# PRIVACIDADE E SEGURANÇA DOS DADOS PESSOAIS A RESPEITO DA INTERNET DAS COISAS

Pedro Henrique Gomes Dourado

POSSE– GO

2022

**PEDRO HENRIQUE GOMES DOURADO**

# PRIVACIDADE E SEGURANÇA DOS DADOS PESSOAIS A RESPEITO DA ITERNET DASCOISAS

Trabalho apresentado como requisito para a Conclusão do Curso de Bacharelado em Sistemas de Informação da Universidade Estadual de Goiás.

**Orientador(a):** Prof. Esp. Givanilde de Assis dos Santos Oliveira

**Coorientador:** Prof. Dr. Roberto Felício Oliveira

POSSE– GO

2022

**COMISSÃO EXAMINADORA**

_____
Prof. Esp. Givanilde de Assis
dos Santos Oliveira
Universidade Estadual de Goiás

_____
Prof. Dr. Roberto Felício Oliveira
Universidade Estadual de Goiás

_____
Prof. Esp. Cristiane Batista Xavier
Universidade Estadual de Goiás

_____
Prof. Esp. Aparecido Alves da Silva Júnior
Universidade Estadual de Goiás

Posse, ____ de_____ de 2022

## FICHA CATALOGRÁFICA

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UEG
com os dados fornecidos pelo(a) autor(a).

GG633 p

Gomes Dourado, Pedro Henrique
Privacidade e segurança dos dados pessoais a respeito da internet das coisas / Pedro Henrique Gomes Dourado; orientador Givanilde de Assis dos Santos Oliveira; co-orientador Roberto Felício de Oliveira. -- Posse- Go, 2023.
40 p.

Graduação - Sistemas de Informação -- Unidade de Posse, Universidade Estadual de Goiás, 2023.

1. Tecnologia. 2. Internet das Coisas. I. de Assis dos Santos Oliveira, Givanilde , orient. II. Felício de Oliveira, Roberto, co-orient. III. Título.

## DEDICATÓRIA

A Deus, por ser extremamente paciente e piedoso comigo...

Aos meus, aos que sonham em todas as horas...

## AGRADECIMENTOS

A Deus primeiramente! Pela força e por me guiar a seguir este caminho, por me ajudar a enfrentar todos os obstáculos ao longo desta jornada.

A minha família, pela confiança e motivação para que eu possa sempre alcançar meus objetivos.

Aos meus amigos e colegas pelos incentivos e por compreenderem a minha ausência enquanto eu dedicava meu tempo a este trabalho, pois é uma etapa muito importante em minha vida.

Aos meus professores orientadores, pela paciência, auxílio e orientações, que de perto me permitiram e proporcionaram apresentar um melhor desempenho para realizar este sonho.

**EPÍGRAFE**

“Não podemos prever o futuro,

mas podemos criá-lo.”

(Peter Drucker)

## RESUMO

A Internet das Coisas (*Internet of Things - IoT)* pode ser definida como uma rede de sensores que se comunicam e compartilham informações entre si, desempenham atividades de identificação inteligente, localização, rastreamento, monitoramento e administração de ‘coisas’. A *IoT* atualmente possui grande relevância no momento atual da sociedade, porque ela oferece várias possibilidades de aplicações em diversas áreas como por exemplo negócios, saúde, agricultura, espaços públicos, e também possibilita automatização e auxílio de algumas tarefas do dia a dia das pessoas e usuários. Mediante a isto, existe a preocupação com a privacidade e a segurança dos dados pessoais a respeito desta tecnologia, pelo fato da facilidade referente a coleta de dados das pessoas e as particularidades dos dispositivos que compõem este ecossistema. Através da revisão de literatura e utilização do método de pesquisa bibliográfica foi possível colher informações relacionadas a este tema. Foi possível verificar através dos resultados obtidos, alguns riscos, como por exemplo o monitoramento intenso, coleta de dados e informações médicas, e o desafio da privacidade nos espaços públicos, são apresentadas particularidades sobre esta tecnologia, e alguns ataques que são inferidos na *IoT*. A partir desses resultados conclui-se que, embora exista preocupações por parte do ordenamento jurídico, sobre a proteção dos dados pessoais, ainda existem desafios nesse contexto de privacidade dos dados pessoais. É ressaltada neste trabalho a importância da preocupação com a segurança, atualização e manutenção de dispositivos, e aparelhos conectados à *internet*.



**Palavras-chave:** Tecnologia, dados, privacidade, segurança, Internet das Coisas.

***ABSTRACT***

*The Internet of Things (IoT) can be defined as a network of sensors that communicate and share information with each other, perform activities of intelligent identification, location, tracking, monitoring and administration of 'things'. The IoT currently has great relevance in the current moment of society, because it offers several possibilities of applications in different areas such as business, health, agriculture, public spaces, and also enables automation and assistance of some day-to-day tasks of people and users. In light of this, there is concern about the privacy and security of personal data regarding this technology, due to the fact that it is easy to collect data from people and the particularities of the devices that make up this ecosystem. Through the literature review and use of the bibliographic research method, it was possible to collect information related to this theme. It was possible to verify through the results obtained, some risks, such as intense monitoring, data collection and medical information, and the challenge of privacy in public spaces, particularities about this technology are presented, and some attacks that are inferred in IoT. From these results it is concluded that, although there are concerns on the part of the legal system, about the protection of personal data, there are still challenges in this context of privacy of personal data. This work highlights the importance of concern for security, updating and maintenance of devices and devices connected to the internet.*

***Key Words:*** *Technology, data, privacy, security, Internet of Things.*

## LISTA DE TABELAS

## LISTA DE FIGURAS

## LISTA DE SIGLAS, ABREVIAÇÕES E SÍMBOLOS

| | | | |
|---|---|---|---|
| *IoT* | - | *Internet of Things* | 14 |
| LGPD | - | Lei Geral de Proteção de Dados | 19 |
| *TICs* | - | Tecnologia da Informação e Comunicação | 19 |
| *M2M* | - | Machine to Machine | 19 |
| *WSNs* | - | Wireless sensor network | 25 |
| *DoS* | - | *Denial of Service* | 26 |
| *DDoS* | - | *Distributed Denial of Service* | 26 |
| *WEF* | - | *World Economic Forum* | 26 |
| *DNS* | - | *Domain Name System* | 27 |

SUMÁRIO

# 1 INTRODUÇÃO

A Internet das Coisas (*Internet of Things - IoT* ) pode ser definida como “uma rede de sensores que se comunicam e compartilham informações entre si, com o intuito de desempenhar atividades de identificação inteligente, localização, rastreamento, monitoramento e administração de ‘coisas’” (LOUISE, 2018). A ideia básica da *IoT* é conectar à *internet* objetos comuns do dia a dia, melhorar a qualidade de vida dos seus usuários, utilizando para isso objetos inteligentes. Nesse contexto desta tecnologia a privacidade e a segurança são questões que estão ligadas intimamente a quem pode ter o controle e acesso dos dados e informações pessoais.

A importância de se estudar esse tema é que ele possui bastante relevância no momento atual da nossa sociedade e no mundo, pelo fato de que esta tecnologia é considerada por muitos especialistas da área como a nova era da *internet.* Este ecossistema inteligente, de acordo com a literatura, oferece aplicações para as mais diversas áreas de negócios, do comércio, da agricultura e da indústria. A *IoT* faz com que as tecnologias desenvolvidas para a Internet das Coisas possam influenciar na vida de todas as pessoas, diretamente ou indiretamente (SOUZA 2022).

