tabela 3 estão os descritores e valores de retorno da busca, o período de publicação dos estudos compreendeu os últimos 6 anos (2015 a 2021).

Tabela 3 – Resultado da busca na base de dados

Descritor	Retorno(resultados)
"internet das coisas"	12400
"internet das coisas"*AND* "segurança"	8480
"internet das coisas"*AND* "ITIL"	86
"LGPD"	2420
"LGPD"*AND* "IoT"	324
"LGPD"*AND* "Governança de dados"	138
"LGPD"*AND* "ITIL"	29
"ITIL"	1370
"COBIT"	48100
"Segurança da informação"	8890
"Protocolos de segurança IoT"	187

Fonte: O autor

Após realizar a busca na base de dados (*Google Scholar*) e armazenamento dos resultados é aplicado o primeiro filtro (Figura 3, passo 2). Nesse filtro são lidos apenas o título, resumo e palavras-chave. Deve-se verificar a adequação desses filtros aos objetivos da RBS. Os artigos que estiverem alinhados aos objetivos e atenderem aos critérios de inclusão serão selecionados para o próximo filtro. (CONFORTO *et al.*, 2011, p. 9) ressaltam que havendo dúvida com relação ao artigo e ocorrer exclusão pelo filtro é importante mantê-lo guardado na lista de artigos para submetê-lo ao filtro 2 (Figura 3, passo 3), pois apenas a leitura do titulo, palavras-chave e resumo podem não ser suficiente para saber se o artigo é adequado ou não aos objetivos da RBS.

O filtro 2 consiste na leitura da introdução, conclusão e também os dados do filtro 1. Mais uma vez os artigos que não atenderem aos objetivos da busca e os critérios de inclusão são eliminados da RBS. Na próxima fase, aplicação do filtro 3 (Figura 3, passo 4), os artigos até então selecionados são sujeitos à leitura completa. De acordo com os autores (CONFORTO *et al.*, 2011, p. 9): "Nesse momento é importante ter foco nos objetivos e critérios de inclusão. Os artigos que passarem por este filtro certamente serão relevantes para a pesquisa e síntese da teoria, e poderão compor a dissertação ou tese".

A busca cruzada (Figura 3, passo 5) tem por finalidade encontrar estudos relevantes à RBS que não foram encontrados na primeira busca, além disso, é nesse momento que são definidos os critérios de qualificação do artigo. As variáveis utilizadas para qualificar os artigos são: quantidade de citações, objetivo, resultados do estudo, método de pesquisa utilizado, dentre outros. O propósito nesse momento é realizar leitura e avaliação detalhadas dos trabalhos, assim, será mais fácil identificar trabalhos mais relevantes para o estudo (CONFORTO *et al.*, 2011).

Dá-se mais atenção ao filtro 3, haja vista que ele é o pontapé inicial para o início do processo iterativo de busca cruzada, dado que são localizados e identificados artigos relevantes por meio das citações dos autores. Nesse momento são identificados estudos pertinentes que não foram encontrados nas primeiras buscas, também é nesse momento que são preenchidos os critérios de qualificação do artigo (CONFORTO *et al.*, 2011).

No Apêndice A[1] está disponível a ferramenta de coleta utilizada para organização das informações do estudo no primeiro momento, a seguinte correlação de cor e valor representa o critério de exclusão (Seção 4.2.1.5) utilizado na análise dos resultados das etapas anteriores: amarelo - (1); verde - (2); vermelho - (3); azul - (4). No Apêndice B está a ferramenta utilizada

[1] Link para acesso ao arquivo completo no *Google* Planilha: <https://docs.google.com/spreadsheets/d/14JL7juK5uSzzKVjYdd7LZOfWtkoztosI0BQzwOt8Zxw/edit?usp=sharing>

para qualificação dos artigos selecionados. Essa planilha será útil na construção da síntese final da RBS e análise dos resultados obtidos.

A última etapa do processamento (2.3 - documentação) constitui o Passo 6 (Figura 3). Segundo (CONFORTO *et al.*, 2011): "Todos os resultados obtidos durante a fase de processamento, utilizando-se os seis passos apresentados, em conjunto com os filtros de busca e formulários de registro dos artigos, serão úteis na etapa final da RBS".

4.2.3 Terceira etapa: Saída

Etapa final do roteiro RBS *Roadmap* adaptado. Nesta etapa os dados são catalogados, armazenados e por fim é feito a síntese e gerar resultados.

4.2.3.1 Fase 1: Categorização dos estudos selecionados

Nesta fase serão identificados os possíveis resultados divergentes, contraditórios ou conflitantes, sendo o ponto de partida para as recomendações de possíveis mudanças na prática (SOUZA *et al.*, 2010, p. 104). Feito esse reconhecimento torna-se capaz priorizar os artigos e consequentemente identificar os principais periódicos para a área de estudo (CONFORTO *et al.*, 2011, p. 10).

No Apêndice A está disponível a ferramenta de coleta utilizada para organização das informações no estudo. No Apêndice B está a ferramenta utilizada para qualificação dos artigos selecionados.

4.2.3.2 Fase 2: Cadastro e arquivo

Os arquivos selecionados e estudados serão incluídos na coleção de arquivos da pesquisa. Com o auxílio da ferramenta *Google* Planilhas foi criado um inventário cuja finalidade é organizar o material de estudo para o presente trabalho. Os arquivos foram armazenados e ordenados por título, autor(es), ano de publicação e seu respectivo endereço eletrônico. A utilização do *Google* Planilhas permite o compartilhamento do inventário entre os participantes da elaboração deste trabalho, além de ser uma ferramenta fácil de usar quando for necessário alteração no inventário.

4.2.3.3 Fase 3: Síntese e resultados

A síntese engloba atividades como combinar, integrar, modificar, reorganizar, projetar e compor (LEVY; ELLIS, 2006, p. 200). Nesta fase ocorre a discussão dos principais resultados da pesquisa, é feito a comparação entre os resultados da avaliação crítica dos estudos com o conhecimento teórico (SOUZA *et al.*, 2010, p. 104).

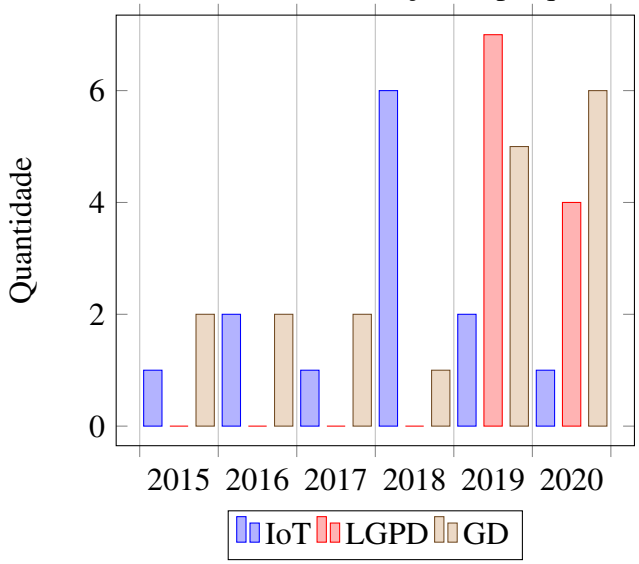
É elaborado um relatório que será um resumo da bibliografia estudada, nele estarão descritos as fases executadas pelo pesquisador, a fim de possibilitar a replicação do estudo (CONFORTO *et al.*, 2011, p. 10).

A RBS deve ser apresentada de maneira clara o objetiva permitindo ao leitor avaliação crítica dos resultados. Sendo assim, deve conter informações pertinentes e detalhadas, com embasamento metodológico contextualizado, sem omissão de qualquer evidência relacionada (SOUZA *et al.*, 2010, 104).

5 RESULTADOS

Para elaboração deste trabalho foi realizada uma revisão bibliográfica sistemática sobre IoT e LGPD. Cento e dez trabalhos foram selecionados para a base bibliográfica, sendo eles artigos, capítulos de livros, dissertações de mestrado e graduação. Desse total, após passarem pelos critérios de filtragem da RBS definidos na seção 4.2.1.6, quarenta e seis foram lidos por completo.

O histograma abaixo trata da quantidade de trabalhos selecionados pela área de estudo (IoT, LGPD, GD) nos anos de limitação da pesquisa.



Os resultados encontrados, de certa forma, são semelhantes entre os trabalhos, alguns analisaram as arquiteturas de rede e os protocolos em busca de fragilidades enquanto outros buscaram meios de contornar essas brechas, propondo uma nova abordagem para resolver o problema em questão. A Tabela 4 abaixo traz um resumo dos resultados analisados.

