UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

MICHAEL PACHECO VORNES

SEGURANÇA EM INTERNET DAS COISAS: ESTUDO DE CASO NO SETOR INDUSTRIAL

GUARAPUAVA

2022

MICHAEL PACHECO VORNES

SEGURANÇA EM INTERNET DAS COISAS: ESTUDO DE CASO NO SETOR INDUSTRIAL

Internet of Things Security: Case Study in the Industrial Sector

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Tecnólogo em Tecnologia em Sistemas para Internet do Curso Superior de Tecnologia em Sistemas para Internet da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Hermano Pereira

GUARAPUAVA

2022

4.0 Internacional

Esta licença permite compartilhamento, remixe, adaptação e criação a partir do trabalho, mesmo para fins comerciais, desde que sejam atribuídos créditos ao(s) autor(es). Conteúdos elaborados por terceiros, citados e referenciados nesta obra não são cobertos pela licença.

MICHAEL PACHECO VORNES

SEGURANÇA EM INTERNET DAS COISAS: ESTUDO DE CASO NO SETOR INDUSTRIAL

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Tecnológo em Sistemas para Internet do Curso de Tecnologia em Sistemas para Internet da Universidade Tecnológica Federal do Paraná (UTFPR).

Data da aprovação: 30/junho/2022

Prof. Hermano Pereira
Doutor
Universidade Tecnológica Federal do Paraná - Campus Guarapuava

---

Prof. Luciano Ogiboski
Doutor
Universidade Tecnológica Federal do Paraná - Campus Guarapuava

---

Prof. Sediane Carmem Lunardi Hernandes
Doutora
Universidade Tecnológica Federal do Paraná - Campus Guarapuava

GUARAPUAVA
2022

Dedico este trabalho à minha família que sempre esteve ao meu lado e me apoiou em todos os momentos e decisões.

AGRADECIMENTOS

Agradeço à minha família por todo o apoio em todos os momentos e decisões difíceis, por nunca terem medido esforços para me proporcionar a melhor educação possível.

Aos professores da Universidade Tecnológica Federal do Paraná, principalmente aos professores do curso de Tecnologia em Sistemas para Internet, em especial ao meu orientador prof. Dr. Hermano Pereira e ao prof. Dr. Diego Marczal, pelo incentivo e apoio na realização deste trabalho.

RESUMO

O aumento de objetos inteligentes fez com que o campo denominado Internet das Coisas, também conhecido pela sigla IoT *(Internet of Things)*, recebesse muita atenção devido ao seu potencial de uso, proporcionando que objetos com diferentes recursos possam estar conectados, possibilitando o surgimento de novas aplicações. Assim, surgem também alguns desafios como as restrições desses objetos, limitações de sistema operacional e especificidade de protocolos de comunicação utilizados, impactando no aspecto de segurança. Por isso a importância de um tratamento adequado para a segurança de dispositivos de IoT, visto que, muitas vezes tais objetos não podem receber soluções de segurança convencionais. Porém, antes mesmo se pensar em um tratamento de segurança se faz necessário entender as características de tais dispositivos. Sendo assim, o objetivo do presente trabalho foi realizar um estudo para conceituar dispositivos IoT, propor um modelo de classificação para tais dispositivos e um processo de governança voltado para segurança destes dispositivos. A pesquisa foi realizada utilizando-se o modelo metodológico de estudo de caso, aplicado ao setor industrial.

Palavras-chave: internet das coisas; classificação; governança; segurança.

ABSTRACT

The increase in smart objects has made the field called Internet of Things (IoT) receive much attention due to its great potential for use, where objects with different characteristics can be connected, enabling the emergence of new applications. There are also some challenges, such as the restrictions of those objects, limitation of the operating system and the particularity of the communication protocols used, impacting the security aspect. That's why the importance of proper treatment for the security of IoT devices, many times, those objects cannot receive conventional security solutions. However, even before considering a security treatment, it is necessary to understand the characteristics of those devices. Therefore, the objective of the present work was to conceptualize IoT devices and propose a classification model for those devices and a governance process aimed at the security of those devices. The research was conducted using the case study model applied to the industrial sector.

Keywords: internet of things; classification; governance; security.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AC-DC	Alternate Current - Direct Current
AGV	Automatic Guided Vehicle
CCTV	Closed circuit television
CLP	Controlador Lógico Programável
CPS	CyberIphysical Systems
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
GE	General Electric
HTTP	Hypertext Transfer Protocol
ICD	Implantable Cardioverter Defibrillator
IDC	International Data Group
IIoT	Industrial Internet of Things
IoT	Internet of Things
ISO	International Organization for Standardization
LPWAN	Low Power Wide Area Network
NI	National Instruments
OWASP	Open Web Application Security Project
RFID	Radio Frequency Identification
SBRC	Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos
SCADA	Supervisory Control and Data Acquisition
VLAN	Virtual Local Area Network

SUMÁRIO

1 INTRODUÇÃO

O crescente aumento de objetos inteligentes que podem captar informações, processar e se comunicar, tem evidenciado o campo de Internet das Coisas, também conhecido pela sigla IoT (*Internet of Things*), o qual tem recebido bastante atenção devido ao potencial de uso em diversas áreas.

De modo geral, a Internet das Coisas pode ser encarada como uma extensão da Internet conhecida atualmente. Conceitualmente falando, não existe uma definição única para o termo, que varia de acordo com o contexto em que se está inserido, seja em ambiente doméstico, corporativo ou industrial.

No contexto industrial também surge a sigla IIoT (*Industrial Internet of Things*) que se refere aos objetos de IoT comumente aplicados dentro do setor industrial. Apesar destes objetos estarem mais focados para um setor específico também existe a dificuldade para definição conceitual devido à grande variedade de dispositivos que podem ser utilizados.

Um grande desafio para o campo de IoT se refere à segurança destes dispositivos, pois as restrições desses objetos em relação a processamento, memória e comunicação, além de suas limitações em âmbito de sistema operacional, que muitas vezes são simplificados e específicos para dispositivos com poucos recursos, bem como sua especificidade em relação aos protocolos de comunicação utilizados, são características que impactam substancialmente na segurança dos referidos dispositivos.

Sendo assim, fica clara a importância de um tratamento adequado no que se refere à segurança de dispositivos de IoT, pois muitas vezes tais objetos não são passíveis de receberem soluções de segurança convencionais. No que se refere ao setor industrial essas características são ainda mais acentuadas, pois existem muitos sistemas legados e proprietários, muitas vezes rodando *firmwares* extremamente simplificados, se fazendo ainda mais evidente a necessidade de uma gestão de segurança adequada, considerando que os impactos causados por falhas de segurança podem ser ainda maiores do que os impactos sofridos por falhas em dispositivos domésticos.

Desta forma o objetivo do presente trabalho foi propor um modelo de categorização de dispositivos de Internet das Coisas e um processo de governança voltado para segurança destes dispositivos delimitando o escopo da pesquisa para o setor industrial. O modelo metodológico escolhido foi estudo de caso com observação de campo e análise dos aspectos observados. O estudo foi realizado em uma indústria situada no estado do Paraná.