No entanto, um problema relacionado a este tema, seria a preocupação com a privacidade e a segurança dos dados pessoais, que são gerados ou administrados por dispositivos e infraestruturas de *IoT.* “O uso de dispositivos móveis, a disseminação de sensores, nas cidades, nos prédios e nos corpos ampliam as possibilidades de coleta de dados pessoais.” (AMADEU 2017, pg. 43). Deve-se levar em consideração que atualmente existe uma ampla possibilidade e facilidade de coleta e processamento de dados pessoais, proporcionados por tecnologias emergentes e dispositivos inteligentes.

Outro ponto é que esses dispositivos que compõem o ecossistema, possuem limitação de recursos, como por exemplo, fontes de alimentação, que na maioria dos casos são dispositivos pequenos que necessitam de algum tipo de fonte de energia, como baterias, para manterem seu estado normal de funcionamento. Outro exemplo desta limitação de recurso é a de poder de processamento por parte dos dispositivos, com isto, estes componentes podem estar na mira de atacantes que

podem inferir softwares maliciosos, colocando em perigo a integridade, privacidade e a segurança dos dados e informações pessoais dos usuários.

Nesse contexto, o desenvolvimento desta revisão da literatura sobre o tema privacidade e segurança dos dados pessoais, contribuiu com informações concretas e precisas sobre o assunto abordado, que servirão para que a sociedade e comunidade acadêmica interessada no tema possa utiliza-las para aumentar o seu conhecimento sobre o assunto. Uma vez que as revisões têm a função de possibilitar uma análise sobre um determinado assunto a partir de diferentes perspectivas, auxiliando em sua compreensão (ROTHER, 2007).

## 1.1 JUSTIFICATIVA

Embora esse tema seja muito relevante em nosso cenário atual conforme apresentado no estudo de Louise 2018 e Souza 2019, até o momento foram encontrados poucos trabalhos que discutam esse assunto sob o ponto de vista teórico e contextual, compilando as informações mais importantes sobre ele nas obras encontradas referentes aos autores (Figueira, 2016, Rovere, 2022).

Dessa maneira, foi realizada uma revisão de literatura sobre o tema privacidade e segurança dos dados pessoais a respeito da internet das coisas, isso contribuiu com a ampliação dos conhecimentos dos leitores sobre essa temática específica, pois as revisões tem a função de preencher as lacunas existentes na literatura através da combinação de diferentes pesquisas bibliográficas (CORDEIRO, 2007).

O que justificou a realização deste trabalho desenvolvido, pois a função dele é sumarizar as principais descobertas científicas sobre o tema proposto e apresentar os resultados obtidos para uma análise sobre o assunto.

## 1.2 Objetivos

### 1.2.1 Objetivo geral

O objetivo deste estudo foi a realização de uma revisão de literatura sobre o tema privacidade e segurança dos dados pessoais a respeito da internet das coisas.

### 1.2.2 Objetivos específicos

- Apresentar informações referentes ao ecossistema Internet da Coisas;
- Levantar informações relacionados ao contexto da privacidade e a segurança dos dados pessoais a respeito da tecnologia Internet das Coisas;
- Identificar ameaças referentes a segurança dos dados na *IoT;*
- Verificar informações jurídicas sobre a privacidade dos dados pessoais;

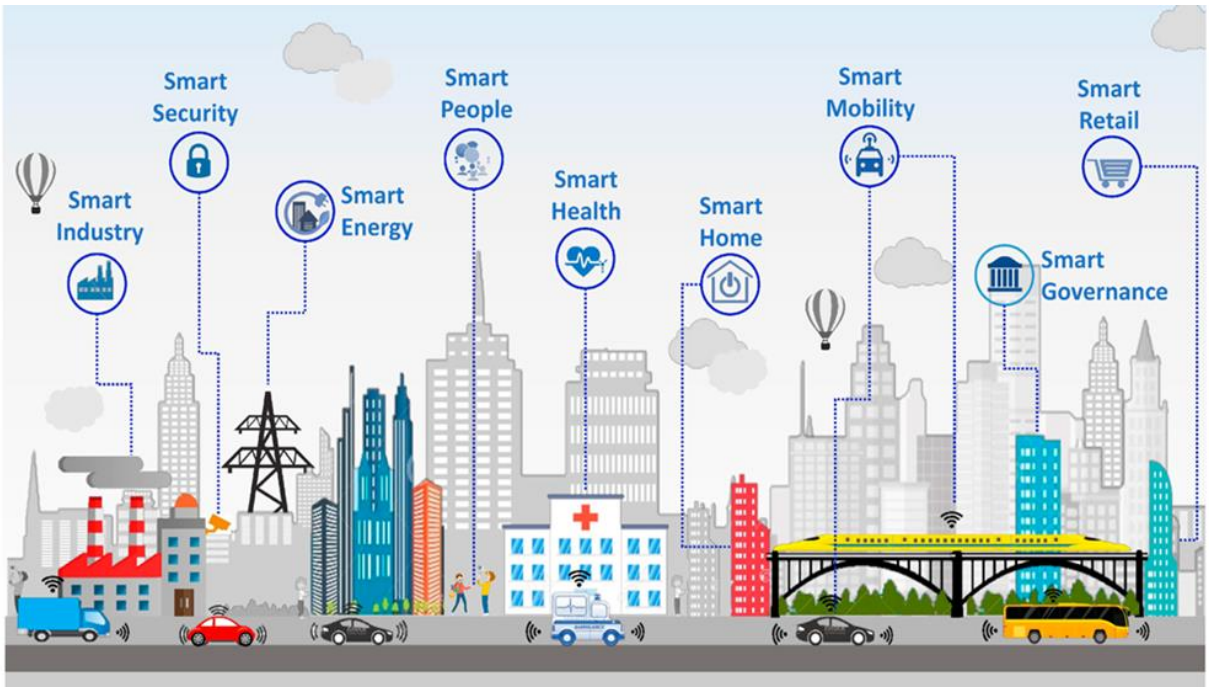
# 2 REVISÃO DA LITERATURA

## 2.1 Introdução à Internet das Coisas (*IoT)*

A *Internet of Things IoT*, ou Internet das Coisas, como é chamada em português, ganhou uso pela primeira vez em 1999 por Ashton (2009), um dos autores pioneiros nesse tipo de tecnologia (CESAR 2015). A *IoT* pode ser compreendida como uma extensão da *Internet* atual, onde propicia que objetos do dia a dia que possuem capacidade computacional e de comunicação, se conectem à *Internet* e possam ser controladas remotamente e acessadas como provedores de serviços (SANTOS et al., 2016). Estes objetos são conhecidos e mencionados pela literatura na maioria das vezes como “coisas” e podem estar presentes em vários ambientes.

Assim, esta tecnologia pode ser utilizada para uma ampla variedade de aplicações, incluindo residências, aeroportos, estações, segurança e vigilância, transporte, cidades, agricultura, saúde, indústria, logística e meio ambiente, como pode ser observado na Figura 1.

**Figura 1.** Representação da presença da *IoT* nos mais variados ambientes




**Fonte:** https://www.bing.com/

Não há quase nenhuma área de aplicação onde o *IoT* não consiga encontrar uma função e principalmente não há área de aplicação onde *a IoT* não traga alguma vantagem econômica ao longo do tempo (SILVA,2017). A seguir a contextualização de algumas das aplicações desta tecnologia:

• *Healthcare (Saúde)*: Atividades *fitness* que se resumem no monitoramento e controle da frequência cardíaca, e funções vitais durante os exercícios (de Jesus, 2021). Com a *IoT*, um paciente pode ser observado e, em alguns casos, tratado remotamente através de câmeras de vídeo e outros atuadores eletrônicos. Conforme a empresa de consultoria (Tractica 2016), com a ajuda da *IoT* é possível medir indicadores como a pressão arterial, batimentos cardíacos e temperatura corporal à distância (Cristina, 2018).