Tabela 4 – Quadro resumo

Autor(es)	Resultados
(MONTEIRO *et al.*, 2021)	Análise de segurança em redes com base na senhas utilizadas e definição de requisitos para elaboração das senhas
(JUNIOR, 2018)	Proposta de um paradigma para equilíbrio entre a privacidade do usuário e a IoT
(GASETA *et al.*, 2018)	Boas práticas e GD na escolha de uma plataforma de IoT
(SANTOS; PAULA, 2017)	Uso dos *framewroks* ITIL e COBIT na gestão da IoT
(NAKAMURA *et al.*, 2019)	Proposta de uma metodologia de avaliação de riscos envolvendo privacidade e segurança dos dados
(ROCHA *et al.*, 2019)	Uso das normas ISO como ferramenta de controle para a LGPD
(BURHAN *et al.*, 2018)	Apresenta uma visão geral sobre diferentes arquiteturas em camadas na IoT e ataques relacionados à segurança sob a perspectiva de cada camada. Além disso, é apresentada uma revisão dos mecanismos que fornecem soluções para esses problemas
(SANTO *et al.*, 2018)	Revisão bibliográfica sobre as principais características de segurança nos protocolos de comunicação utilizados na IoT alertando para as possíveis falhas
(BORBA, 2018)	Proposta de um modelo de referência a ser adotado na IoT para ter maior segurança na rede
(BURKART, 2021)	Revisão bibliográfica sobre a LGPD a fim de diminuir as lacunas existentes entre os direitos pessoais e a garantia de privacidade da própria Lei
(NOBRE *et al.*, 2019)	Revisão bibliográfica sobre o relacionamento da LGPD com a IoT
(ALMEIDA *et al.*, 2019)	Uso de um modelo com base na segurança adaptativa no contexto da IoT para o gerenciamento da rede

Fonte: o Autor

5.1 Segurança na infraestrutura da IoT

A IoT tem uma característica essencial no que diz respeito à sua capacidade de proporcionar conhecimento sobre o mundo físico. Por meio da coleta de dados e análise dessas coletas é possível descobrir padrões comportamentais do ambiente ou usuários e realizar implicações sobre eles. Por exemplo, a utilização de sensores ligados a pacientes permite aos médicos monitorizarem seu atendimento, dentro ou fora do hospital e em tempo real. A IoT possibilita aprimorar o controle da saúde e prevenção de eventos prejudiciais aos pacientes.

Contudo, para utilizar todo o potencial da IoT é necessário que algumas medidas sejam tomadas. Nesta seção são abordados temas relacionados ao foco do trabalho de maneira mais aprofundada, bem como aspectos de segurança em redes IoT, vulnerabilidades de modelos e arquiteturas comumente utilizados e, por fim, a relação entre esses temas com a LGPD.

Assim como mencionado na Seção 3.1.6, um sistema considerado seguro é aquele

que possui objetivos de segurança desejáveis estabelecidos. Existem diversos objetivos para segurança em IoT, dentre eles os mais referenciados, conhecidos como pilares da SI, são: confidencialidade, integridade e disponibilidade.

Esses aspectos de segurança são necessários e fundamentais em qualquer tipo de rede por onde informações e dados sejam transmitidos.

Na pesquisa (MONTEIRO *et al.*, 2021), o autor realiza uma revisão bibliográfica acerca dos principais desafios relacionados aos aspectos de segurança em redes IoT e seus requisitos de implantação. A proposta do autor dá-se no uso de senhas confiáveis e robustas em todos os dispositivos e redes IoT. O processo inicia-se na criação de senhas no aplicativo gratuito *Safe in Cloud*, neste aplicativo é possível escolher parâmetros para as senhas. Quando a senha é criada, um outro aplicativo indica seu nível de segurança.

Os testes de segurança realizados pelo autor incluíram o site *Kaspersky Password Checker*[1] e o site da Universidade de Illinois em Chicago[2] . Esses testes buscaram analisar parâmetros de quebra da senha, bem como o tempo necessário para sua decodificação, aspectos positivos e negativos da senha como a força da senha, utilização de caracteres especiais.

(MONTEIRO *et al.*, 2021, p. 75) elenca requisitos que uma rede IoT deve garantir visando maior proteção das informações ali presentes. Sendo eles:

1. A senha utilizada no roteador entre os dispositivos IoT e a *internet* deve:
   a) Ter pelo menos 20 caracteres de tamanho;
   b) Utilizar números, letras e caracteres especiais;
2. Seguir o mesmos critérios acima mencionados nas senhas de dispositivos de controle e sensores das redes IoT;
3. Não compartilhamento das senhas com pessoas que não devem ter acesso aos dados em trânsito na rede.

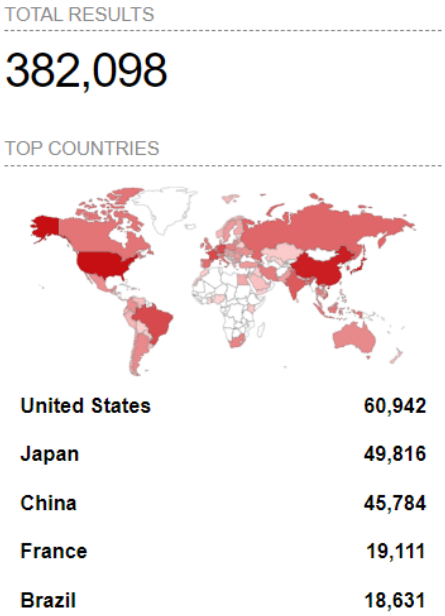
O resultado da pesquisa de (MONTEIRO *et al.*, 2021) revelou dados alarmantes sobre a segurança das redes brasileiras. O autor utilizou a ferramenta *Shodan* para fazer uma busca entre os dispositivos que mantiveram sua senha de acesso padrão de fábrica, ou seja, não sofreram alteração do usuário. A ferramenta permite realizar uma análise de segurança gratuitamente em todos os dispositivos que podem ser localizados na *internet*.

Em uma busca no site *Shodan.io* foram encontrados 382.098 dispositivos, em todo o mundo, que mantiveram a senha "Admin". O Brasil está presente no top 5 dos países que mantiveram a senha de fábrica. Dessa forma, diversas redes brasileiras têm fraquezas na sua própria segurança, e isso é amplamente usado para ataques de intrusão. Logo, a utilização

[1] Site: <https://password.kaspersky.com/pt/>
[2] Site: <https://www.uic.edu>

de uma senha personalizada e exclusiva é de extrema importância na segurança das redes IoT (MONTEIRO *et al.*, 2021, p. 54). Os resultados podem ser observados na Figura 4, abaixo.

Figura 4 – Busca por senha "Admin".



Fonte: SHODAN.IO, 2021

Por sua vez, (JUNIOR, 2018, p. 102) propõe um paradigma para que haja convívio entre a IoT e a privacidade dos usuários sem que a evolução tecnológica domine a privacidade.

O paradigma é composto de 3 etapas, sendo elas definidas abaixo:

1. Princípios

   Primeiramente são considerados os princípios "privacidade"e "política restritiva". Isso significa que os dados são classificados como privados e restritos por padrão, também são estabelecidos critérios que deverão ser seguidos por todas as regras de segurança. Assim, as conexões de entrada e saída são bloqueadas num primeiro momento, qualquer equipamento IoT deve adotar uma política restritiva, e a liberação do acesso deve ocorrer à medida que for necessário (JUNIOR, 2018, p. 106).

2. Validação humana

   A etapa de validação humana salienta a autoridade do usuário na aprovação do uso dos dados privados na IoT, ou seja, afirma a confiança no dispositivo ao qual os dados serão enviados. São decisões humanas desta etapa: permissão explícita do usuário, ciência da necessidade de compartilhamento externo e confiabilidade no dispositivo vinculado. Após a validação, as informações transmitidas são armazenadas em *log* assegurando

auditabilidade posterior (JUNIOR, 2018, p. 107).