1.1 Objetivos

1.1.1 Objetivo geral

Propor um modelo de categorização de dispositivos de Internet das Coisas e um processo de governança voltado para segurança de dispositivos de Internet das Coisas.

1.1.2 Objetivos específicos

- Conceituar o termo Internet das Coisas;
- Conceituar dispositivo de Internet das Coisas;
- Propor modelo de classificação para dispositivos de Internet das Coisas;
- Analisar protocolos de comunicação de dispositivos de Internet das Coisas;
- Analisar aspectos de segurança de dispositivos de Internet das Coisas;
- Propor um processo de governança voltado para segurança de dispositivos de Internet das Coisas.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 DEFINIÇÃO DE INTERNET DAS COISAS

O termo Internet das Coisas tem recebido bastante atenção pois tem grande potencial de uso nas mais diversas áreas. A Internet das Coisas se refere a integração de objetos físicos e virtuais em redes conectadas à Internet, permitindo que ”coisas” coletem, troquem e armazenem uma enorme quantidade de dados (ALMEIDA, 2015).

Esse campo proporciona que objetos do dia-a-dia, adaptados com capacidade computacional e de comunicação, possam estar conectados, provendo comunicação entre usuários e dispositivos, possibilitando assim, o surgimento de uma nova gama de aplicações nas mais diversas áreas.

Existem inúmeras definições para Internet das Coisas, partindo de diferentes perspectivas. Nesta seção serão apresentadas algumas definições estabelecidas por diferentes entidades, desde grandes organizações atuantes no ramo da tecnologia, até mesmo consultorias e órgãos reguladores. Para facilitar a leitura e entendimento, as definições foram organizadas na Tabela 1, contendo definição original e a tradução em Português do Brasil (PT-BR).

Definição Original	**Tradução PT-BR**
"The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment" (GARTNER, 2017a).	A Internet das Coisas (IoT) é a rede de objetos físicos que contêm tecnologia incorporada para comunicar e sentir ou interagir com seus estados internos ou o ambiente externo
"The Internet of Things (IoT) is a term coined by Kevin Ashton, who conceived a system of ubiquitous sensors connecting the physical world to the Internet. Although things, Internet, and connectivity are the three core components of IoT, the value is in closing the gap between the physical and digital world in self-reinforcing and self-improving systems" (AMAZON, 2017).	A Internet das Coisas (IoT) é um termo cunhado por Kevin Ashton, que concebeu um sistema de sensores onipresentes conectando o mundo físico à Internet. Embora as coisas, a Internet e a conectividade sejam os três componentes principais da IoT, o valor está em fechar a lacuna entre o mundo físico e o digital em sistemas de auto-reforço e auto-aperfeiçoamento
"The Internet of Things refers to the growing range of connected devices that send data across the Internet" (IBM, 2017).	A Internet das Coisas refere-se à crescente gama de dispositivos conectados que enviam dados pela Internet

"Internet of Things (IoT) is a sprawling set of technologies and use cases that has no clear, single definition. One workable view frames IoT as the use of network-connected devices, embedded in the physical environment, to improve some existing process or to enable a new scenario not previously possible" (GOOGLE, 2017).	A Internet das Coisas (IoT) é um amplo conjunto de tecnologias e casos de uso que não possui uma definição clara e única. Uma visão viável enquadra a IoT como o uso de dispositivos conectados à rede, incorporados ao ambiente físico, para melhorar algum processo existente ou para permitir um novo cenário que antes não era possível
"The Internet of Things (IoT) is a robust network of devices, all embedded with electronics, software, and sensors that enable them to exchange and analyze data. The IoT has been transforming the way we live for nearly two decades, paving the way for responsive solutions, innovative products, efficient manufacturing, and ultimately, amazing new ways to do business" (INTEL, 2017).	A Internet das Coisas (IoT) é uma rede robusta de dispositivos, todos incorporados com eletrônicos, software e sensores que permitem a troca e análise de dados. A IoT vem transformando a maneira como vivemos há quase duas décadas, abrindo caminho para soluções responsivas, produtos inovadores, fabricação eficiente e, finalmente, novas maneiras incríveis de fazer negócios
"The IoT links objects to the Internet, enabling data and insights never available before" (CISCO, 2017).	A IoT vincula objetos à Internet, permitindo dados e insights nunca antes disponíveis
"The land of networked devices and other objects embedded with electronics, sensors, and software" (SALESFORCE, 2017).	A terra dos dispositivos em rede e outros objetos incorporados com eletrônicos, sensores e software
"The basic idea is that IoT will connect objects around us (electronic, electrical, non-electrical) to provide seamless communication and contextual services provided by them. Development of RFID tags, sensors, actuators, mobile phones make it possible to materialize IoT which interact and cooperate each other to make the service better and accessible anytime, from anywhere" (IETF, 2017).	A ideia básica é que a IoT conectará objetos ao nosso redor (eletrônicos, elétricos, não elétricos) para fornecer comunicação perfeita e serviços contextuais fornecidos por eles. O desenvolvimento de tags RFID, sensores, atuadores, telefones celulares possibilitam a materialização da IoT que interagem e cooperam entre si para tornar o serviço melhor e acessível a qualquer hora, de qualquer lugar
"The vast network of devices connected to the Internet, including smart phones and tablets and almost anything with a sensor on it – cars, machines in production plants, jet engines, oil drills, wearable devices, and more. These "things" collect and exchange data" (SAP, 2017).	A vasta rede de dispositivos conectados à Internet, incluindo smartphones e tablets e quase tudo com um sensor – carros, máquinas em fábricas, motores a jato, perfuratrizes de petróleo, dispositivos vestíveis e muito mais. Essas "coisas" coletam e trocam dados

"A network of items—each embedded with sensors—which are connected to the Internet" (IEEE, 2017).	Uma rede de itens - cada um embutido com sensores - que estão conectados à Internet
"The Internet of Things is the concept of everyday objects – from industrial machines to wearable devices – using built-in sensors to gather data and take action on that data across a network. So it's a building that uses sensors to automatically adjust heating and lighting. Or production equipment alerting maintenance personnel to an impending failure. Simply put, the Internet of Things is the future of technology that can make our lives more efficient" (SAS, 2017).	A Internet das Coisas é o conceito de objetos do cotidiano – de máquinas industriais a dispositivos vestíveis – usando sensores integrados para coletar dados e agir sobre esses dados em uma rede. Portanto, é um edifício que usa sensores para ajustar automaticamente o aquecimento e a iluminação. Ou equipamento de produção alertando o pessoal de manutenção sobre uma falha iminente. Simplificando, a Internet das Coisas é o futuro da tecnologia que pode tornar nossas vidas mais eficientes
"An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react" (ISO, 2014).	Uma infraestrutura de objetos, pessoas, sistemas e recursos de informação interconectados juntamente com serviços inteligentes para permitir que eles processem informações do mundo físico e virtual e reajam

Tabela 1 – Definições de Internet das Coisas.
Fonte: Elaborado pelo autor.

Além das definições genéricas existem também outros termos derivados, que se referem à aplicações ainda mais específicas para a Internet das Coisas, como é o caso da aplicação da Internet das Coisas na Indústria, por vezes referida como Industrial Internet of Things (IIoT).