• *Smart Home* (Casas inteligentes): Esse conceito de moradia envolve o uso da tecnologia para garantir mais conforto, segurança e praticidade aos moradores(de Jesus 2021). Uma *Smart home* pode facilitar verdadeiramente a vida dos seus habitantes, podendo ter facilidades desde controlar à distância o ar condicionado, as luzes e a máquina de lavar através do *Smartphone* (Miguel,2016);

• *Smart Cities (cidades* inteligentes): São basicamente diversos sensores espalhados pela cidade com objetivo de monitorar e analisar um ambiente, (INTERNATIONAL BUSINESS MACHINES, 2011). *Smart Cities* também são instrumentos para melhorar a competitividade de tal forma que a comunidade e a qualidade de vida são reforçadas. (Batty et al., 2012).

O ambiente da internet das coisas envolve objetos físicos e a qualidade da internet, propiciando as comunicações e compartilhamento de dados entres os dispositivos inteligentes através da rede. Também pode-se mencionar fontes de energia da qual é necessário para realizar o seu funcionamento, processamento e coleta de dados. Objetos físicos interconectados com a internet por meio de sensores pequenos e embutidos, criam um ecossistema de computação onipresente (ubíqua), voltado para a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia" (MAGRANI 2018, pag. 20).

Além disso, é importante relatar que a *IoT* está associada a hiper conectividade, comunicação máquina a máquina (M2M), assuntos inter-relacionados a *IoT*, pois no

ambiente da internet das coisas os objetos que possuem capacidade de produzir dados, trazem interatividade e sempre estão compartilhando dados entre si, e trocando informações com a outras máquinas utilizadas por usuários através da rede de internet, e de acordo com LOUISE 2018:

> A M2M e a comunicação entre humano e máquina fazem dos dispositivos partes integrais de uma sociedade mais conectada, em que se observa o emprego de big data e a expansão de plataformas capazes de administrar essas redes de “coisas”. (LOUISE 2018, pg. 11).

A promessa da *IoT* é a de que a proliferação de dispositivos e a possibilidade de captação de dados em massa resultem em uma maior capacidade de conhecer eventos, fenômenos e indivíduos e seus hábitos (LOUISE, 2018). Atualmente existem tecnologias que possibilitam a fácil captação de dados, além disso, ferramentas que possibilitam realizar esse feito, principalmente se tratando de fontes como os dados pessoais.

## 2.2 Privacidade em *IoT*

Privacidade e segurança são dois conceitos de fundamental importância ao se referir ao contexto de Internet das Coisas. São conceitos distintos, entretanto, muitas das vezes utilizados e interpretados como sinônimos, de forma errônea. Os dois conceitos podem possuir dependência ao se tratar do contexto e esfera da segurança da informação. Porém quando se remete a palavra segurança, nesse contexto, refere-se a elementos como a confidencialidade, integridade e disponibilidade. Enquanto a privacidade está correlacionada de forma relativa à intimidade do usuário/pessoa.

No contexto da Internet e Tecnologias da Informação e Comunicação (TICs), o conceito de privacidade está relacionado ao controle sobre a coleção de dados pessoais existentes e quem possui acesso a esse conjunto de informações. “Privacidade é a capacidade de um indivíduo ou grupo de manter sua intimidade não divulgada” (MARQUES 2011). Na esfera jurídica existem preocupações por parte dos legisladores a respeito da privacidade e proteção dos dados e informações pessoais, onde existem medidas técnicas e administrativas de segurança que podem ser adotadas para proteger dados pessoais.

Pode-se mencionar a lei 13709/2018 mais conhecida como LGPD (Lei Geral de Proteção de Dados) que descreve em seu artigo 1º a disposição sobre o tratamento dos dados pessoais, inclusive nos meios digitais e possui o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL 2018).

A privacidade nesta lei aparece em seu Art. 2º, inciso I, apresentando-a como um dos fundamentos da proteção de dados pessoais. A Lei também traz a definição de alguns conceitos importantes, apresentados na **Tabela 1.**

**Tabela 1.** Definições sobre dados de acordo com a lei 13709/2018 LGPD Artigo 5º

| **Conceito** | **Descrição** |
|---|---|
| Dado pessoal | Informação relacionada a pessoa natural identificada ou identificável. |
| Dado pessoal sensível | Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. |
| 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. |

**Fonte: Lei 13709/18 Artigo 5º**

No Artigo 11 da referida é mencionado a respeito do tratamento de dados pessoais sensíveis, somente poderão ocorrer nas seguintes hipóteses:

I - Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

e) proteção da vida ou da incolumidade física do titular ou de terceiros;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Na literatura foram colhidos alguns estudos relacionados a privacidade dos dados pessoais no contexto da internet das coisas, como por exemplo, o autor Rosner 2016 expõe em seu livro "*Privacy and the Internet of Things*" alguns riscos à privacidade considerando o contexto de Internet das Coisas:

(a) monitoramento intenso;

(b) coleta de dados não consentida;

(c) coleta de informações médicas;

(d) quebras de contexto da informação.

Vale a pena ressaltar alguns pontos relacionados a esses riscos. Como por exemplo, relacionado ao risco do monitoramento intenso está o direito de privacidade no âmbito do direito de estar sozinho. Quanto ao risco coleta de dados não consentida pode-se discutir também a questão dos dados de crianças e adolescentes, o que aumenta o grau de severidade deste ponto.

Referente ao risco coleta de informações médicas, o cenário de aplicação e sensores de baixo custo (um relógio ou celular) que capturam dados relacionados à saúde da pessoa, juntamente com a aplicação de técnicas de mineração de dados geram informações confiáveis sobre a saúde do indivíduo. Com isso, os consumidores enfrentam diversos riscos e uma situação de vulnerabilidade a constrangimentos e danos à reputação e à discriminação. A seguir a **Tabela 2** apresenta a definição dos riscos mencionados pelo autor.

**Tabela 2.** Riscos a privacidade em *IoT*

| **Conceito** | **Descrição** |
|---|---|
| Monitoramento intenso | Aplicação intensa do sensoriamento, dispositivos conectados para monitoramento da atividade humana. Rastreamento de todos os movimentos das pessoas. |
| Coleta de dados não consentida | Dados de qualquer natureza são coletados, deve haver autorização do titular dos dados, utilização para fins comerciais. |
| Coleta de informações médicas | Informações médicas são dados sensíveis que, se divulgadas, colocam os consumidores em posição de vulnerabilidade à constrangimento e danos. |
| Quebra de contextos da informação | Risco gerado pela “fusão de sensores”. Dados de diferentes contextos são reunidos e geram novas informações acerca do indivíduo. Desrespeito do limite das informações de cada contexto é uma violação à privacidade. |

**Fonte: Rosner 2016**

Figueira 2016 menciona que existem várias formas de privacidade que propõem uma taxonomia. Essa taxonomia de privacidade representa uma perspectiva das atividades que podem conduzir a sua violação. São elas:

- Coleta de informação que envolve atividades de violação de privacidade no momento da coleta de dados sobre um indivíduo. Cobranças forçadas ou interrogatórias podem levar a uma violação de privacidade, mesmo que esses dados tenham sido coletados com o consentimento do indivíduo;
- O processamento da informação que envolve atividades prejudiciais à privacidade a partir do processo de armazenamento, manipulação e utilização dos dados sobre indivíduos;
- A disseminação da informação que envolve atividades de divulgação, exposição e disseminação de informações sobre indivíduos. Quando realizadas pode incorrer no extrapolar a confidencialidade;
- Por último as atividades de invasão à privacidade de indivíduos. Pode ocorrer através de acesso intrusivo e interferências decisórias.