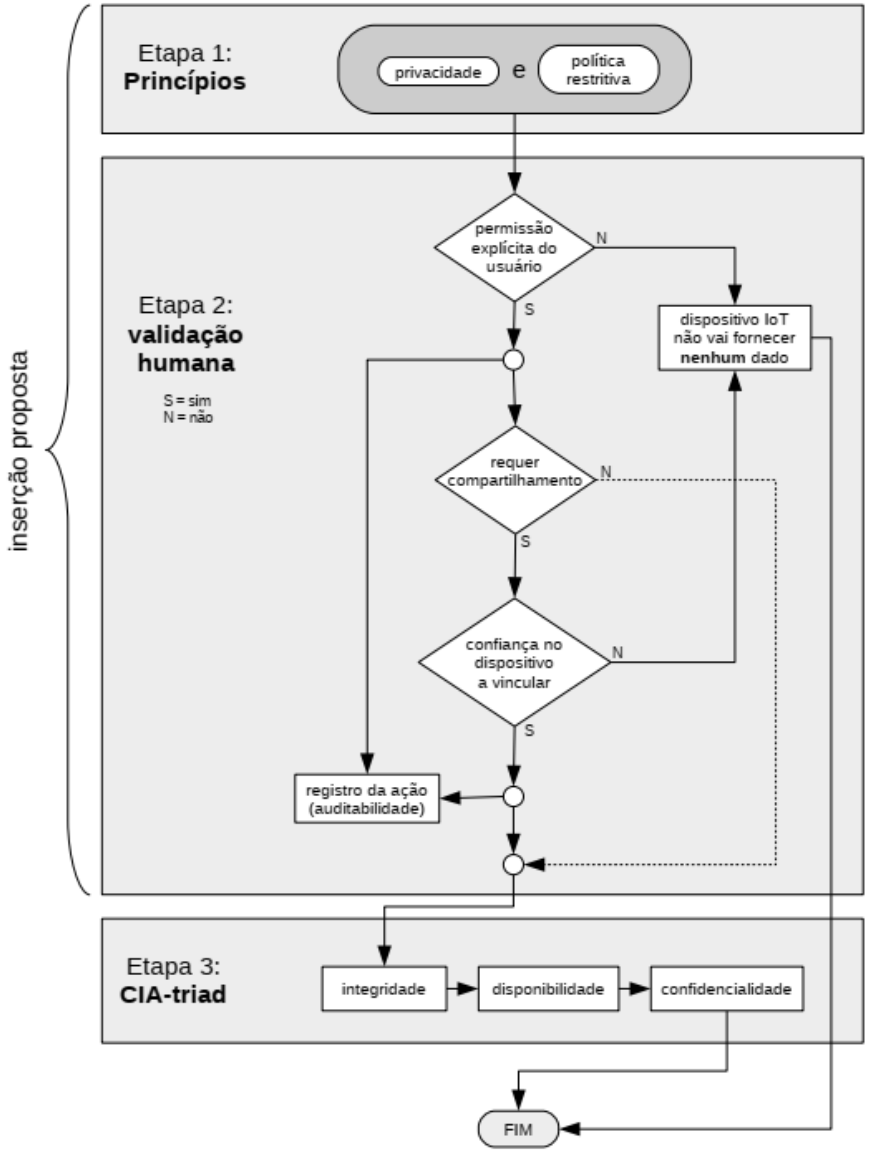
3. Confidencialidade, integridade e disponibilidade

   Uma vez concluídas as etapas anteriores, integra-se a confiabilidade integridade e disponibilidade dos dados com ênfase na proteção.

O autor destaca a abrangência para proteção da privacidade de dados na iot através do paradigma, visto sua observância a leis e regulamentações da área como, por exemplo, a GDPR. Contudo, trata-se de um modelo não testado, e a validação do mesmo é tida como trabalho futuro e continuidade da pesquisa (JUNIOR, 2018, p. 121).

O paradigma está representado na Figura 5, abaixo.

Figura 5 – Fluxograma funcional da abordagem de (JUNIOR, 2018)



Fonte: (JUNIOR, 2018)

A proposta de (GASETA *et al.*, 2018) baseia-se nas boas práticas da GD nos serviços da IoT. Utiliza um modelo de tomada de decisão fundamentado no método *Analytic Hierarchy Process* (AHP) para a escolha de uma plataforma tecnológica para IoT no *framework* COBIT.

A escolha da AHP como método multicritério ocorreu devido ao método se adaptar melhor a situação problema, porque tem uma estrutura hierárquica simples e objetiva, escolha de valores e regra de avaliação da inconsistência já padronizada. Além disso, utilizou-se o COBIT 5 para avaliar a maturidade dos processos de TI do local onde o trabalho foi aplicado.

Em suma, em um primeiro momento, o autor aplicou um formulário para realizar o levantamento das necessidades, deficiências e diagnóstico local. Depois houve a definição dos critérios de análise considerando as características mais importantes para a escolha da plataforma IoT de acordo com o modelo da organização avaliada. Dessa forma, a AHP é utilizada para auxiliar na escolha da plataforma a partir da importância de cada critério (GASETA *et al.*, 2018, p. 24).

Dentre os critérios aplicados estão: segurança, conectividade, escalabilidade, gerenciamento de dados e modelo de operação. Comparando estes pontos com os levantamentos dos demais trabalhos já apresentados nota-se que são pontos em comum quanto a avaliação de uma nova tecnologia e sua implantação.

Assim, o trabalho de (GASETA *et al.*, 2018) apresenta relevância para a área, alinhando os objetivos da pesquisa desenvolvida pelo autor e a importância na definição de diretrizes e ações a serem realizadas durante o estabelecimento de um ambiente tecnológico de forma organizada e planejada é possível a definição das diretrizes para a implantação dos serviços inteligentes desejados.

O trabalho (SANTOS; PAULA, 2017) segue essa mesma linha de raciocínio, tratando da governança de TI com os *frameworks* ITIL e COBIT. Os autores realizaram uma revisão bibliográfica acerca do tema a fim de deliberar sobre propósito dos *frameworks* em questão e o papel de cada um numa organização. No início da pesquisa são detalhados os modelos e apontados os cenários mais adequados para o uso de cada um.

Os resultados da pesquisa apontam para redução de custos e aumento do rendimento na execução dos processos, entretanto, a implantação não é fácil, requer suporte da gerência da organização e o custo pode ser uma barreira orçamentária (SANTOS; PAULA, 2017, p. 23). Os autores também destacam que a adoção de *frameworks* para gestão de TI e GD não necessariamente irá obter resultados imediatos para a organização, mas a adesão deles faz com

que ocorra integração entre seus processos e o negócio. Desse modo, a TI poderá entregar e suportar a demanda dos seus serviços (SANTOS; PAULA, 2017, p. 25).

Já o artigo (NAKAMURA *et al.*, 2019) trata de aspectos relacionados a proteção de dados pessoais, criação de legislação sobre o tema e como as empresas estão lidando para atender as mudanças estabelecidas por tais leis. Os autores apresentam o trabalho com uma avaliação de risco e segurança para amparar empresas na aderência aos requisitos de segurança demandados pela LGPD e GDPR.

Para (NAKAMURA *et al.*, 2019) o uso, com as devidas adaptações, dos *frameworks* ou padrões de segurança é uma das maneiras das empresas que operam com dados pessoais se ajustarem ao que é exigido pelas leis de proteção de dados. Porém, a implantação isolada desses padrões não garante cumprimento total às leis gerais de proteção de dados. "Fundamentalmente, a família de normas 27000 trata de proteção de informações do ponto de vista da entidade que está implementando o SGSI e não do ponto de vista dos direitos dos indivíduos"(NAKAMURA *et al.*, 2019, p. 3).

A metodologia de avaliação de risco proposta pelos autores é composta de 3 fases, sendo elas:

1. Identificação do fluxo de dados pessoais

   A definição do fluxo de dados possibilita a compreensão dos dados e seus estados (dado em uso, movimento, repouso) em todos os seus componentes, ou seja, os pontos de ataque em que podem ocorrer vazamentos (NAKAMURA *et al.*, 2019, p. 4).
2. Análise de *gap* e de serviços

   A análise de *gap* e de serviços visa identificar as necessidades e prioridades para implementação dos controles de segurança indispensáveis no fluxo de dados (NAKAMURA *et al.*, 2019, p. 4).
3. Estratégia de adequação à LGPD

   Definida de acordo com os resultados da análise de *gap* e de serviços (NAKAMURA *et al.*, 2019, p. 4).

Outra pesquisa igualmente interessante é a de (ROCHA *et al.*, 2019). O artigo em questão analisa como a ISO 27.001 pode ser usada como recurso para a LGPD. Para tanto, os autores realizaram uma revisão bibliográfica a fim de comparar a lei e a norma, abarcando pontos em comum entre ambas e assim ter como resultado um meio das empresas entrarem em conformidade à lei.