Definição Original	**Tradução PT-BR**
"The Industrial Internet of Things (IIoT), also known as the Industrial Internet, brings together brilliant machines, advanced analytics, and people at work. It's the network of a multitude of devices connected by communications technologies that results in systems that can monitor, collect, exchange, analyze, and deliver valuable new insights like never before. These insights can then help drive smarter, faster business decisions for industrial companies" (GE, 2017).	A Internet Industrial das Coisas (IIoT), também conhecida como Internet Industrial, reúne máquinas brilhantes, análises avançadas e pessoas trabalhando. É a rede de uma infinidade de dispositivos conectados por tecnologias de comunicação que resulta em sistemas que podem monitorar, coletar, trocar, analisar e fornecer novos insights valiosos como nunca antes. Esses insights podem ajudar a impulsionar decisões de negócios mais inteligentes e rápidas para empresas industriais

Tabela 2 – Definições de Internet Industrial das Coisas.
Fonte: Elaborado pelo autor.

Além de se estabelecer uma definição conceitual para o termo Internet das Coisas também é importante entender quais são as caraterísticias de dispositivos que fazem parte da Internet das coisas, tanto aspectos de hardware, sistema operacional como forma de comunicação. O entendimento destas características contribui para o estudo e melhor compreensão dos apectos de segurança importantes para estes dispositivos.

2.2 HARDWARE EM INTERNET DAS COISAS

O *hardware* da Internet das Coisas é bastante diversificado, pois existem inúmeros dispositivos que podem ser considerados dispositivos de Internet das Coisas, desde os objetos convencionais que estão inseridos no cotidiano das pessoas, até mesmo sensores, atuadores, micro controladores, entre outros objetos de aplicações mais específicas, sendo este um dos principais fatores que evidenciam a relevância de um tratamento adequado para gestão e segurança de tais dispositivos. Mesmo com tanta diversidade é possível identificar algumas características básicas que geralmente estão presentes nestes dispositivos.

2.2.1 Arquitetura Convencional

A arquitetura básica de um dispositivo de IoT geralmente é composta, minimamente, por 4 unidades, sendo as unidades de processamento/memória, comunicação, energia e sensores/atuadores, conforme ilustra a Figura 1.

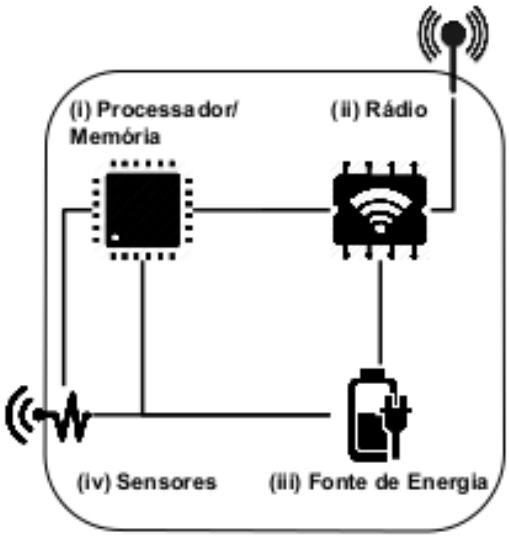

Figura 1 – Arquitetura Básica de Objetos Inteligentes
Fonte: SBRC (2016).

A unidade de processamento/memória (Figura 1.i) é composta de uma memória interna para armazenamento de dados e programas, um micro-controlador e um conversor analógico-digital para recepção de sinais de sensores. As CPUs empregadas nesses tipos de dispositivos geralmente são as mesmas utilizadas em sistemas embarcados e não apresentam alto poder computacional, visto que a prioridade é o consumo reduzido de energia e ocupar o menor espaço possível (SBRC, 2016).

A unidade de comunicação (Figura 1.ii) consiste em pelo menos um canal de comunicação com ou sem fio, sendo mais comum o meio sem fio. A maioria das plataformas usam rádio

de baixo custo e baixa potência. Assim, a comunicação é de curto alcance e apresenta perdas frequentes (SBRC, 2016).

A fonte de energia (Figura 1.iii) é responsável por fornecer energia aos componentes do objeto inteligente. De maneira geral, a fonte de energia consiste de uma bateria (recarregável ou não) e um conversor AC-DC e tem a função de alimentar os componentes. Entretanto, existem outras fontes de alimentação como energia elétrica, solar e mesmo a captura de energia do ambiente através de técnicas de conversão (SBRC, 2016).

As unidades de sensores/atuadores (Figura 1.iv) realizam o monitoramento do ambiente no qual o objeto está inserido. Estes sensores capturam valores de grandezas físicas como temperatura, umidade, pressão e presença. Existem muitos tipos de sensores diferentes que são capazes de capturar essas grandezas. Atuadores são dispositivos que produzem alguma ação, atendendo a comandos que podem ser manuais, elétricos ou mecânicos (SBRC, 2016).

2.3 SISTEMA OPERACIONAL EM INTERNET DAS COISAS

Assim como o hardware, se tratando de sistema operacional, existe uma grande variedade de sistemas operacionais para Internet das Coisas.

Devido às limitações destes objetos é necessário a utilização de sistemas operacionais específicos, com menor consumo de recursos. Existem diversos sistemas operacionais para IoT, sendo os mais conhecidos no mercado: CONTIKI, o TINYOS, o RIOT, o SNAPPY, o RASPBIAN.

Vale ressaltar que existe uma vasta gama de sistemas operacionais e que por diversas vezes o dispositivo IoT nem mesmo rodará um sistema operacional mas sim um *firmware* bastante simplificado. Se tratando do setor industrial, esta característica é ainda mais recorrente, sendo muito comum que dispositivos rodem apenas *firmwares* ou sistemas simplificados específicos e de propriedade do próprio fabricante do dispositivo.

2.3.1 Sistemas Operacionais IoT mais conhecidos

Cada sistema operacional possui características específicas sendo otimizados para determinados tipos de dispositivos, alguns sistemas exigem menos recursos, entre outras diferenças, conforme apresentado na Tabela 3.

Sistema	Min. RAM	Min. ROM	Linguagem
Contiki	< 2 KB	< 30KB	C
TinyOS	< 1 KB	< 4 KB	nesC e oTcl
RIOT	~ 1.5 KB	~ 5 KB	C e C++
Snappy	128 MB	-	Python, C/C++, Node JS e outras
Raspbian	256 MB	-	Python, C/C++, Node JS e outras

Tabela 3 – Comparativo entre os Principais SOs para IoT.
Fonte: SBRC (2016).

2.4 COMUNICAÇÃO ENTRE DISPOSITIVOS DE INTERNET DAS COISAS

Um dos fundamentos da Internet das Coisas é o fato de tais dispositivos estarem conectados. A comunicação entre estes dispositivos ocorre de diferentes maneiras, por isso a importância de se entender quais as características destas comunicações.

Assim como qualquer dispositivo convencional, um dispositivo de IoT conectado se utiliza de protocolos para comunicação com demais elementos da rede. Existem diversos tipos de protocolos, se tratando de dispositivos IoT, a quantidade de protocolos de comunicação é ainda maior, devido à grande diversidade de características presentes nestes dispositivos.