(Cesar 2015) reforça a ideia anterior, em seu estudo baseado em Solove (2006) onde menciona que existem várias formas de privacidade, propondo uma taxonomia de privacidade com uma visão geral das atividades que possam levar a sua violação, sendo elas:

- A coleta de informações, que embora a informação geralmente seja recolhida com o consentimento do proprietário da informação, cobranças forçadas ou interrogatórios podem levar a violação da privacidade da pessoa;
- A disseminação da informação, quando realizada pode extrapolar a confidencialidade, podendo tal situação ser gerada de múltiplas formas;
- A divulgação pode acontecer com a publicação de fatos verídicos, no entanto, tais fatos podem afetar a reputação da pessoa, por meio da exposição de dados e informações privados que possam vir a serem vinculados;
- E a invasão que pode ocorrer nos dados pessoais por meio do acesso intrusivo em sua pessoalidade e através da interferência decisória.

## 2.3 Segurança em *IoT*

A informação deve ser protegida nos ambientes de sistemas de informação, pois ela gera conhecimentos que podem ser alvo de ataques a privacidades e os dados dos usuários. A Segurança da informação baseia-se em proteger ativos (informação e sistemas de informação) de acesso, uso, divulgação, perturbação, modificação ou destruição indevidos ou não autorizados (SATTAROVA; KIM 2007).

Atualmente, a área de segurança da informação é de extrema relevância devido ao grande número de informações sigilosas trafegadas em redes de comunicação (GOMES 2020). Essa área é constituída em três pilares: confidencialidade, integridade e disponibilidade dos recursos de uma rede. Esses pilares da segurança são considerados requisitos fundamentais para o desenvolvimento de novas tecnologias, especialmente nas aplicações de Internet das Coisas (RAJ; RAMAN, 2017) com descrição detalhada na **Tabela 3**.

**Tabela 3**. Pilares da segurança da informação**.**

| Pilar | Descrição |
|---|---|
| Confidencialidade | Garantir que a informação seja acessada apenas por pessoas autorizadas; |
| Integridade | Garantir que a informação seja original e verdadeira, não tendo sido modificada; |
| Disponibilidade | Garantir que as pessoas autorizadas tenham acesso aos dados e recursos sempre que desejado. |

**Fonte: GOMES 2020**

(SILVA, 2017) menciona que devido a magnitude das redes de comunicação, em conjunto com a diversidade de ataques disponíveis, o estabelecimento e manutenção da segurança em redes vem se tornando cada vez mais complexos. (OLIVEIRA NETO, 2015) complementa que em relação a *IOT*, é fundamental que

esses dispositivos possam receber constantes atualizações de segurança com o objetivo de sobrepor possíveis vulnerabilidades em seus sistemas.

### 2.3.1 Riscos e ameaças à Segurança

Os ataques a segurança do ecossistema inteligente são realizados através de *malwares* que podem ser definidos como códigos maliciosos desenvolvidos para infectar computadores ou dispositivos. Quando instalado, esse tipo de *software* possui a capacidade de executar ações prejudiciais em seu hospedeiro, além de adquirir acesso aos dados armazenados.

Segundo o Relatório Global de Riscos do Fórum Econômico Mundial de 2020 (WEF, 2020), os ataques cibernéticos são um dos dez maiores riscos levantados para a próxima década, com impacto profundo em diversas esferas. Ataques cibernéticos em larga escala são vistos como riscos à quebra de redes e infraestruturas de comunicação em escala mundial. (Figueira 2016) menciona que a *IoT* ainda está muito longe de estar segura o suficiente contra os problemas de segurança e ataques da internet atual, muito em parte, devido a particularidades desta tecnologia, tais como:

- Comunicações em *IoT* podem ser realizadas através de redes sem fio: qualquer indivíduo com mais intenções pode ouvir essas transmissões e se comunicar usando esse mesmo meio;
- É possível acessar os dispositivos fisicamente: os dispositivos IoT podem ser colocados em locais públicos onde estão ao alcance de qualquer indivíduo;
- Muitos dispositivos contam com recursos limitados: a limitação de recursos insere medidas de segurança bem restritas nesses dispositivos.

(Kalita e Kar et al, 2009) enumeraram e apresentaram uma descrição sobre alguns possíveis ataques que as redes sem fio (*WSNs*) estão sujeitas e que são transponíveis à *IoT*, entre esses possíveis ataques estão:

- Ataques de Negação de Serviço (*DoS*): impedimento ou restrição do uso normal da rede ou administração de dispositivos de rede ou rede sem fio;
- Ataques *Sybil*: dispositivos maliciosos ilegitimamente que tomam inúmeras identidades.

- Análise de Tráfego: monitoramento das transmissões vias redes sem fio para o propósito de identificar padrões de comunicação e participantes;
- Espionagem: um atacante mal-intencionado monitora de forma passiva redes sem fio para coletar dados, incluindo credencias de autenticação.

No estudo de (Rovere 2022) ele cita que a coleta de informação dos sistemas e pessoas que fazem uso dele e, em um mundo em que o conhecimento das preferências de uma pessoa valem cada vez mais, ataques para obtenção destas informações são cada vez mais comuns, sendo estes ataques conhecidos como data-leakage. O intuito deste ataque é obter dados confidenciais a partir de dispositivos individuais e pessoais durante o tráfego dessas informações para que posteriormente sejam divulgados para organizações não autorizadas (RIBEIRO, 2020).

Outra ameaça muito comum e que não se restringe apenas aos dispositivos e ecossistemas de *IoT* é a cópia ou substituição do dispositivo, afirma (Ribeiro 2020). Neste tipo de ataque, fábricas não confiáveis copiam características físicas, software e configurações de segurança dos dispositivos originais, de forma que os dispositivos copiados sejam vendidos mais baratos no mercado, podendo conter modificações funcionais, incluindo *backdoors*, que são formas de obter acesso ao sistema do dispositivo sem conhecimento do proprietário *DDoS*.