Entre os pontos que estão presentes tanto na LGPD quanto na ISO 27001, destacados por (ROCHA *et al.*, 2019, p. 89), vale citar:

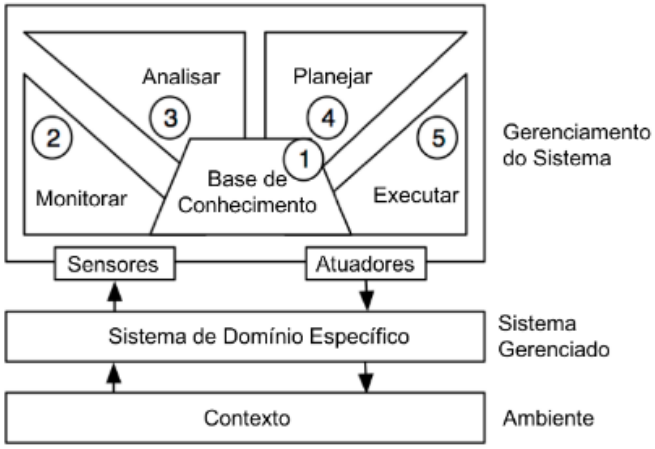
1. Estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da organização;
2. Identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos;
3. Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização;
4. Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços;
5. Manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas;
6. Garantir que a segurança da informação seja parte integrante de todo o ciclo de vida dos sistemas de informação. Isto também inclui os requisitos para sistemas de informação que fornecem serviços sobre as redes públicas;
7. Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação .

De acordo com os autores, se as empresas adotarem o padrão ISO 27001 elas terão *compliance* parcial com a LGPD. Além disso, os empresário serão desafiados a encontrar soluções tecnológicas para garantir a segurança e privacidade das informações dos seus clientes, por outro lado, os usuários serão mais beneficiados pela LGPD, pois passaram a ter mais controle sobre seus dados (ROCHA *et al.*, 2019, p. 96).

Assim, nota-se que o uso de *frameworks* como o ITIL, COBIT e as normas da família ISO 27000 por empresas do ramo da TI, tal como por aquelas que empregam tecnologias da IoT em seus serviços, é bastante relevante ao negócio. A admissão de técnicas de gerência da informação e dos processos significa maior segurança nas atividades desenvolvidas pela empresa e cuidados com o tratamento dessas informações, uma vez que os ciclos bem definidos para a realização do trabalho, definição de uma autoridade nas operações de tratamento, regras de como proceder a cada situação podem atenuar a ocorrência de erros e evitar um problema mais grave, como um vazamento de dados. Lembrando que a inobservância aos cuidados no tratamento dos dados ensejam sanções definidas na LGPD.

Em (ALMEIDA *et al.*, 2019, p. 3), os autores abordam a segurança adaptativa no contexto da IoT. Esse modelo consiste na capacidade do sistema monitorar de forma autônoma em tempo hábil ou de execução o seu comportamento de acordo com a sua situação. Além disso, os autores também frisam a utilização do modelo MAPE-K, ferramenta desenvolvida pela IBM, para realizar as atividades de monitoramento, análise, planejamento e execução empregando um ciclo de controle em um *loop* de *feedback*. O interessante dessa abordagem é que a intervenção da ação humana não ocorrerá frequentemente, visto que o próprio sistema será capaz de se regular. O modelo MAPE-K está ilustrado na Figura 6.

Figura 6 – MAPE-K



Fonte: Adaptado de (IGLESIA; WEYNS, 2015)

(ALMEIDA *et al.*, 2019, p. 3) retratam seu funcionamento da seguinte maneira.

> O componente "Monitor"coleta os dados apropriados dos recursos gerenciados por meio dos sensores. Os dados são correlacionados, filtrados e/ou agregados e o sintoma descoberto é passado para o componente "Analisar". Sintomas e outros dados também podem ser armazenados em uma base de conhecimento compartilhada. O analisador determina se uma mudança precisa ser feita com base no conhecimento compartilhado e nos sintomas. Caso pertinente, uma solicitação de mudança no ambiente é passada para o componente "Planejar". O planejador gera os comandos ou fluxos de trabalho necessários na forma de um plano de alteração que é passado para o componente "Executar". O executor aplica o plano de mudança no recurso de gerenciamento usando os atuadores. Caso necessário, a base de conhecimento pode ser atualizada,fornecendo dados do impacto da adaptação para serem aplicados como *feedback* para o próximo ciclo.

5.1.1 Desafios de segurança nos diferentes modelos de arquitetura IoT

No trabalho (BURHAN *et al.*, 2018), os autores expõem uma visão geral sobre os diferentes modelos de arquitetura em camadas da IoT e os diversos ataques que cada camada

pode sofrer. Também é apresentada uma revisão das técnicas para solucionar esses problemas.

A pesquisa tem por base uma revisão bibliográfica da área para definir os elementos da IoT para então comentar acerca das arquiteturas. Em cada camada são observados os protocolos que nelas atuam e suas vulnerabilidades. Os protocolos abordados são, em grande parte, os mesmos estudados na Seção 3.1.5. No Apêndice C está a síntese dos resultados dessa análise.

Conforme (BURHAN *et al.*, 2018, p. 21), devido as características heterogêneas de cada dispositivo, os recursos de *software* e *hardware* são distintos e limitados. Logo, implementar meios de melhorar a segurança desses dispositivos tornou-se uma tarefa complicada, diante dessa situação muitas técnicas foram propostas e uma delas é o uso de *Software-Defined Network* (SDN). Essa técnica é usada para eliminar restrições em redes tradicionais, além de fornecer melhor desempenho com menor custo.

No modelo SDN existem as figuras de agentes no processo de transmissão de dados, sendo eles o *IoT Agent*, o *IoT Controller* e o *SDN Controller*, essas figuras são importantes porque elas decidirão as ações a serem realizadas no decorrer da transmissão. O agente IoT opera como uma camada de percepção, tem a tarefa de conferir o ambiente constantemente, caso haja alguma alteração ele coleta informações através de sensores e envia essas informações para o controlador IoT. Antes de realizar o envio ocorre autenticação em ambos os dispositivos. O agente IoT verifica a autenticidade antes de enviar e o controlador IoT verifica a autenticidade antes de receber as informações repassadas. O controlador SDN funciona no *backend* dessa arquitetura, ele fornece proteção aos dispositivos gerenciando e controlando a segurança. Por exemplo, se um agente IoT enviar informações falsas para o controlador IoT essa transmissão será interrompida e a entrada da informação na rede será negada. O mecanismo SDN é implementado na camada de rede devido suas características (BURHAN *et al.*, 2018, p. 22). A arquitetura SDN está representada na Figura 7.

Outras propostas dos autores são:

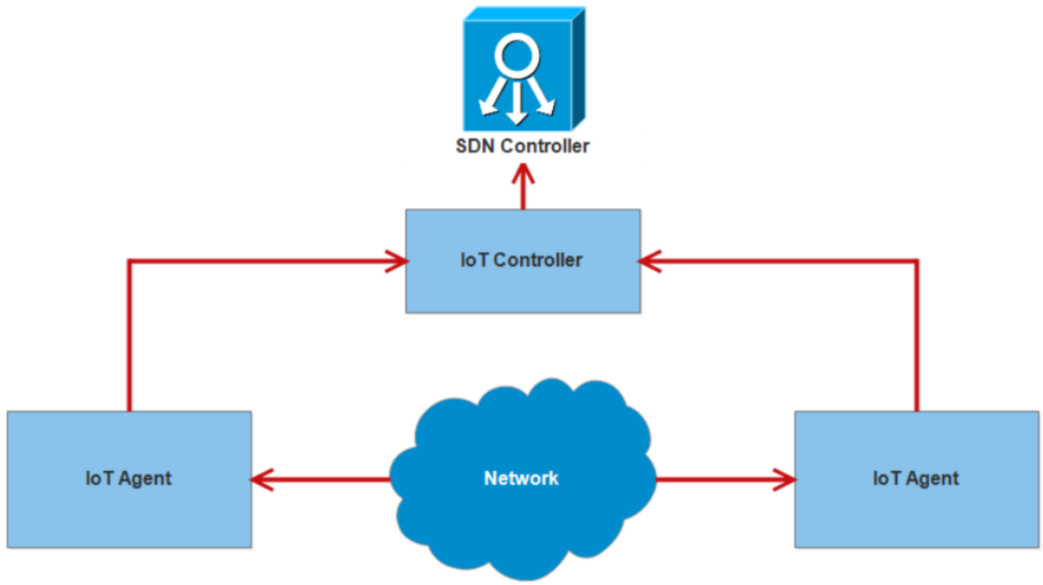
- Protocolo baseado em ambiente *ad hoc*

  A finalidade é detectar os nós que podem afetar toda a rede por meio de seu mau comportamento (BURHAN *et al.*, 2018, p. 22).