De maneira geral, estes protocolos podem ser classificados em duas grandes categorias: Redes de longo alcance e baixa potência (LPWAN - Low Power Wide Area Network) e Redes de curto alcance (Short Range Network), conforme menciona (AL-SARAWI *et al.*, 2017) *"Commonly, the communication protocols for IoT can be categorized into: (1) LPWAN and (2) short range network"*.

Se tratando de protocolos LPWAN, destaca-se o SigFox sendo um dos protocolos mais utilizados para IoT. Para categoria de Short Range Network exitem também vários protocolos vastamente utilizados e já conhecidos, como o próprio Bluetooth, RFID, ZigBee entre outros, conforme ilustra a Figura 2.

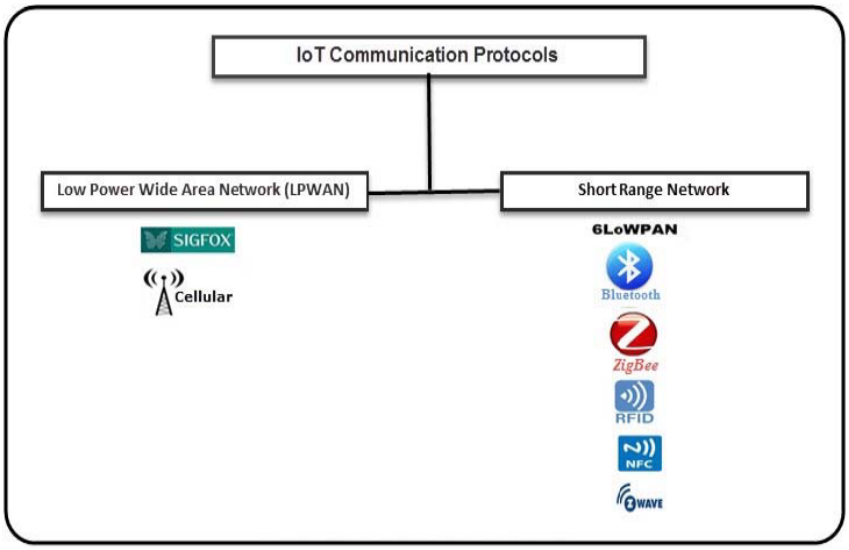

Figura 2 – Protocolos de Comunicação IoT
Fonte: Al-Sarawi *et al.* (2017).

2.5 SEGURANÇA EM INTERNET DAS COISAS

Garantir a segurança dos dispositivos de Internet das Coisas é um importante fator, pois com o exponencial crescimento será um segmento cada vez mais visado, visto que ocorrerá um crescente aumento da interface de vulnerabilidade, passando de uma gama de dispositivos convencionais como computadores, para uma interface maior de vulnerabilidade, composta pelos mais diversos tipos de dispositivos.

2.5.1 Crescimento da Internet das Coisas.

A Internet das Coisas cresce de maneira exponencial, diversas são as provisões para este segmento. Sejam pesquisadores da área, grandes entidades do segmento ou até mesmo grandes consultorias, todos possuem suas previsões para este crescente segmento.

A Gartner estimou que seriam aproximadamente 25 bilhões de dispositivos conectados até 2020 (GARTNER, 2017b). Já a IDC estimou que para esta data seriam aproximadamente 30 bilhões de dispositivos (IDC, 2017).

Com o crescimento deste segmento os ataques em dispositivos de Internet das Coisas se tornarão cada vez mais frequentes. Alguns ataques já ocorridos mostram a vulnerabilidade destes dispositivos e como este segmento ainda está despreparado.

2.5.2 Ataques e Vulnerabilidades em Internet das Coisas

Estudar as características dos ataques já ocorridos pode contribuir para o entendimento das vulnerabilidades e garantir a segurança relacionada à alguns elementos. A cada ataque novas são as lições aprendidas tanto pelos fabricantes quanto pelas companias que buscam cada vez mais um processo de gestão de segurança robusto.

Diversos ataques em dispositivos IoT já foram registrados no decorrer dos últimos anos, além de diversas vulnerabilidades descobertas por pesquisadores. Abaixo estão os principais ataques mostrados no infográfico de evolução de ataques IoT da (SECTIGO, 2020).

• **2005 – Virus Stuxnet em Usina Nuclear:** Em 2005 o vírus Stuxnet foi usado para atacar uma usina nuclear no Irã. O vírus se aproveitava das vulnerabilidades do sistema operacional SCADA (desenvolvido pela Siemens) utilizados em centrífugas de enriquecimento de urânio. Esse vírus foi um dos primeiros indicadores de vulnerabilidades da IoT e como elas podem causar a violações críticas de infraestrutura.

• **2008 – Vulnerabilidades em Monitores Cardíacos da Medtronic:** Em 2008 pesquisadores americanos descobriram que os desfibriladores cardíacos implantáveis (ICD) da empresa Medtronic poderiam ser controlados externamente, permitindo que invasores interceptassem in-

formações médicas e manipulassem os dispositivos, através dos sinais não criptografados no rádio embutido no dispositivo.

• **2009 – Ataque em Medidores de Energia Elétrica em Porto Rico:** Em 2009 uma concessionária de energia elétrica de Porto Rico perdeu centenas de milhões de dólares depois que o valor do consumo de energia foi manipulado, permitindo que os medidores inteligentes fossem controlados por dispositivos externos, não medindo com precisão a quantidade de energia usada, causando grandes prejuízos.

• **2011 – Vulnerabilidades em Bombas de Insulina da Medtronic:** Em 2011 vulnerabilidades em bombas de insulina utilizadas por pacientes com diabetes permitiram que pesquisadores localizassem e controlassem os dispositivos por meio de seus transmissores de rádio, tendo inclusive possibilidade de bombear quantidades excessivas de insulina no sangue.

• **2011 – Ataque em Empresa de Distribuição de Água de Illinois:** Em 2011 hackers conseguiram acessar e controlar o sistema industrial de uma concessionária de água de uma cidade de Illinois. Eles conseguiram queimar as bombas de água fazendo com que o sistema SCADA que controlava a bomba ligasse e desligasse repetidamente.

• **2014 – Bashlite Botnet:** Em 2014 surgiu a primeira versão da Botnet BASHLITE que infectou mais de 2 milhões de dispositivos em dois anos. Espalhando-se através da força-bruta (*brute-force*), o BASHLITE foi capaz de lançar vários tipos de ataques DDoS em larga escala simultaneamente.

• **2014 – Vulnerabilidade nos Semáforos na Universidade de Michigan:** Em 2014 pesquisadores tomaram o controle de um sistema inteiro de mais de 100 semáforos a partir de um único ponto de acesso. Facilmente hackeado, o sistema de semáforos usava comunicação via rádios, com criptografia bem básica e sem senha.

• **2014 – Ataque em Siderúrgica Alemã:** Em 2014 hackers usaram *spear phishing* para se infiltrar na rede de uma siderúrgica alemã e manipular seus controles para comprometer uma infinidade de sistemas, incluindo componentes industriais na rede de produção e um forno, que não puderam ser desligados adequadamente, resultando em danos substanciais.