### 2.3.2 Ataque de Negação de Serviço Distribuído

Um ataque de *DDoS* (*Distributed Denial of Service*) consiste na tentativa de saturar uma rede, um hospedeiro ou um componente de infraestrutura de rede, bloqueando o acesso dos usuários legítimos. Conforme DOULIGERIS 2004:

> [...] ataques DoS (Denial of Service - acrônimo em inglês para Negação de Serviço) hoje são uma das maiores ameaças de segurança presentes na Internet, especificamente ataques DDoS (acrônimo em inglês para Ataque Distribuído de Negação de Serviço), em que o impacto é de maior escala e com maiores danos ao alvo, principalmente por eles ocorrerem sem nenhum tipo de sinal ou aviso, em que no momento que o ataque é iniciado, as capacidades computacionais do alvo acabam comprometidas ou até mesmo são anuladas muito rapidamente. (DOULIGERIS 2004)

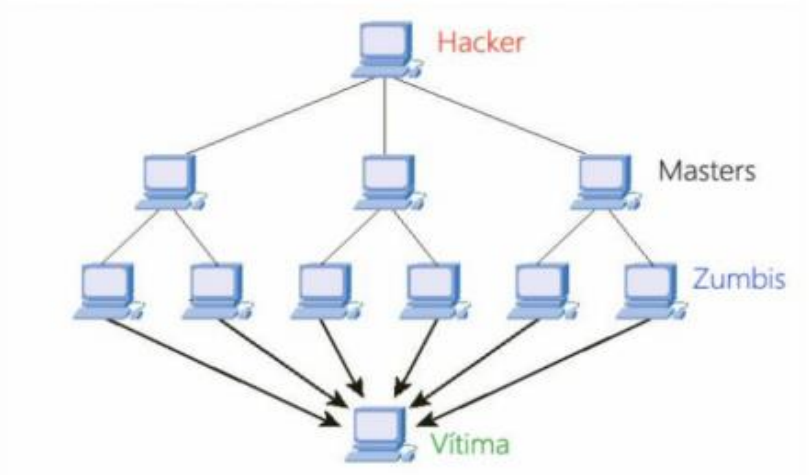
(Souza, 2019) complementa que existe preocupações a respeito deste ataque quando inferido em dispositivos *IoT* , pois com bilhões de dispositivos alvos esses dispositivos sequestrados podem ser usados para realizar ataques distribuídos,

objetivando por meio deste ataques interromper a funcionalidade de serviços de servidores em qualquer lugar do mundo. Esse tipo de ataque fere diretamente o princípio da disponibilidade na segurança da informação e pode ser potencialmente ampliado com a eminente disseminação da *IoT* (RAJ; RAMAN, 2017).

A arquitetura de um ataque *DDoS* geralmente constitui-se de um único atacante e um único alvo. “Porém, o fluxo de ataque é composto por máquinas intermediárias, que podem também ser consideradas vítimas secundárias do ataque”. (SILVA 2020) Sendo assim, a estrutura do ataque disponibiliza quatro principais componentes, ilustrados na Figura 2.

- Atacante: O coordenador de todo o ataque.
- Mestres: Máquinas que recebem do atacante os parâmetros de ataque e comandam os agentes.
- Agentes ou “*Zumbis*”: Máquinas que enviam diretamente as requisições para a vítima e concretizam o ataque *DDoS*.
- Vítima: Máquina que é alvo do fluxo massivo de pacote.

**Figura 2**. Componentes do ataque *DDoS*




**Fonte: Silva 2017**

Pode-se verificar os ataques do tipo *DDoS* em infraestruturas de *IoT*. Este tipo de ataque atingiu a Dyn, uma empresa com controle de significante parte da infraestrutura de *DNS* nos Estados Unidos e conforme a empresa de segurança Kaspersky 2019:

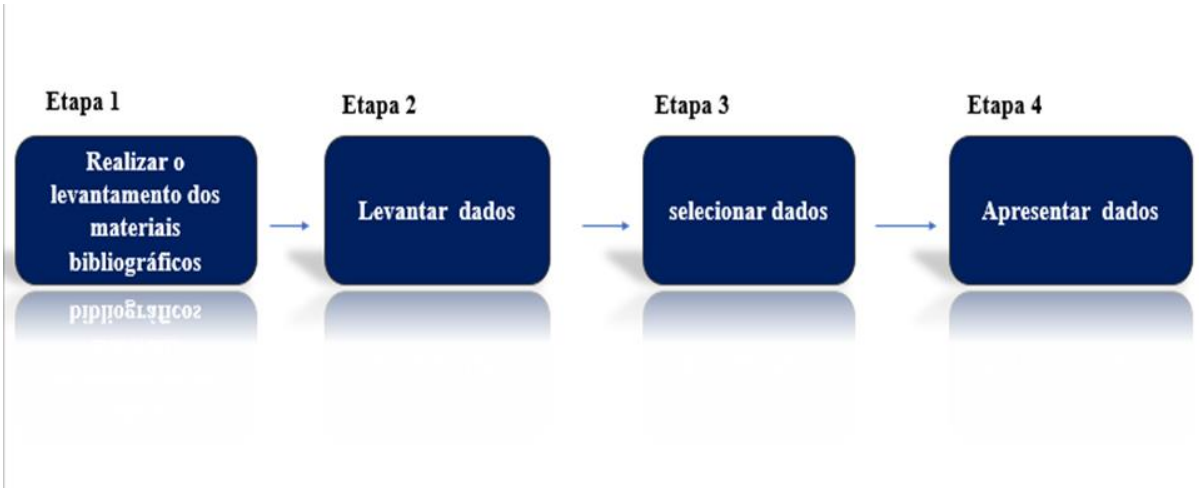
> Recentemente, fomos confrontados com uma nova versão do Mirai (botnet de propagação própria que tem como alvo dispositivos IoT e foi responsável por um ataque DDoS massivo em servidores Dyn em 2016). Segundo os analistas, a botnet está equipada com Mais exploits, o que a torna ainda mais perigosa e permite que se expanda mais rapidamente. O mais preocupante é que esta nova versão não só atende às suas vítimas habituais (roteadores, câmeras IP e outras coisas inteligentes), mas agora também vai contra dispositivos IoT das empresas. (KASPERSKY 2019, p.1)

O ataque ultrapassou a ordem de *terabytes* por segundo e foi o maior ataque de negação de serviço já registrado até hoje (Silva 2017). As redes de *bots* podem ser usadas para executar ataques do tipo *DDoS*. *Mirai Botnet* é uma ameaça de *malware* que consiste em uma enorme quantidade de dispositivos comprometidos que podem ser usados em coordenação para realizar ataques de *malware.*

## 3 METODOLOGIA

Para elaboração desta revisão foram elencadas algumas etapas referentes às fases de desenvolvimento que compõe a pesquisa, serão apresentadas na Figura 3 e detalhadas logo abaixo:

**Figura 3:** Esquema de procedimentos metodológicos.




**Fonte: Autor próprio**

Na etapa 1 foi realizado o levantamento dos materiais bibliográficos para melhor embasamento teórico, assim como absorção de conhecimento através pesquisas serviram de base para a realização da revisão. O levantamento dos materiais bibliográficos foi realizado nas seguintes bases: Google Acadêmico e Scielo, pelo fato de serem reconhecidas no meio acadêmico científico. Foi utilizado como parâmetro de pesquisa as seguintes palavras chaves relacionadas ao tema de pesquisa: “privacidade”, “segurança”, “Internet das Coisas”.

Referente a etapa 2 foi realizado o levantamento dos dados onde foi utilizado o procedimento de pesquisa bibliográfica, e segundo MARCONI 2003:

> A pesquisa bibliográfica é um apanhado geral sobre os principais trabalhos já realizados, revestidos de importância, por serem capazes de fornecer dados atuais e relevantes relacionados com o tema. O estudo da literatura pertinente pode ajudar a planificação do trabalho, evitar publicações e certos erros, e representa uma fonte indispensável de informações, podendo até orientar as indagações. (MARCONI 2003, pg. 158).

Baseando-se no procedimento de pesquisa bibliográfico descrito pela autora, espera-se obter mais relevância no trabalho realizado. Diante disso, a classificação da pesquisa é exploratória onde se possui como objetivo proporcionar maior familiaridade

com o problema, com vistas a torná-lo mais explícito, conforme apontado por Gil (2002, p.41). O levantamento dos dados ocorreu entre o período de 05 de junho de 2022 a 02 de novembro de 2022, onde foi selecionado e feita a utilização de artigos, monografias, dissertações e livros a respeito do assunto, também foi utilizada a Lei 13709 que serviu de base para absorção de conteúdos jurídicos sobre o tema.