- Mecanismo baseado em sistema de reputação

  A detecção do mau funcionamento de um nó em um ambiente de comunicação *ad hoc* ocorre por meio da colaboração dos outros nós. "sempre que um nó recebe um pacote

Figura 7 – Associação de SDN com IoT como uma solução de segurança



Fonte: (BURHAN *et al.*, 2018)

de outros nó, ele aciona um mecanismo de vigilância e armazena o valor em um *buffer* temporário e o compara com o resultado observado. Se ambos forem iguais (calculados e observados), o valor calculado é removido do *buffer* e entra no estágio ocioso e espera por outras observações"(BURHAN *et al.*, 2018, p. 23).

- Sistema de detecção e prevenção de intrusão baseado em *cluster*

  Nessa proposta, a rede é dividida em *clusters* e cada *cluster* tem um chefe. O chefe *cluster* tem a responsabilidade de calcular o nível de confiança de todos os *clusters* existentes em seu intervalo da rede. Se um *cluster* apresentar comportamento malicioso de acordo com o nível de confiança, ele será desprezado, assim a rede para de enviar e receber pacotes através dele (BURHAN *et al.*, 2018, p. 23).

Na pesquisa (YOUSUF *et al.*, 2015), os autores elaboram um *survey* sobre o status atual e as preocupações com a segurança da IoT. Citam o trabalho de (ABOMHARA; KØIEN, 2014) na visão da IoT, as ameaças de segurança existentes e os desafios abertos no domínio da IoT; o *survey* de (ZHAO; GE, 2013) com a exposição de vários problemas de segurança da IoT que existem na estrutura do sistema de três camadas e apresentação de soluções para os problemas, juntamente com as principais tecnologias envolvidas; o artigo de (KHAIRI *et al.*, 2015) que analisa os problemas e desafios de segurança e fornece uma arquitetura de segurança bem definida como uma confidencialidade da privacidade e segurança do usuário; o trabalho de (ROMAN *et al.*, 2011) ao analisar questões de segurança em IoT; e, por fim o artigo de (WEN *et al.*, 2012) que aborda a estrutura de segurança da camada de percepção, camada de rede e

camada de aplicação em IoT.

A proposta de (SANTO *et al.*, 2018) compreende uma revisão sistemática dos principais problemas de segurança que afetam os protocolos de comunicação no contexto da IoT, a fim de identificar suas possíveis ameaças. São analisadas as camadas do modelo TCP/IP (física, rede, transporte e aplicação) e, para cada camada é verificado o tipo de ataque mais propício de acontecer de acordo com as vulnerabilidades encontradas nas camadas e protocolos. Ao final, os autores elaboram um resumo (Figura 8) dos protocolos e suas ameaças mais significantes.

Figura 8 – Ataques que podem ser explorados por camada

CAMADA	PROTOCOLO	AMEAÇA																	
		SSL *Stripping*,;RC4, Problema de Usabilidade	*Eavesdropping*	*Relay*	*Main-in-the-Middle*	*Jamming* Físico	Injeção de Comandos; UDP *Flooding*	*Spoofing*	DoS	Fragmentação	CRIME,;TIME,;*Breach*,; Parâmetro *Diffie-Hellman*	BEAST,;*Passing Oracle*; Problema de Implementação	Roubo de Chaves do RSA; Certificado RSA	*Relay Attack*	*Handshake* Triplo,;Renegociação	Confusão de Hospedeiro Virtual,	Amplificação	*Masquerading*	*Trashing*
Aplicação	CoAP																X	X**	
	MQTT																	X**	X**
Transporte	DTLS	X					X		X		X	X	X		X	X			
Rede	6loWPAN		X		X			X		X				X					
Física e Enlace	RFID e NFC		X*	X	X	X			X										

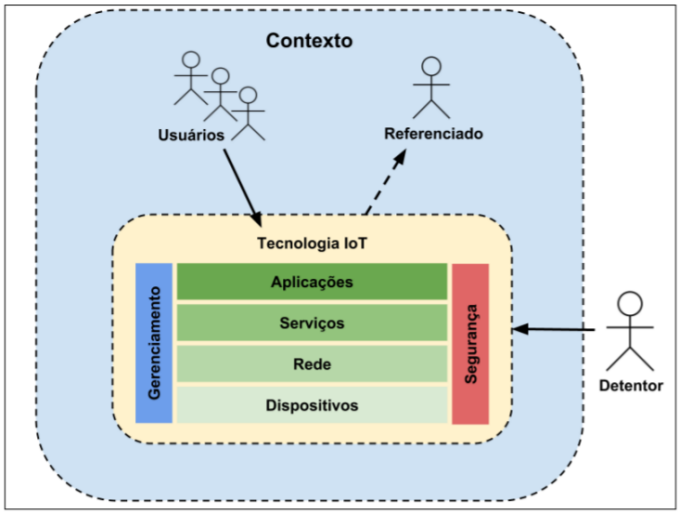
Fonte: (SANTO *et al.*, 2018)

*Modos de segurança sem criptografia.

**CoAP e MQTT estão vulneráveis a certos ataques somente quando não utilizam DTLS.

O modelo proposto por (BORBA, 2018) tem por base os modelos (BAUER *et al.*, 2013), (ITU-T, 2012a) e *Web of Things* (WoT), projeto de padronização de (JACOBS; WALSH, 2004). Neste modelo há a figura do *usuário* (aquele que irá utilizar a tecnologia), o *referenciado* (o alvo de determinada tecnologia), a própria tecnologia, que é composta das camadas horizontais de Aplicação, Serviços, Rede, Dispositivos, e as camadas verticais de Gerenciamento e de Segurança que abrangem as quatro camadas horizontais e, por fim, a figura do *detentor*, sendo este o setor privado, ente governamental ou uma solução particular de uma pessoa física. (BORBA, 2018, p. 70). O modelo está representado na Figura 9.

Figura 9 – Modelo de referência IoT proposto por (BORBA, 2018)



Fonte: (BORBA, 2018)

As camadas de Aplicação, Serviços, Rede, Dispositivos (percepção) já foram vistas na Seção 3.1.4. O Gerenciamento é responsável pelo funcionamento das camadas, bem como realizar o acompanhamento de falhas e outras complicações que podem ocorrer nas outras camadas. A Segurança é responsável por assegurar a implementação de quesitos de segurança e privacidade em todas as camadas da arquitetura. No estudo, o autor considera relevantes as funções de segurança propostas na arquitetura (BAUER *et al.*, 2013), onde são observadas as funções de: Autenticação, Autorização, Confiança e Reputação, Gerenciamento de Identidade, Troca de Chaves e Gerenciamento (BORBA, 2018, p. 75).

A figura do *detentor* tem uma função importante neste modelo. Ele é o responsável pelos dados coletados e tratados pela tecnologia IoT, ou seja, deve garantir a segurança e privacidade para os *usuários* e *referenciados* (BORBA, 2018, p. 71). Assim, o *detentor* assume papel parecido ao dos agentes de tratamento de dados da LGPD, sendo o controlador quando exerce função de tomada de decisão referente ao tratamento de dados e o operador quando realiza

o tratamento de dados (TEMER *et al.*, 2018).

Já ao tratar de redes construídas com base no modelo OSI, as aplicações de segurança estarão em diversas camadas. Assim, a implementação em uma dada camada está ligada aos tipos de ataques que cada camada poderá sofrer. (MONTEIRO *et al.*, 2021, p. 28) analisa os ataques que podem ocorrer neste modelo de arquitetura. São eles:

> Mascaramento: é quando um invasor se faz passar por um usuário autorizado a acessar a rede;
>
> 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* (DoS)): impede que um recurso/dispositivo seja utilizado pelos demais integrantes da rede através da inserção de um grande número de pacotes enviados ao receptor;
>
> 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;
>
> 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 Troia e *Worms*.

Esses ataques e ameaças são mais comuns quando se refere a redes de dados. Para assegurar a proteção da informação e dos dados que trafegam pelas redes IoT é necessário o uso de alguns tipos de contramedidas. Segundo (BUFFENOIR, 1988, p. 147) os tipos mais comuns e eficientes de contramedidas são:

> 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.

Em conjunto, essas contramedidas podem ser utilizadas para garantir maior eficiência. Por outro lado, podem ser aplicadas individualmente para garantir o direcionamento da proteção ao ataque sofrido (MONTEIRO *et al.*, 2021, p.30).

Os resultados dos trabalhos apresentados apontam para uma conclusão comum. Em termos de segurança os riscos são, na maioria dos casos, do tipo DoS, ou seja, ocorre uma sobrecarga em um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus utilizadores, além da obtenção de dados indevidamente aproveitando-se das fraquezas dos dispositivos.