• **2015 – Vulnerabilidades no sistema Connected Drive da BMW:** Em 2015 pesquisadores exploraram uma vulnerabilidade no sistema Connected Drive da BMW e simularam os servidores da BMW para enviar instruções de desbloqueio remoto aos veículos. O teste aproveitou o recurso de desbloqueio remoto, que pode ser solicitado por meio de uma linha de assistência da BMW.

• **2015 – Vulnerabilidades no sistema Uconnect da Fiat Chrysler:** Em 2015 foram encontradas vulnerabilidades no sistema Uconnect, um recurso inteligente que controla o entretenimento e navegação dos veículos Fiat Chrysler, que dava acesso à unidade principal do carro para código malicioso, que por sua vez poderia ser usado para enviar comandos para manipular componentes físicos, incluindo direção e freios.

• **2015 – Ataque à Rede Elétrica na Ucrânia:** Em 2015 hackers comprometeram a rede corporativa interna por meio de e-mails de malware de spear phishing. Eles conseguiram então

assumir o controle da rede SCADA (Sistema Operacional Siemens) e desligar as subestações, deixando 230 mil pessoas sem eletricidade. O malware também desativou os dispositivos de controle de IoT implantando *firmware* malicioso nos dispositivos.

• **2016 – Vulnerabilidades em Tesla Model S:** Em 2016 pesquisadores hackearam remotamente um Tesla Model S e assumiram o sistema multimídia e as telas do painel, conseguindo ligar o sinal de mudança de direção e abrir as portas sem usar uma chave. Eles também conseguiram ativar os limpadores de para-brisa, dobrar o retrovisor lateral e abrir o porta-malas enquanto o carro estava em movimento.

• **2016 – MIRAI Botnet:** Em 2016 uma das maiores redes de bots IoT chamada de Mirai aproveitou os dispositivos IoT com senhas padrão fracas e obteve o controle de um grande número de câmeras e roteadores, usando-os para lançar um ataque DDoS que prejudicou grandes áreas da Internet, incluindo o Twitter, The Guardian, Netflix, Reddit e CNN.

• **2016 – Malware de Atualização Automática Nyadrop:** Em 2016 um ataque de força-bruta (*brute-force*) direcionado à dispositivos IoT executando uma vasta lista de nomes de usuário e senhas comuns conseguiu obter acesso em vários IoT. O malware era difícil de diagnosticar e remover porque se autoexcluía e se alterava toda vez que invadia com sucesso um sistema.

• **2016 – Hajime Botnet:** Em 2016 surgiu uma botnet mais sofisticado que a Mirai, a Hajime lutaria contra botnets rivais pelo controle de um dispositivo. Hajime não tinha ferramentas para ataques DoS, apenas maneiras de continuar expandindo seu alcance e continuar lutando contra outras botnets. É conhecido por deixar mensagens peculiares, como “Fique atento!” em sistemas comprometidos.

• **2016 – CCTV Botnet:** Em 2016 esta botnet sequestrou 25,5 mil câmeras de CCTV conectadas à Internet para realizar ataques contra lojas online. A operação massiva conseguiu inundar sites com mais de 35 mil solicitações HTTP por segundo.

Na figura 3 elaborada pela Sectigo é possível ver os acontecimentos relacionados aos principais ataques IoT no decorrer do tempo, na ordem em que aconteceram.

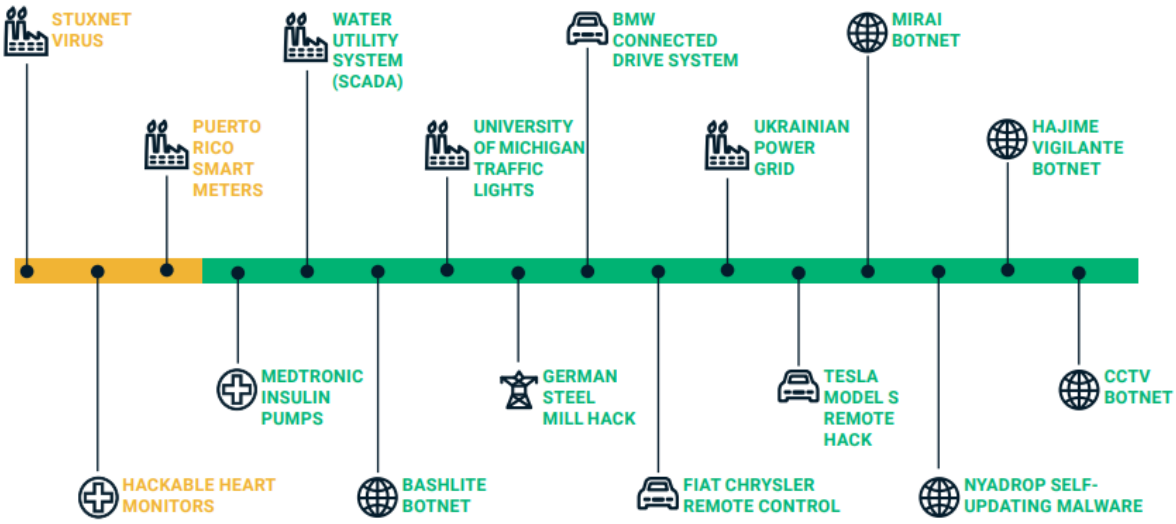

Figura 3 – Evolução de Ataques IoT
Fonte: Sectigo (2020).

3 PROCEDIMENTOS METODOLÓGICOS

O modelo metodológico utilizado foi o Estudo de Caso. Inicialmente foi feita a contextualização do termo Internet das Coisas por meio de conceitos apresentados na literatura com intuito de se estabelecer uma definição aproximada para o termo e evidenciar quais as características de IoT.

Posteriormente aplicou-se o estudo de caso no setor industrial com intuito de exploração para criar proximidade com o termo e entender como estes dispositivos são tratados no dia-a-dia pelas indústrias.

O estudo contemplou a etapa de exploração onde foi feito levantamento de todos os dispositivos existentes, posteriormente a classificação destes dispositivos em macro categorias para facilitar a gestão e por fim foi feito o estudo das caraterísticas destes dispositivos, gerando o framework apresentado para gestão de segurança.

Por motivos de segurança e privacidade, os dados reais da empresa onde o estudo de caso foi realizado foram omitidos e o framework final apresentado neste trabalho teve algumas informações removidas pois faziam sentido apenas para o contexto desta empresa em específico, porém as demais informações mantidas se aplicam de maneira geral para qualquer indústria.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Esta seção descreve os principais resultados obtidos com o presente trabalho, resultados estes ligados aos objetivos estabelecidos.

4.1 ESTUDO DE CASO NO SETOR INDUSTRIAL

Conforme mencionado nos procedimentos metodológicos do presente trabalho, a pesquisa foi realizada utilizando o modelo metodológico de estudo de caso com o objetivo de promover proximidade com o tempo e coleta e análise de dados em campo.

O estudo de caso foi realizado em empresa do setor industrial no estado do Paraná. Desta forma, os dispositivos de IoT abordados na presente pesquisa se referem majoritariamente à dispositivos utilizados dentro dos processos de fabricação.