A etapa 3 foi constituída pela coleta e seleção dos dados. Quanto à forma de análise dos dados da pesquisa, foi adotada uma avaliação qualitativa na qual utilizando-se das informações apresentadas pelas fontes bibliográficas, serão extraídas as informações que serão de extrema relevância para concretização da pesquisa.

Foram realizadas análises dos títulos e resumos das literaturas selecionadas. Aqui também foi adotada a realização da leitura integral dos materiais, e excluídos aqueles que não possuíam informações que poderiam ser utilizadas na pesquisa. Mediante a isto foi criado um documento utilizando o programa de formatação e edição de texto Word, o documento foi constituído por tabelas que continham informações referentes as literaturas que foram selecionadas para utilização na pesquisa.

Referente a etapa 4, é a etapa de apresentação da pesquisa, onde serão apresentadas as informações, e selecionadas mediante metodologia adotada, e serão apresentados os resultados e as discussões relativas ao tema de pesquisa.

## 4 RESULTADOS E DISCUSSÕES

Baseado na literatura e nas análises realizadas através de estudos sobre o tema, estima-se como objetivo, neste tópico, realizar a apresentação dos resultados obtidos. Dessa forma, uma das ideias que resultou na motivação para a execução dessa pesquisa foi a de estudar, investigar informações sobre a privacidade e a segurança da informação no ambiente de Internet das Coisas.

Esse estudo se mostrou necessário devido ao eminente estabelecimento do paradigma da Internet das Coisas. Além disso, com esse estudo pretende-se realizar contribuições através do levantamento de informações concretas e estudos literários sobre o tema mencionado, que são relacionados ao ecossistema inteligente. Mediante a metodologia adotada para o levantamento das fontes bibliográficas, nesta seção foi elaborado uma tabela que contém informações referentes às principais fontes bibliográficas que serviram de embasamento para o estudo do tema proposto. estas informações estão apresentadas na **tabela 4**:

**Tabela 4:** Bibliografias consultadas.

| **Bibliografias Consultadas** | | | |
|---|---|---|---|
| **Titulo** | **Autor(es)** | **Ano de Publicação** | **Material** |
| Privacy and the Internet of Things. | ROSNER, Gilad | 2016 | Artigo |
| Internet das coisas: um estudo sobre questões de segurança, privacidade e infraestrutura | FIGUEIRA, Vitor Pinheiro | 2016 | Monografia |
| O Desafio da Privacidade na Internet das Coisas | Carlos Cesar e Jefferson David de Araújo Sales | 2015 | Artigo |
| Estudo Sobre Segurança E Privacidade Na Internet Das Coisas (Iot) | Lucas Della Rovere, Fabiana Florian | 2022 | Artigo |
| Lei 13709/2018 Lei Geral de Proteção de Dados (LGPD) | Brasil | 2018 | Lei |
| Síntese de requisitos de segurança para internet das | OLIVEIRA NETO, I. R | 2015 | Dissertação |

| | | | |
|---|---|---|---|
| coisas baseada em modelos em tempo de execução | | | |
| Uma revisão sistemática sobre a Segurança nos Protocolos de Comunicação para Internet das Coisas | MORENO, Edward | 2018 | Artigo |
| Segurança em IoT | CARVALHO, André. | 2021 | Artigo |

**Fonte:** Autor (2023)

Na literatura foram encontrados alguns riscos existentes a respeito da privacidade em *IoT.* (Rosner, 2016) menciona alguns riscos relacionados a privacidade dos dados pessoais no contexto da internet das coisas, são exemplos destes riscos a coleta de dados não consentida, coletas de informações médicas, monitoramento e rastreamento das atividades humanas através de dispositivos e sensores no ambiente de *IoT*. Outros autores como por exemplo (Figueira, 2016) menciona uma taxonomia no contexto da privacidade, onde cobranças forçadas ou interrogatórias podem levar a uma violação de privacidade, mesmo que esses dados tenham sido coletados com o consentimento do indivíduo.

(Cesar 2015) em seu trabalho sobre o desafio da privacidade em *IoT* baseado em Solove (2006) menciona uma taxonomia em que a divulgação pode acontecer com a publicação de fatos verídicos, no entanto, tais fatos podem afetar a reputação da pessoa, por meio da exposição de dados e informações privados. (FIGUEIRA 2016) complementa esta ideia de riscos a privacidade, mencionando em sua bibliografia a ideia de desafio a privacidade nos espaços públicos. E segundo esta pesquisa:

> A IoT pode ameaçar as pretensões de privacidade que um indivíduo tem em situações comuns. Entretanto, existem normas sociais e expectativas de privacidade que se diferenciam em espaços públicos e privados. Entretanto, os dispositivos IoT desafiam essas normas e expectativas. Por exemplo, expectativas de privacidade de um indivíduo em espaços considerados públicos, estão sendo desafiados pelo aumento do monitoramento nesses espaços. (FIGUEIRA 2016, m pg. 52)

A grande maioria dos dispositivos *IoT* podem ser encontrados em muitos lugares e tem uma familiaridade e um envolvimento social com o ambiente (Figueira, 2016). Os autores Cordeiro e Beiguelman, 2015 apontam para o “efeito *big brother*”

das *IoT* no espaço urbano, um problema de liberdade pessoal que torna a vida íntima em um dado público.

No ordenamento jurídico existe a Lei 13709/2018 (LGPD) que define medidas administrativas para a proteção da privacidade e dos dados pessoais inclusive quando se trata dos meios digitais. Nesta Lei existem medidas como por exemplo o artigo 11 onde é mencionado o tratamento dos dados pessoais sensíveis. O tratamento desses dados só é permitido mediante a própria concessão do titular. Entretanto, nesse mesmo artigo é destacada algumas hipóteses onde os dados pessoais sensíveis podem ser manipulados sem fornecimento ou consentimento do titular, esses exemplos foram citados na seção 2 de referencial teórico.

Estas exceções se aplicam em alguns cenários de *IoT* como por exemplo na área da saúde onde profissionais ou autoridades desta área possuem exclusivamente a tutela da saúde, existindo a possibilidade de profissionais desta área realizarem o monitoramento remoto do estado de saúde de um paciente através de aplicações de *IoT.* Outra exceção que pode ser mencionada é enfatizada referente a não dependência do consentimento do titular para tratamento e coleta dos dados pessoais nos meios digitais que também engloba *IoT,* são a respeito das hipóteses de interesse de execução da administração pública, do exercício regular de direitos e a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis (Brasil 2018).

No contexto da segurança no ecossistema inteligente, (Figueira, 2016) menciona claramente que a *IoT* ainda não está suficientemente segura devido às suas particularidades. Rovere complementa esta ideia onde foi mencionado a seguinte evidencia em seus estudos:

> Foi possível ainda evidenciar que um dos grandes empecilhos ligados a segurança em *IoT* está associado aos próprios dispositivos, isso porque grande parte deles possuem limitações de hardware, como memória, largura de banda, energia e capacidade de processamento, impossibilitando que os mecanismos de segurança utilizados em outros sistemas e equipamentos sejam aplicados a eles, tornando assim estes dispositivos ainda mais seguros. (ROVERE 2016, pg. 9)

Neste contexto, essas limitações de recursos dos dispositivos na maioria das vezes existem por conta dos requisitos da aplicação de *IoT,* às vezes são dispositivos

que precisam ser flexíveis como por exemplo em relação a tamanho e a movimentação, interdependência, exemplo disso são dispositivos pequenos que sua fonte de alimentação se dá através de baterias, que logicamente não são conectados a tomada.