5.2 LGPD

Na seção 3.2 os princípios da LGPD foram apresentados de modo pragmático. Nesta seção o foco será o vínculo entre a IoT e a LGPD. Dessa maneira será possível compreender os desafios enfrentados pela IoT com a adoção da nova lei no território brasileiro.

O desenvolvimento e redução de custos da TI aperfeiçoam os meios de acesso e controle na circulação e obtenção de dados. Torna-se urgente estabelecer métricas de tutela dos direitos fundamentais, com destaque aos que se referem a dados sensíveis (TEPEDINO, 2014, p. 69).

A LGPD surge como ferramenta para basilar a maneira como a informação coletada será tratada. Em seus artigos há questões da segurança, de boas práticas, da fiscalização, dentre outros pontos importantíssimos (SILVA; JESUS, 2020, p. 7).

Quanto aos ramos mais afetados pela LGPD, o *site* do Serviço Federal de Processamento de Dados (SERPRO) enumera as áreas em questão, sendo elas: *Software* e Tecnologia, Direito e Advocacia, Financeira e Seguros, Comércio digital, Pesquisa e Perfilamento, Saúde privada e Planos, Publicidade e *Marketing* (SERPRO, 20–). Além disso, (BURKART, 2021, p .59) salienta que a Lei tem equilíbrio nas esferas federal, estadual e municipal.

A princípio, (BURKART, 2021, p. 84) destaca a importância das pessoas terem noção dos seus direitos. Há uma lacuna entre o direito e o saber e, por tal motivo, ainda que haja uma legislação que verse acerca do assunto, os indivíduos não estão protegidos pois não conhecem seus direitos. A pesquisa da autora teve por objetivo principal analisar a LGPD, trazendo informações sobre a lei e criar um guia para a população brasileira.

Para validar a necessidade do trabalho, a autora realizou entrevistas com especialistas sobre a LGPD, sendo um deles da área do direito e outro da TI. Os resultados da pesquisa expli-

citaram a falta de saber dos indivíduos sobre a nova lei. O estudo propôs reunir as informações fundamentais da lei, seus impactos, sua aplicabilidade nas organizações, além de estreitar o vão entre o conhecimento da sociedade e os direitos do cidadão através da educação tecnológica (BURKART, 2021, p. 85).

(SILVA; JESUS, 2020, p. 5) enfatizam a proximidade no relacionamento da LGPD e a IoT como algo obrigatório. (NOBRE *et al.*, 2019, p. 3) exemplificam essa relação da seguinte maneira:

> A automação residencial, onde dispositivos estariam coletando uma gama de informações pessoais, aplicando algoritmos de inteligência artificial e ainda cruzando estas informações através de *Machine Learning* (ML) afim de gerar estatísticas para detectar padrões e comportamentos. Tais características compõem os principais objetivos de IoT no nicho de automação residencial, sendo os principais desafios; especificar métodos para coleta da autorização de uso dos dados do usuário pela empresa, padrões seguros para transmissão destes dados, modelos para promover o armazenamento seguro destas informações além de procedimentos para apagar todos os dados do usuário quando findado o relacionamento entre o mesmo e a empresa que coletou seus dados.

(NOBRE *et al.*, 2019, p. 3) destacam que apesar de a LGPD oferecer orientações básicas para a regulamentação de serviços, será um trabalho complexo alcançar um equilíbrio entre o tratamento dos dados dos usuários e seus direitos de privacidade.

A pesquisa de (NOBRE *et al.*, 2019) vale-se de uma revisão bibliográfica acerca do relacionamento da LGPD com o uso da IoT, a fim de respaldar a responsabilidade das empresas quanto ao uso e armazenamento dos dados de usuários. De acordo com os autores, essa responsabilidade pode ser alcançada através da aplicação de mecanismos e técnicas da SI onde a abordagem de muitos aspectos da lei está diretamente relacionada a controles e modelos de privacidade de dados.

Os processos de coleta, transmissão e armazenamento de dados são abordados pelos autores com base na SI e as normas ISO como referência de boas práticas e governança.

Durante a fase de coleta, (NOBRE *et al.*, 2019, p. 9) ressaltam a importância dos operadores e controladores em formular regras que estabeleçam as condições da operação, em especial as práticas da família ISO 2700. Além disso, os autores reforçam que outras questões precisam de esclarecimentos e definições, tal como: o regime de funcionamento, os procedimentos (incluindo reclamações e petições de titulares), as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Já para a fase de transmissão, o maior problema encontrado por (NOBRE *et al.*, 2019, p. 9) ocorre por conta dos dispositivos inteligentes, haja vista que tais equipamentos não possuem recursos suficientes para executarem, por exemplo, a pilha TCP/IP e protocolos adaptados para IoT na camada de aplicação. Uma solução abordada pelos autores seria a utilização de *gateways*, onde determinados equipamentos realizam a comunicação e o envio de informações para um ponto comum na rede, suprindo as necessidades dos dispositivos. Esta utilização de *gateways* pode, em um primeiro momento, amparar a escassez de recursos computacionais, entretanto aumenta a topologia da rede e os pontos de vulnerabilidades.

A LGPD traz referências relacionadas à segurança tais como: uso de medidas técnicas e administrativas para proteger os dados pessoais e sigilosos contra acessos nao autorizados, de situações acidentais, ilícitas de destruição, perda ou alteração na comunicação e difusão dos dados (NOBRE *et al.*, 2019, p. 9).

Por fim, o armazenamento dos dados é encarado como um desafio na IoT por (NOBRE *et al.*, 2019, p. 11), dado que não há muitas maneiras de fazer alterações físicas nos dispositivos com intenção de aplicar os requisitos observados na LGPD. Uma possibilidade para contornar esse problema é o uso de criptografia no armazenamento dos dados para aumentar sua segurança.

Os resultados da pesquisa de (NOBRE *et al.*, 2019) indicam a ISO 27002 e 27003 como técnicas de controle dos dados na coleta, utilização de *gateways* para aumentar os recursos de proteção na transmissão dos dados e o uso de criptografia para aumentar a segurança no seu armazenamento como meios de garantir o mínimo de cuidado e privacidade aos usuários, seguindo os princípios da LGPD. Verificou-se ainda a relevância da SI nesse contexto, pois ela serve de base para alcançar os pressupostos legais vistos na LGPD.

6 CONCLUSÃO

A IoT pode representar uma revolução para a sociedade moderna, seu uso proporciona inúmeros cenários de controle e otimização, o que pode ser bastante útil para o usuário. Todavia, questões como segurança, disponibilidade, confidencialidade, acessibilidade, dentre outras, ainda geram incertezas que necessitam mais atenção e melhorias. Além disso, o processamento de dados na era digital também ganhou mais visibilidade, recentemente com a pandemia da Covid-19 a migração de serviços que eram realizados presencialmente já são realizados de modo virtual, o que acarretou em um número mais expressivo de informações trafegando pela *internet*.

Posto isso, a LGPD entra em um cenário de controle das operações que envolvem dados pessoais, tendo em consideração a necessidade de regulamentar e ordenar como esse tratamento deve ser feito.

Ademais, as diretrizes da LGPD obrigaram as empresas a readaptarem seus negócios para que haja compatibilidade à lei. O modo como essas adaptações serão feitas fica a critério da empresa decidir, sendo assim é possível escolher uma solução já existente no mercado ou criar uma nova. No decorrer do presente trabalho foram apresentadas algumas soluções, como as normas da família ISO 27000, a utilização de *framewroks* de gerência de processos, como o ITIL e o COBIT, e até mesmo a adaptação de um modelo de gerenciamento existente, a exemplo o MAPE-K.

Essa escolha leva em consideração fatores internos à empresa, bem como questão financeira e a cultura organizacional. Uma mudança abrupta como essa é algo difícil no começo e tem custos, tanto monetário quanto humano, por isso o investimento em capacitação e tecnologia é algo que agrega valor a empresa.

Outro fator importante a ser considerado é o fator humano, por mais que os protocolos de segurança e os procedimentos estejam todos bem estabelecidos, a falha humana não deixa de estar presente e é uma questão a ser levada em consideração na elaboração de tais protocolos.

Com relação a IoT, a LGPD não será aplicada aos fins particulares, ou seja, um indivíduo que utiliza um dado serviço para fins próprios e não econômicos não estará obrigado a cumprir a lei. Quando se tratar de uma pessoa ou empresa explorando fim comercial em um serviço a lei deverá ser aplicada. Deste modo, o grande desafio das empresas será em como ajustar seu modelo de negócio protegendo os dados dos seus usuários durante todo o tratamento realizado.

No decorrer deste trabalho foram apresentadas algumas propostas de solução para um gerenciamento mais eficiente da rede IoT, os autores de tais propostas se preocuparam em conhecer as tecnologias, entender seu funcionamento e analisar pontos de vulnerabilidades, ou seja, essas soluções foram formadas adequando-se ao que já está em uso e seguindo o texto da LGPD.