As etapas realizadas no presente estudo foram inicialmente a conceituação e definição de Internet das Coisas no ambiente do estudo de caso, seguido de coleta de dados, observação e análise destes dispositivos identificados como IoT.

Posteriormente foi elaborada uma proposta de macro categorização para estes dispositivos baseada nas suas características, seguida do estudo dos requisitos de segurança necessários para estes dispositivos e em concordância com a necessidade da organização onde foi realizado o estudo de caso.

Com isto foi possível a criação de questionário (framework) para avaliação dos requisitos de segurança com objetivo de classificar o nível de segurança de cada dispositivos analisado. Por fim foi elaborada a proposta inicial de um modelo genérico de governança levando em consideração a ferramenta disponibilizada para avaliação de segurança, o nível de segurança de cada dispositivo e quais os níveis de segurança permitidos em cada área da organização dependendo do nível de criticidade da referida área.

4.2 DEFINIÇÃO DE INTERNET DAS COISAS DENTRO DO ESTUDO DE CASO

A primeira etapa realizada durante o estudo de caso foi a definição de Internet das Coisas, com objetivo de se chegar à um consenso de quais dispositivos seriam tratados como dispositivos IoT para a realização do estudo de caso, levando em consideração o contexto industrial.

Devido à grande quantidade de definições diferentes, conforme abordado na fundamentação teórica, foi bastante desafiador chegar ao consenso interno sobre qual seria a melhor definição de dispositivos IoT a ser aplicada para o estudo.

Levando em consideração as principais definições e também as orientações do comitê interno de infraestrutura da organização onde foi realizado o estudo de caso em questão, ficou

evidente que para a empresa em questão a melhor definição seria a mais simples possível, sem levar em consideração aspectos técnicos tão detalhados. Essa decisão se deu ao fato de que seria necessário que pessoas com pouco conhecimento técnico conseguissem entender o termo e saber distinguir um objeto IoT para direcionar para o processo de governança adequado, pois o processo de gestão começa muito antes de chegar no departamento de TI, até mesmo o setor de compras precisaria saber identificar este tipo de dispositivo para direcionar para o procedimento adequado.

Diante destas considerações ficou conceituado para a organização e o estudo de caso em questão a seguinte definição de um dispositivo de Internet das Coisas: *"An IoT device is any nonstandard computing device that connects to a network"* (Um dispositivo IoT é qualquer dispositivo computacional não padrão que conecta na rede).

O objetivo desta definição foi primariamente excluir todos os dispositivos considerados "padrões" dentro da organização, que eram os *desktops*, *laptops* e impressoras, considerando todo e qualquer outro tipo de dispositivo que não seja um destes 3 dispositivos mencionados como sendo um dispositivo IoT desde que conectado à rede intranet/internet. O intuito de excluir os dispositivos "padrões" foi devido ao fato de a organização já possuir processo de governança e gestão de segurança sólido para estes tipos de dispositivos.

4.3 COLETA DE DADOS E OBSERVAÇÃO DE CAMPO (INVENTÁRIO)

Após definição do que seria considerado um dispositivo de Internet das Coisas iniciou-se a etapa de coleta de dados e observação de campo. O objetivo desta etapa foi descobrir tudo que estava conectado à rede e poderia ser classificado como um dispositivo IoT e então entender suas características.

A coleta de dados inicial foi feita com o auxílio do software *Cisco Prime Infrastructure* que era utilizado pela organização para gerenciamento de rede. Este software foi utilizado para fazer varredura de todas as VLans *(Virtual Local Area Network)* dentro das dependências da organização.

Com a base de dados extraída do *Cisco Prime Infrastructure* foi possível ter uma visão inicial de todas as VLans existentes e todos os dispositivos conectados, tanto via cabo quanto Wireless. Nesta mesma base de dados também foi possível identificar a localização de cada dispositivo, bem como o *vendor* (fornecedor) de cada dispositivo, que é identificado pelo software a partir do *Mac Address* de cada dispositivo.

Após a coleta inicial de dados por meio da varredura de rede iniciou-se a etapa de observação de campo, que foi realizada por processo de amostragem. Com a informação da localização física dos dispositivos foi possível ir até o local dos dispositivos para observação de campo. O processo de verificação presencial dos dispositivos foi feito por amostragem, utilizando uma quantidade mínima de dispositivos de cada vendor identificado na base extraída do *Cisco Prime Infrastructure*. O intuito de se utilizar amostragem por vendor foi devido ao fato

de que um mesmo vendor em geral fornece um único tipo de dispositivo, de acordo com o processo interno da organização, não sendo necessário verificar fisicamente todos os dispositivos do mesmo vendor, sendo possível assumir que estes dispositivos pertencem à mesma categoria.

Após a etapa de observação de campo por amostragem foi possível gerar algumas informações relevantes para o entendimento do cenário da organização em relação à dispositivos IoT.

Um dado relevante foi identificar que aproximadamente 16% de todos os dispositivos conectados nas redes da empresa poderiam ser classificados como dispositivos IoT, levando em consideração o conceito de dispositivo IoT que foi definido em conjunto com a própria organização no início do estudo de caso.

Estes dispositivos IoT estavam majoritariamente dentro do setor industrial da empresa, distribuídos em diversos tipos de dispositivos.

• **Impressoras Industriais:** Impressoras específicas para segmento industrial utilizadas dentro do processo de fabricação e montagem. Um exemplo deste dispositivo se encontra na Figura 4.

Figura 4 – Impressora Industrial
Fonte: iSub (2022).

• **Controladores Lógicos Programáveis (CLPs):** Controladores utilizados para facilitar a automação dentro do processo de fabricação e montagem, controlando e monitorando outros equipamentos e processos específicos dentro da linha de produção. Um exemplo deste dispositivo se encontra na Figura 5.

Figura 5 – Controlador Lógico Programável
Fonte: Siemens (2022a).

• **Câmeras:** Utilizadas tanto para monitoramento do espaço físico e controle de acesso quanto para aplicações específicas dentro da linha de produção, em processo de reconhecimento de imagem, entre outros. Um exemplo deste dispositivo se encontra na Figura 6.

Figura 6 – Câmeras
Fonte: JN (2022).

• **Andons Industriais:** Painéis de Alerta utilizados dentro da linha de produção com objetivo de alertar de forma rápida e de fácil visualização informações importantes e em tempo real dentro da linha de produção, como falta de materiais, ausência de operador, atrasos ou erros em processos críticos, problemas em equipamentos. Um exemplo deste dispositivo se encontra na Figura 7.

Figura 7 – Andon
Fonte: Infrakom (2022).

• **Raspberrys:** Micro-computadores geralmente acoplados a outros dispositivos para controle e comunicação em processos específicos dentro da linha de produção. Um exemplo deste dispositivo se encontra na Figura 8.

Figura 8 – Raspberry
Fonte: Elektronica (2022).

• **AGVs:** Veículos autônomos utilizados para transportes de materiais dentro da linha de produção. Também fazem coletas de dados por meio de sensores para monitoramento do espaço físico, geralmente se comunicando e reportando à um controlador lógico ou gateway que centraliza as informações e faz a coordenação automática dos AGVs. Um exemplo deste dispositivo se encontra na Figura 9.