Existe a necessidade da proteção de dados e informações que são geradas pelos dispositivos na Internet das Coisas. (Oliveira, 2015) menciona que em relação a segurança em *IoT*, é fundamental que os dispositivos possam receber constantes atualizações de segurança com o objetivo de sobrepor possíveis vulnerabilidades em seus sistemas. E segundo Moreno 2018:

> Os principais problemas de segurança em *IoT,* que estão relacionados com questões relativas à privacidade, devem ser orquestrados a partir da estipulação de padrões, ou seja, protocolos que permitam a implementação de soluções para estes problemas. (MORENO 2018)

Por fim complementando esta ideia, (Carvalho 2021) diz sobre a adoção de protocolos de segurança mais rígidos, que é um dos principais métodos contra ataques e invasões gerais, que pode ser uma das soluções para proteger dispositivos e equipamentos na *IoT*.

# 5 CONCLUSÃO

A *IoT*, como observado neste trabalho, abre portas para diversas áreas e possibilidades de negócios. Nesta revisão foram abordados aspectos pertinentes a questões relacionadas com a privacidade e a segurança dos dados pessoais. Pois quando são considerados inúmeros objetos, dispositivos e aparelhos conectados à internet existe uma preocupação com estas questões abordadas. Neste contexto quando é pensado em privacidade e segurança, estas questões estão intimamente ligadas a vida intima das pessoas ou usuários.

Foi possível observar nesta pesquisa a existência de riscos e ameaças referentes a privacidade dos dados pessoais, assim também como questões sobre a segurança no ecossistema inteligente*,* como por exemplo, ataques e falta de mecanismos de segurança. Embora exista preocupações por parte do ordenamento jurídico e legislação, sobre a privacidade dos dados pessoais, ainda existem desafios que se remetem a este contexto, isto foi observado através dos resultados obtidos, sendo estas informações validadas através de estudos e revisões de literatura.

Observa-se a importância da preocupação com a segurança e manutenção de dispositivos, e aparelhos conectados à *internet*. Mesmo que a *IoT* ainda não se encontra totalmente segura devido suas particularidades, existem medidas que podem contribuir com a preservação dos dados pessoais e até mesmo tentativas de ataques. Conclui-se que a relação da segurança nesse ambiente é de extrema necessidade. De acordo com a literatura existe a necessidade de adequação de protocolos e mecanismos de segurança aos dispositivos conectados à rede, com a finalidade de administrar os problemas de privacidade, como por exemplo a adoção de alguns mecanismos como a criptografia e instalação de *firewalls* para varredura contra vírus, e protocolos mais seguros.

Tendenciando novas contribuições para trabalhos futuros, esta revisão deixa espaço para que se possa realizar pesquisas sobre o assunto abordado, que é pertinente no momento atual da sociedade. Sugere-se a realização de estudos que contribuam para geração de informações importantes como por exemplo, realização de análises de protocolos ou *software* que estão presentes no mercado relacionados segurança dos dados e informações no ambiente de *IoT*.

## 6 REFERÊNCIAS


LOUISE, Marie. **Segurança e privacidade para a Internet das Coisas.** Rio de Janeiro: Instituto Igarapé. 2018. 11 p. Disponível em : <https://igarape.org.br/wp-content/uploads/2018/11/Seguranc%CC%A7a-e-Privacidade-para-a-Internet-das-Coisas.pdf> Acesso em : 15 de junho de 2022

SOUZA, Jovani. **Segurança e privacidade na internet das coisas.** Estudo de caso com a Kaa IoT plataforma. Chapecó, SC: Universidade Federal da Fronteira Sul, curso de Ciência da Computação. 2019. 10 p. Disponível em: <https://rd.uffs.edu.br/bitstream/prefix/3369/1/SOUZA.pdf>

ROTHER, Edna Terezinha. **Revisão sistemática X revisão narrativa**. Acta paulista de enfermagem, v. 20, n. 2, p. v-vi, 2007.

CORDEIRO, Alexander Magno et al. **Systematic review: a narrative review**. Revista do colégio Brasileiro de Cirurgiões, v. 34, n. 6, p. 428-431, 2007.

SANTOS, B. P.; SILVA, L. A. M.; CELES, C. S. F. S.; BORGES, J. B; PERES. B. S.; VIEIRA, M. A. M.; VIEIRA, L. F. M.; GOUSSEVSKAIA, O. N.; LOUREIRO, A. A. F. **Internet das Coisas**: da Teoria à Prática, Belo Horizonte: UFMG, 2016. Disponível em: <https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/internet-das-coisas.pdf.> Acesso em :12 de Outubro de 2022.

Atzori, L.; Iera, A.; Morabito, G. —**The internet of things: A surveyl**. Computer Networks, v. 54, no. 15, pp. 2787-2805, 2010.

SILVA, Leandro Jamir. **Monografia deTrabalho de Conclusão de Curso.Internet Das Coisas**. Universidade do Sul de Santa Catarina[UNISUL]. Disponível em: <https://riuni.unisul.br/handle/12345/3940>. Acesso: Outubro 2022.

Batty M., Axhausen K. W., Giannotti F., Pozdnoukhov A., Bazzani A., Wachowicz M., Ouzounis G., & Portugali Y. (2012). **Smart cities of the future**. European Physical Journal: Special Topics, 214(1), 481-518. doi: 10.1140/epjst/e2012-01703-3.~

De JESUS, Klebio. **Aplicação de internet das coisas (iot) na agricultura de precisão.** Unidade Universitária de Posse (unu Posse). Posse-Go 2021. Disponível em: <http://aprender.posse.ueg.br:8081/jspui/handle/123456789/274> Acesso: Novembro 2022

CRISTINA, Silze. **O uso da internet das coisas (iot) a favor da saúde.** Faculdade de Tecnologia de Taquaritinga (FATEC) –SP –Brasil- 2018. Disponível em: < https://revista.fatectq.edu.br/interfacetecnologica/article/view/515/304> Acesso: Fevereiro 2023

MIGUEL, Pedro. **Internet das coisas: O desafio da privacidade.** Estudo de caso. Setúbal 2016. Instituto Politécnico de Setúbal. Disponível em: < https://core.ac.uk/download/75985137.pdf> Acesso: janeiro 2023

INTERNATIONAL BUSINESS MACHINES. **Cities – Rio de Janeiro 2011**. Rio de Janeiro: International Business Machines, 2011. Disponível em: <http://www.ibm.com/smarterplanet/us/en/smarter_cities/article/rio.html/>. Acesso: Novembro 2022

MAGRANI, Eduardo. **A Internet das Coisas**. 1º edição, Rio de Janeiro : FGV Editora, 2018.

LOUISE, Marie. **Segurança e privacidade para a Internet das Coisas.** Rio de Janeiro: Instituto Igarapé. 2018. 11 p. Disponível em : <https://igarape.org.br/wp-content/uploads/2018/11/Seguranc%CC%A7a-e-Privacidade-para-a-Internet-das-Coisas.pdf> Acesso em : 15 de junho de 2022

MARQUES, Rodrigo. **Segurança, Privacidade, Questões Éticas em Sistemas de Informação e seus Impactos Sociais.** Ribeirão Preto, 2011. 1 p. Disponível em: <http://marcos.bocca.adm.br/academic/2011/semar/sistema_de_informacao/aula15_Seguran%E7a2.pdf> Acesso em : 20 de julho de 2022

BRASIL. **Lei n. 13.709/2018, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm > Acesso em: 22 jun. 2022.