É notável a importância de pesquisas sobre as características que proporcionam o funcionamento correto da IoT com as atribuições da LGPD, além de ser um assunto recente e de suma importância para ser estudado. Vale salientar que nem toda tecnologia estará livre de defeitos e falhas ou não tenha algo a ser melhorado.

REFERÊNCIAS

ABOMHARA, M.; KØIEN, G. M. Security and privacy in the internet of things: Current status and open issues. In: IEEE. **2014 international conference on privacy and security in mobile systems (PRISMS)**. [S.l.], 2014. p. 1–8.

ALLIANCE, L. What is lorawan specification. **LoRa Alliance**, 2021. Disponível em: <https://lora-alliance.org/about-lorawan/>. Acesso em: 10 de jun. de 2021.

ALMEIDA, R.; MACHADO, R. da S.; YAMIN, A.; PERNAS, A. M. Revisão sistemática sobre segurança adaptativa ciente de contexto para a internet das coisas. In: SBC. **Anais do XXXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos**. [S.l.], 2019. p. 735–748.

ARMSTRONG, M.; ALMEIDA, M. M. d. J.; SANTOS, E. Marques dos; SOUZA, J. Gileá de. Ciclo de vida da informação no suporte ao processo de inovação: uma proposta de modelo interativo. **Gestão & Planejamento-G&P**, v. 20, 2019.

BAUER, M.; BOUSSARD, M.; BUI, N.; CARREZ, F.; (SIEMENS, C.; (ALUBE, J.; (SAP, C.; MEISSNER, S.; IML, A.; OLIVEREAU, A.; (SAP, M.; JOACHIM, W.; STEFA, J.; SALINAS, A. Internet of things – architecture iot-a deliverable d1.5 – final architectural reference model for the iot v3.0. 07 2013.

BIOLCHINI, J. C. de A.; MIAN, P. G.; NATALI, A. C. C.; CONTE, T. U.; TRAVASSOS, G. H. Scientific research ontology to support systematic review in software engineering. **Advanced Engineering Informatics**, Elsevier, v. 21, n. 2, p. 133–151, 2007.

BORBA, V. U. Proposta de um modelo de referência para internet das coisas: aspectos de segurança e privacidade na coleta de dados. Universidade Estadual Paulista (UNESP), 2018.

BRASIL, W. Uma visão técnica da rede sigfox. **Embarcados**, 2017. Disponível em: <https://www.embarcados.com.br/uma-visao-tecnica-da-rede-sigfox/>. Acesso em: 10 de jun. de 2021.

BUFFENOIR, T. Security in the osi model. **Computer standards & interfaces**, Elsevier, v. 7, n. 1-2, p. 145–150, 1988.

BURHAN, M.; REHMAN, R. A.; KHAN, B.; KIM, B.-S. Iot elements, layered architectures and security issues: A comprehensive survey. **Sensors**, Multidisciplinary Digital Publishing Institute, v. 18, n. 9, p. 2796, 2018.

BURKART, D. V. V. Proteção de dados e o estudo da lgpd. Universidade Estadual Paulista (UNESP), 2021.

CONFORTO, E. C.; AMARAL, D. C.; SILVA, S. d. Roteiro para revisão bibliográfica sistemática: aplicação no desenvolvimento de produtos e gerenciamento de projetos. **Trabalho apresentado**, v. 8, 2011.

ESPÍNDOLA, P. L.; JUNIOR, J. F. S.; ROSA, F.; JULIANI, J. P. Governança de dados aplicada à ciência da informação: análise de um sistema de dados científicos para a área da saúde. **RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação**, v. 16, n. 3, p. 274–298, 2018.

FONSECA, G. d. O. d.; MACHADO, G. P.; MACHADO, T. L. D. Near field communication. **Grupo de Teleinformática e Automação / UFRJ**, 2018. Disponível em: <https://www.gta.ufrj.br/ensino/eel878/redes1-2018-1/trabalhos-v1/nfc/>. Acesso em: 10 de jun. de 2021.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. [S.l.]: AMGH Editora, 2009.

G1. Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. **Globo.com**, 2021. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml>. Acesso em: 26 de jul. de 2021.

GASETA, E. R. *et al.* Diretrizes para governança e implantação de serviços em um campus universitário inteligente. Pontifícia Universidade Católica de Campinas, 2018.

GOGONI, R. O que é bluetooth? **tecnoblog**, 2019. Disponível em: <https://tecnoblog.net/278962/o-que-e-bluetooth/>. Acesso em: 10 de jun. de 2021.

HINTZBERGEN, J.; HINTZBERGEN, K.; SMULDERS, A.; BAARS, H. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**. [S.l.]: Brasport, 2018.

IGLESIA, D. G. D. L.; WEYNS, D. Mape-k formal templates to rigorously design behaviors for self-adaptive systems. **ACM Transactions on Autonomous and Adaptive Systems (TAAS)**, ACM New York, NY, USA, v. 10, n. 3, p. 1–31, 2015.

ITU-T. Itu-t y.2060: Overview of the internet of things. ITU, 2012. Disponível em: <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559>. Acesso em: 25 de nov. de 2021.

ITU-T. **New ITU standards define the Internet of Things and provide the blueprints for its development**. [S.l.]: ITU, 2012.

JACOBS, I.; WALSH, N. Architecture of the world wide web. wc recommendation. **World Wide Web Consortium (WC), Dec.,.: http://www. w3. org/TR/2004/REC-webarch-20041215/.(Cit. on p.)**, 2004.

JUNIOR, D. M. M. **Segurança da informação: uma abordagem sobre proteção da privacidade em internet das coisas.** Tese (Doutorado) — Pontifícia Universidade Católica de São Paulo, Brazil, 2018.

KHAIRI, A.; FAROOQ, M.; WASEEM, M.; MAZHAR, S. A critical analysis on the security concerns of internet of things (iot). **Perception**, v. 111, 2015.

LEVY, Y.; ELLIS, T. J. A systems approach to conduct an effective literature review in support of information systems research. 2006.

LORENZON, L. N. Análise comparada entre regulamentações de dados pessoais no brasil e na união europeia (lgpd e gdpr) e seus respectivos instrumentos de enforcement. **Revista do Programa de Direito da União Europeia**, v. 1, p. 39–52, 2021.

LOUREIRO, G. d. S. M.; SOUZA, I. Q. d.; LOPES, M. G. d. M. Rfid- identificação por rádio frequência. **Grupo de Teleinformática e Automação / UFRJ**, 2015. Disponível em: <https://www.gta.ufrj.br/grad/15_1/rfid/>. Acesso em: 10 de jun. de 2021.

LUGLI, D.; SOBRINHO, D. G. Tecnologias wireless para automação industrial: Wireless_hart, bluetooth, wisa, wi-fi, zigbee e sp-100. **Instituto Nacional de Telecomunicações Inatel**, 2012.

MARR, B. As cinco maiores tendências da internet das coisas para 2021. **Forbes**, 2020. Disponível em: <https://forbes.com.br/forbes-tech/2020/10/as-5-maiores-tendencias-da-internet-das-coisas-para-2021/>. Acesso em: 10 de jun. de 2021.

MOMO, F. d. S.; LIMA, M. C. R. Tópicos emergentes em sistemas de informações gerenciais: contabilidade e tecnologia: o novo contexto contábil. [sn], 2021.

MONTEIRO, T. G. *et al.* Análise de requisitos de segurança para uma rede de iot. Pontifícia Universidade Católica de Campinas, 2021.

NAKAMURA, E.; FILHO, J. R. F.; IDE, M. C. Metodologia de avaliação de riscos e medidas de segurança na proteção de dados pessoais. In: SBC. **Anais do V Workshop de Regulação, Avaliação da Conformidade e Certificação de Segurança**. [S.l.], 2019. p. 11–16.

NOBRE, J.; LOPES, R.; GOMES, M.; OLIVEIRA, N. de. Segurança da informação para internet das coisas (iot): uma abordagem sobre a lei geral de proteção de dados (lgpd). **Revista Eletrônica de Iniciação Científica em Computação**, v. 17, n. 4, 2019.

OLIVEIRA, M. S.; PEIXOTO, S. C.; SANTOS, A. F.; MANIÇOBA, R. H. C.; GUIMARÃES, M. A. Aplicaçao das normas abnt nbr iso/iec 27001 e abnt nbr iso/iec 27002 em uma média empresa. **Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica**, v. 6, n. 2, 2016.