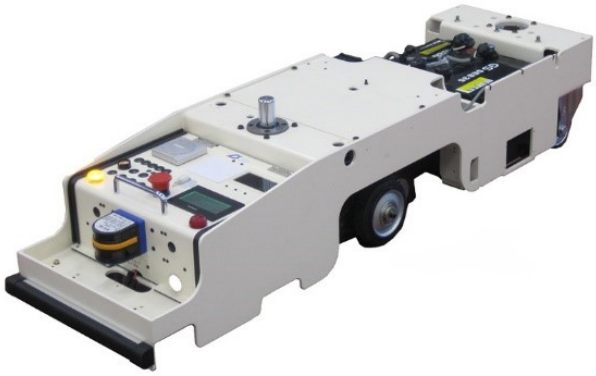

Figura 9 – AGV
Fonte: Aichikikai (2022).

• **Tablets Industriais:** Utilizados por operadores em funções específicas dentro do processo de fabricação, para comunicação e monitoramento de processos específicos da linha de produção. Um exemplo deste dispositivo se encontra na Figura 10.

Figura 10 – Tablet
Fonte: Siemens (2022b).

• **Celulares (Aplicação Industrial):** Celulares utilizados especificamente no setor industrial, conectados diretamente à rede industrial para controle e acesso de aplicações da linha de produção. Um exemplo deste dispositivo se encontra na Figura 11.

Figura 11 – Celular (Aplicação Industrial)
Fonte: DACOM (2022).

• **Pagers:** Utilizados para comunicações e notificações rápidas dentro do processo de fabricação, conectados em redes específicas para comunicação com Andons e Controladores Lógicos. Um exemplo deste dispositivo se encontra na Figura 12.

Figura 12 – Pager
Fonte: MMCall (2022).

• **Maletas de Teste:** Utilizadas para testes e manutenção preditiva constante em outros equipamentos geralmente com maior criticidade dentro da linha de produção. Podem fazer diversos tipos de medição como tensão, frequência, pressão, entre outras grandezas. Se comunicam com a rede industrial para fazer upload de dados para monitoramento de saúde dos dispositivos fabris. Um exemplo deste dispositivo se encontra na Figura 13.

Figura 13 – Maleta de Teste
Fonte: Surge (2022).

• **Coletores de Dados:** Utilizados para registro de informações de insumos utilizados dentro da linha de produção (geralmente por leitura de código de barras) fazendo comunicação e enviando dados em tempo real para outros equipamentos e aplicações. Um exemplo deste dispositivo se encontra na Figura 14.

Figura 14 – Coletores de Dados
Fonte: CiviTech (2022).

• **Braços Robóticos:** Utilizados na linha de montagem para atuação em diversas atividades, como encaixe de peças, soldagem, calibragem, ajuste de parafusos, medição, entre outros. Estão presentes em diversas etapas da linha de montagem e se comunicam com controladores lógicos ligados à rede industrial para monitoramento e controle de processos específicos dentro da linha de produção. Um exemplo deste dispositivo se encontra na Figura 15.

Figura 15 – Braços Robóticos
Fonte: Kalatec (2022).

4.4 CATEGORIZAÇÃO DE DISPOSITIVOS IOT (MODELO MACRO)

Conhecer as características e especificidades dos dispositivos de Internet das Coisas é um importante fator para se estabelecer um adequado processo de governança de dispositivos.

Um elemento importante que contribuiria para este melhor entendimento seria estabelecer uma categorização para tais dispositivos, o que facilitaria o estudo de características específicas de acordo com cada categoria de dispositivo, visto que, seria inviável estabelecer e estudar características específicas para cada dispositivo, devido à grande gama de dispositivos existentes.

No entanto no decorrer do estudo de caso este processo de categorização mostrou-se de pouca relevância para a definição do processo de governança, visto que muitas das características/requisitos de segurança se aplicariam para todas as categorias e poderiam ser tratadas em um único modelo de governança.

Para fins conceituais com intuito de fornecer minimamente um modelo de categorização para IoT, foi estabelecido juntamente com a empresa onde se realizou o estudo de caso um modelo de categorização genérico e de alto nível, onde foram definidas 3 grandes categorias: *Objeto IoT*, *Dispositivo IoT*, *Gateway IoT*.

• **Objeto IoT (IoT Object):** Caracterizado por ser a fonte de dados, geralmente fazendo a coleta/leitura de dados. Exemplos: TAGs, Sensores.

• **Dispositivo IoT (IoT Device):** Caracterizado por ser o dispositivo que contém um ou mais objetos e consegue trocar informações com o objeto. Exemplos: RFID reader, câmera, smartglass.

• **Gateway IoT:** Caraterizado por ser o gateway que se comunica com um ou mais dispositivos, é capaz de entender os protocolos utilizados pelos dispositivos e trocar informações. O IoT Gateway é geralmente quem faz a comunicação com a rede e se conecta às aplicações da empresa, mas não é regra, pois dispositivos e objetos também podem estar conectados diretamente à rede sem estarem atrelados à um gateway.

A Figura 16 mostra as 3 grandes categorias e como se relacionam.

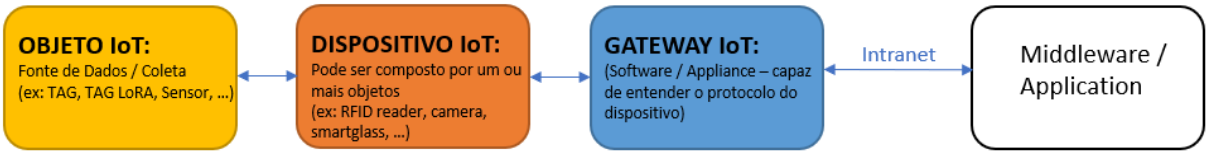

Figura 16 – Macro Categorias IoT
Fonte: Elaborado pelo autor.

4.5 FRAMEWORK PARA AVALIAÇÃO DE REQUISITOS DE SEGURANÇA

Após a definição do conceito de IoT para a organização alvo do estudo de caso, da coleta e análise de dados para entender quais os tipos de dispositivos IoT existentes dentro da organização, bem como definição de um modelo de categorização de alto nível, foi possível entender melhor o ambiente da empresa e conhecer melhor as características destes dispositivos para iniciar o estudo dos requisitos de segurança.

A definição dos requisitos de segurança IoT iniciou-se a partir do guia de segurança IoT apresentando pela OWASP (*Open Web Application Security Project*) Foundation. O objetivo deste guia, segundo OWASP (2018) foi facilitar a identificação de características e requisitos de segurança que devem ser avaliados em dispositivos IoT, características essas inerentes a grande maioria de dispositivos IoT. Baseado neste estudo da OWASP e também em algumas normas internas já existentes dentro da empresa foi possível definir um Framework (conjunto de requisitos) para avaliação de segurança IoT.

Os requisitos de segurança presentes nesse framework foram agrupados em grandes áreas como Interface, Autenticação, Privacidade, Segurança Física, entre outros. Um mesmo requisito também pode depender de ações tanto do lado do fornecedor/fabricante quanto do lado do cliente/usuário do dispositivo.