ROSNER, G. **Privacy and the Internet of Things**. O'Reilly Media, Incorporated, 2016.

GOMES, Sarah. **Segurança, privacidade e blockchain no contexto de internet das coisas.** 2020, Curitiba. Disponível em: <https://repositorio.utfpr.edu.br/jspui/bitstream/1/19677/1/CT_CEIOT_II_2019_10.pdf > Acesso: 06 de junho 2022

FIGUEIRA, Vitor Pinheiro. **“Internet das coisas” : um estudo sobre questões de segurança, privacidade e infraestrutura** . 2016. – Niterói, RJ Disponível em: <https://app.uff.br/riuff/bitstream/handle/1/5150/TCC_VITOR_PINHEIRO_FIGUEIRA_FINAL%20%281%29.pdf?sequence=1&isAllowed=y> Acesso: 26 outubro de 2022

CESAR, Carlos. **O Desafio da Privacidade na Internet das Coisas**. The challenge of privacy on the Internet of things. Revista Gestão.Org, v. 13, Edição Especial, 2015. p. 282-290 ISSN 1679-1827. Disponivel em : <https://periodicos.ufpe.br/revistas/gestaoorg/article/view/22115/18481> Acesso: 29 Outubro 2022.

SATTAROVA F. Y.; KIM, T. H. IT. **security review: Privacy, protection, access control, assurance and system security.** International journal of multimedia and ubiquitous engineering**,** v. 2, n. 2, 2007. 61 p.

_____, Sarah. **Segurança, privacidade e blockchain no contexto de internet das coisas.** 2020, Curitiba. Disponível em: <https://repositorio.utfpr.edu.br/jspui/bitstream/1/19677/1/CT_CEIOT_II_2019_10.pdf > Acesso: 06 de junho 2022

RAJ, P.; RAMAN, A. C. The Internet of Things: Enabling Technologies, Platforms, and Use Cases. Boca Ratón: CRC Press, 2017. Disponível em: <https://books.google.com.br/ books?id=cLI0DgAAQBAJ> Acesso: 26 Outubro de 2022

SILVA, Alessandra . **Estudo sobre vulnerabilidades em dispositivos iot no contexto de ataques com o uso de botnets.** Brasilia , 2017 . Disponível em <https://bdm.unb.br/bitstream/10483/27800/1/2017_AlessandraDeMeloSilva_tcc.pdf> Acesso :11 de Julho 2022.

OLIVEIRA NETO, I. R. **Síntese de requisitos de segurança para internet das coisas baseada em modelos em tempo de execução**. 2015. Diss. (Mestrado) – Goiânia. Disponível em: <http://repositorio.bc.ufg.br/tede/handle/tede/5185> Acesso em: 26 Outubro 2022.

WEF (World Economic Forum). **The global risks report 2020**. Copyright© 2020 World Economic Forum. Disponível em:< https://www.weforum.org/reports/the-global-risks-report-2020> . Acesso em: 02 de agosto de 2022.

ROVERE, Lucas. **Estudo sobre segurança e privacidade na internet das coisas (iot).** RECIMA21 - Revista científica multidisciplinar ISSN 2675-6218. 2022. Disponível em: < <https://recima21.com.br/index.php/recima21/article/view/1601/1231> Acesso: 26 Outubro 2022

_____, Vitor Pinheiro. **“Internet das coisas” : um estudo sobre questões de segurança, privacidade e infraestrutura** . 2016. – Niterói, RJ Disponível em: <https://app.uff.br/riuff/bitstream/handle/1/5150/TCC_VITOR_PINHEIRO_FIGUEIRA_FINAL%20%281%29.pdf?sequence=1&isAllowed=y> Acesso: 26 outubro de 2022

RIBEIRO, A. J. J. Problemas de Segurança na Internet das Coisas. 2020. 132 f. Dissertação (Mestrado em Cibersegurança e Informática Forense) – Escola Superior de Tecnologia e Gestão, Leiria, 2020.

Kalita, Hemanta Kumar and Kar, Avijit. **Wireless Sensor Network Security Analysis (2009)**. International Journal of Next-Generation Networks (IJNGN),Vol.1,

No.1, December 2009 , Available at SSRN: https://ssrn.com/abstract=3878728. Download This Paper. Open PDF in Browser.

DOULIGERIS, Christos. **DDoS attacks and defense mechanisms**: classification and state-of-the-art. Computer Networks, v. 44, n . 643-666, 2004. 5, p.

SOUZA, Jovani. **Segurança e privacidade na internet das coisas.** Estudo de caso com a Kaa IoT plataforma. Chapecó, SC: Universidade Federal da Fronteira Sul, curso de Ciência da Computação. 2019. 10 p. Disponível em:<https://rd.uffs.edu.br/bitstream/prefix/3369/1/SOUZA.pdf>

RAJ, P.; RAMAN, A. C. The Internet of Things: Enabling Technologies, Platforms, and Use Cases. Boca Ratón: CRC Press, 2017. Disponível em: <https://books.google.com.br/ books?id=cLI0DgAAQBAJ>

KASPERSKY. **Empresas são novo foco da botnet Mirai**. Disponível em< https://www.kaspersky.com.br/blog/mirai-enterprise/11616/> Acesso em : 11 de Agosto 2022.

_____, Alessandra . **Estudo sobre vulnerabilidades em dispositivos iot no contexto de ataques com o uso de botnets.** Brasilia , 2017 . Disponivel em <https://bdm.unb.br/bitstream/10483/27800/1/2017_AlessandraDeMeloSilva_tcc.pdf> Acesso :11 de Julho 2022 .

VILAS BOAS, T. de J. R.; KALHIL, J. B.; COELHO FILHO, M. de S.; COSTA, R. D. da S. **O estado da arte de metodologias da produção científica sobre a formação do professor do ensino de ciências com enfoque cts**. REAMEC - Rede Amazônica de Educação em Ciências e Matemática, *[S. l.]*, v. 6, n. 1, p. 65-86, 2018. DOI: 10.26571/REAMEC.a2018.v6.n1.p65-86.i5958. Disponível em: <https://periodicoscientificos.ufmt.br/ojs/index.php/reamec/article/view/5958>. Acesso em: 31 out. 2022.

MORENO, Edward. **Uma revisão sistemática sobre a Segurança nos Protocolos de Comunicação para Internet das Coisas.** Universidade Federal de Sergipe. JADI –Brazil –v. 4 n. 1 – 2018 Disponível em: <https://revista.univem.edu.br/jadi/article/view/2482/749> Acesso: 01 de Novembro 2022

CARVALHO, André. **Segurança em IoT**. Centro Universitário do Planalto Central Apparecido dos Santos – UNICEPLAC: Brasília-DF 2021 Disponível em: < https://dspace.uniceplac.edu.br/bitstream/123456789/1610/1/Andr%C3%A9%20Ferreira%20Almeida%20de%20Carvalho_%20Christyan%20Matteus%20Lima%20Santos_Lucas%20Vaz%20Gon%C3%A7alves.pdf> Acesso : 01 Novembro de 2022.

GIL, Antonio Carlos. Métodos e Técnicas de Pesquisa Social. 6.ed. – São Paulo: Atlas, 2008.

CORDEIRO, A. V.; BEIGUELMAN, G.. Smart city and Internet of Things: Possible changes in the public space. In: **16th International Conference CAAD Futures 2015**, The next city – New technologies and the future of the built environment. São Paulo, pp. 90-98, 2015.