OSTEC. Itil: Saiba o que é e conheça a sua história. **OSTEC - Segurança Digital de Resultados (Site)**, 2016. Disponível em: <https://ostec.blog/certificacoes-seguranca/itil-conceito-e-historia/>. Acesso em: 10 de jun. de 2021.

PEREIRA, C.; FERREIRA, C. Identificação de práticas e recursos de gestão do valor das ti no cobit 5/identification of it value management practices and resources in cobit 5. **Revista Ibérica de Sistemas e Tecnologias de Informação**, Associação Ibérica de Sistemas e Tecnologias de Informacao, n. 15, p. 17, 2015.

PINHEIRO, P. P. **Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018-LGPD**. [S.l.]: Saraiva Educação SA, 2020.

RAMAKRISHNA, C.; KUMAR G. K.AND REDDY, A. M.; RAVI, P. A survey on various iot attacks and its countermeasures. **International Journal of Engineering Reasearch in Computer Science and Engineering (IJERCSE)**, v. 5, n. 4, p. 143–150, 2018.

RAPÔSO, C. F. L.; LIMA, H. M. de; JUNIOR, W. F. de O.; SILVA, P. A. F.; BARROS, E. E. de S. Lgpd-lei geral de proteção de dados pessoais em tecnologia da informação: Revisão sistemática. **RACE-Revista de Administração do Cesmac**, v. 4, p. 58–67, 2019.

ROCHA, C. P. da; CARNEIRO, A. V. S.; MEDEIROS, M. V. B.; MELO, A. Segurança da informação: A iso 27.001 como ferramenta de controle para lgpd. **Revista de Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará**, v. 2, n. 3, p. 78–97, 2019.

ROMAN, R.; NAJERA, P.; LOPEZ, J. Securing the internet of things. **Computer**, IEEE, v. 44, n. 9, p. 51–58, 2011.

RUIZ, L. B.; CORREIA, L. H. A.; VIEIRA, L. F. M.; MACEDO, D. F.; NAKAMURA, E. F.; FIGUEIREDO, C. M.; VIEIRA, M. A. M.; BECHELANE, E. H.; CAMARA, D.; LOUREIRO, A. A. *et al.* Arquiteturas para redes de sensores sem fio. **Tutorial of the simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos(SBRC)**, 2004.

SANTINI, B.; CRUZ, H. V.; VALOIS, R.; CHUNG, R.; GALVÃO, R. A eficacia da lei geral de proteção de dados (lgpd). **OAB Pernambuco: O que estã fazendo com meus dados? A importância da Leieral de Proteção de Dados (LGPD) - Capítulo 2: A eficacia da Lei Geral de Proteção de Dados Pessoais**, 2019. Disponível em: <https://www.udop.com.br/download/noticias/2020/03_03_20_arquivo_oab_pe.pdf#page=19>. Acesso em: 10 de jun. de 2021.

SANTO, W. do E.; ORDOÑEZ, E.; RIBEIRO, A. Uma revisão sistemática sobre a segurança nos protocolos de comunicação para internet das coisas. **Journal on Advances in Theoretical and Applied Informatics**, v. 4, n. 1, p. 1–9, 2018.

SANTOS, B. P.; SILVA, L. A.; CELES, C. S.; NETO, J. B. B.; PERES, B. S.; VIEIRA, M. A. M.; VIEIRA, L. F. M.; GOUSSEVSKAIA, O. N.; LOUREIRO, A. A. Internet das coisas: da teoria à prática. 2016.

SANTOS, D. F. dos; PAULA, L. M. de. Alinhando a governança de ti com os negócios: um estudo entre cobit e itil. **Revista de Tecnologia Aplicada**, v. 5, n. 3, p. 16–26, 2017.

SANTOS, I. M. F. d. **Uma proposta de governança de dados baseada em um método de desenvolvimento de arquitetura empresarial**. Dissertação (Mestrado), 2010.

SEBRAE. Conhecendo a lei nº 13.709 - lgpd e as novas regulamentações. **SEBRAE**, 2020.

SERPRO. O impacto da lgpd nos negócios. SERPRO, 20–. Disponível em: <https://www.serpro.gov.br/lgpd/empresa/o-impacto-lgpd-nos-negocios>. Acesso em: 25 de nov. de 2021.

SILVA, A. B. M. D.; CARVALHO, F. F. D.; NAZARIO, M. D. Constrained application protocol - coap. **Grupo de Teleinformática e Automação / UFRJ**, 2019. Disponível em: <https://www.gta.ufrj.br/ensino/eel878/redes1-2019-1/vf/coap/>. Acesso em: 10 de jun. de 2021.

SILVA, I. L. d. O. da; JESUS, D. S. de. O impacto do avanço da internet das coisas no brasil. **Brazilian Journal of Development**, v. 6, n. 12, p. 101749–101758, 2020.

SOUZA, M. T. d.; SILVA, M. D. d.; CARVALHO, R. d. Revisão integrativa: o que é e como fazer. **Einstein (São Paulo)**, SciELO Brasil, v. 8, n. 1, p. 102–106, 2010.

TEMER, M.; JARDIM, T.; FILHO, A. N. F.; GUARDIA, E. R.; JUNIOR, E. P. C.; OCCHI, G. M.; KASSAB, G.; ROSÁRIO, W. D. C.; ROCHA, G. D. V.; GOLDFAJN, I. *et al.* Lei nº 13.709, de 14 de agosto de 2018. Diário Oficial da União, Seção 1, p. 59, 2018.

TEPEDINO, G. Liberdades, tecnologia e teoria da interpretação. **Revista Forense**, v. 419, p. 77–96, 2014.

TSCHOFENIG, H.; ARKKO, J.; THALER, D.; MCPHERSON, D. Architectural considerations in smart object networking. **RFC 7452**, 2015.

VASHI, S.; RAM, J.; MODI, J.; VERMA, S.; PRAKASH, C. Internet of things (iot): A vision, architectural elements, and security issues. In: IEEE. **2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)**. [S.l.], 2017. p. 492–496.

WEN, Q.; DONG, X.; ZHANG, R. Application of dynamic variable cipher security certificate in internet of things. In: IEEE. **2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems**. [S.l.], 2012. v. 3, p. 1062–1066.

YOUSUF, T.; MAHMOUD, R.; ALOUL, F.; ZUALKERNAN, I. Internet of things (iot) security: Current status, challenges and countermeasures. **International Journal for Information Security Research (IJISR)**, v. 5, n. 4, p. 608–616, 2015.

YUAN, M. Conhecendo o mqtt. **IBM**, 2017. Disponível em: <https://developer.ibm.com/br/technologies/iot/articles/iot-mqtt-why-good-for-iot/>. Acesso em: 10 de jun. de 2021.

ZHAO, K.; GE, L. A survey on the internet of things security. In: IEEE. **2013 Ninth international conference on computational intelligence and security**. [S.l.], 2013. p. 663–667.

APÊNDICE A – CATEGORIZAÇÃO DOS ESTUDOS SELECIONADOS

Tabela 5 – Categorização dos estudos selecionados

Nº	Título	Autor	Ano	Origem	Citações	*URL*

Fonte: O autor

APÊNDICE B – QUALIFICAÇÃO DOS ESTUDOS SELECIONADOS

Tabela 6 – Qualificação dos estudos selecionados

Nº	Título	Autor	Objetivo	Resultados	Metodologia	*URL*

Fonte: O autor

APÊNDICE C – TECNOLOGIAS DE COMUNICAÇÃO USADAS EM IOT

Tabela 7 – Comparação de diferentes tecnologias de comunicação usadas em IoT

Tecnologia	Mecanismo	Segurança	Aplicações	Características	Incoveniente
ZigBee	*Wireless*	Criptografia e Integridade	Casa e Indústria	Baixo consumo e Barato	Chave fixa
Bluetooth	*Wireless*	Criptografia e Autenticação	PDA, *Mobiles* e *Laptops*	Substituição do Cabo e Baixo Custo	*Blue jacking* e *Bluesnarfing*
RFID	Frequência de ondas	Encriptação (AES, DES)	Cuidados com Saúde	Captura de dados sem duplicação	Não Autorização
WSN	*Wireless*	Criptografia Chave e Autenticação	Edifícios e Cuidados com Saúde	Baixo Custo e Potência	Ataque DoS
Wi-Fi	Sinais de rádio	Autenticação e Autorização	Telefonez, PC e IoT	Mais Rápido e Seguro	Espionagem
Rede 5G	*Wireless*	Autenticação e Autorização	Telefone, Multimídia e IoT	Mais Rápido e Seguro	DoS distribuído

Fonte: Adaptado de (BURHAN *et al.*, 2018, p. 13)