O objetivo de definir estes requisitos foi possibilitar uma avaliação de segurança de cada dispositivo IoT. Essa avaliação pode ser feita preenchendo o questionário de requisitos sempre que um novo dispositivo precise ser avaliado. Cada requisito deve ser avaliado e respondido no questionário como *"Aprovado"*, *"Reprovado"*, *"Não Aplicável"*.

Cada requisito também contém uma classificação de nível de impacto percebido pela empresa. Estes níveis de impacto foram alinhados juntamente com a equipe de segurança de informação da organização, chegando-se na definição de requisitos com *"Baixo Impacto"*, requisitos com *"Médio Impacto"* e requisitos com *"Alto Impacto"*. O objetivo de se ter o nível

de impacto para cada requisito foi para definir o número mínimo de requisitos cuja validação de segurança é obrigatória, desta forma, para os requisitos classificados como *"Alto Impacto"* é sempre obrigatório que este tipo de requisito seja avaliado para qualquer dispositivo, para os demais níveis é possível definir o requisito como *"Não Aplicável"* caso não seja necessário avaliação.

INTERFACE IOT		
REQUISITOS		
IMPACTO	AÇÃO DO FORNECEDOR	AÇÃO DO CLIENTE/USUÁRIO
Médio	O firmware/software do dispositivo deve permitir alteração de usuário e senha	Alterar usuário e senha padrão
Médio	O firmware/software do dispositivo deve identificar, notificar e tratar senhas fracas	Usar senha com letras maíusculas e minúsculas, caracteres alfanuméricos e símbolos
Médio	O firmware/software do dispositivo deve bloquear tentativas consecutivas com senhas erradas (proteção contra ataque de força bruta)	
Médio	A interface web deve ser testada contra vulnerabilidades de Cross-Site-Scripting (XSS)	
Médio	A interface web deve ser testada contra vulnerabilidades de SQL Injection (SQLi)	
Médio	A interface web deve ser testada contra vulnerabilidades de Cross-Site Request Forgery (CSRF)	
Médio	A interface web deve usar HTTPS	

Tabela 4 – Requisitos de Segurança para Interface IoT.
Fonte: Elaborado pelo autor baseado nas regras originais da OWASP (2018).

AUTENTICAÇÃO IOT		
REQUISITOS		
IMPACTO	AÇÃO DO FORNECEDOR	AÇÃO DO CLIENTE/USUÁRIO
Médio	O firmware/software do dispositivo deve permitir segregação em múltiplos ambientes para que os dados de um usuário não possam ser acessados por outro usuário	
Baixo	O firmware/software do dispositivo deve permitir autenticação de dois fatores (two-factor authentication)	Habilitar autenticação de dois fatores se disponível
Médio	O firmware/software do dispositivo deve possuir opção de recuperação de senha	
Baixo	O firmware/software do dispositivo deve possuir funcionalidade que faz a senha expirar depois de um certo tempo	Caso o dispositivo não tenha essa funcionalidade, criar uma rotina para alteração periódica de senhas

Tabela 5 – Requisitos de Segurança para Autenticação IoT.

Fonte: Elaborado pelo autor baseado nas regras originais da OWASP (2018).

REDE IOT		
REQUISITOS		
IMPACT	SUPPLIER/PROVIDER ACTION	USER/CUSTOMER ACTION
Alto	O dispositivo deve permitir ser identificado (Mac Address, IP, ID, outros)	
Alto	Assegurar que o dispositivo usa um protocolo de comunicação seguro e estável	Colocar proteção física nas portas de conexões
Alto	Assegurar que é possível desativar portas de serviços não utilizadas	Fechar portas de serviços não utilizadas (SSH, Telnet, SMB, FTP)
Médio	Assegurar que o dispositivo não tem portas de rede/serviços disponíveis via Upnp (Universal Plug and Play)	
Médio	Assegurar que os dispositivos tenham funcionalidades/mecanismos para lidar com buffer overhead e denial of service	

Tabela 6 – Requisitos de Segurança para Rede IoT.

Fonte: Elaborado pelo autor baseado nas regras originais da OWASP (2018).

PRIVACIDADE IOT		
REQUISITOS		
IMPACTO	AÇÃO DO FORNECEDOR	AÇÃO DO CLIENTE/USUÁRIO
Alto	Assegurar que é possível encriptar os dados armazenados	Analisar os tipos de dados armazenados e se algum tipo de criptografia via software ou aplicação se faz necessário
Alto		Assegurar que o acesso físico ao dispositivo é garantido apenas à pessoas autorizadas

Tabela 7 – Requisitos de Segurança para Privacidade IoT.
Fonte: Elaborado pelo autor baseado nas regras originais da OWASP (2018).

CONFIGURAÇÕES DE SEGURANÇA IOT		
REQUISITOS		
IMPACTO	AÇÃO DO FORNECEDOR	AÇÃO DO CLIENTE/USUÁRIO
Médio	Assegurar que logs de segurança estejam disponíveis para eventos de segurança	Quando disponível, mantenha os logs de sistema para os eventos de segurança do dispositivo sempre habilitados
Baixo	Assegurar que alertas e notificação estão disponíveis ao usuário para eventos de segurança	

Tabela 8 – Requisitos de Segurança para Configurações IoT.
Fonte: Elaborado pelo autor baseado nas regras originais da OWASP (2018).

SOFTWARE / FIRMWARE IOT		
REQUISITOS		
IMPACTO	AÇÃO DO FORNECEDOR	AÇÃO DO CLIENTE/USUÁRIO
Alto	Assegurar que o firmware/software do dispositivo possa ser atualizado de maneira segura (localmente e remotamente)	Garantir que exista uma rotina para verificação periódica de atualizações de software/firmware
Médio	Assegurar que os arquivos de atualizações sejam encriptados	
Médio	Assegurar que existam mecanismos/funcionalidades para validação de arquivos de atualização pelo dispositivo antes da instalação	
Médio	Garantir a segurança dos servidores de atualizações	
Médio	Assegurar que o dispositivo possa implementar atualizações agendadas (para automatização do processo de atualização)	
Alto	Assegurar que o dispositivo tenha ferramentas para gerenciar o firmware/software	
Alto	Assegurar que o firmware/software do dispositivo atende a atual legislação do país	
Alto	O firmware/software do dispositivo deve permitir o uso de antivirus ou outras ferramentas de segurança	
Baixo	O firmware/software do dispositivo deve permitir aplicação das regras da compania (senhas, atualizações, patches, entre outros)	

Tabela 9 – Requisitos de Segurança para Software / Firmware IoT.
Fonte: Elaborado pelo autor baseado nas regras originais da OWASP (2018).

SEGURANÇA FÍSICA IOT		
REQUISITOS		
IMPACTO	AÇÃO DO FORNECEDOR	AÇÃO DO CLIENTE/USUÁRIO
Médio	Assegurar que o firmware/software do dispositivo não pode ser acessado por métodos não intencionais, como portas USB	Promover proteção física do dispositivo evitando que ele tenha partes facilmente removíveis
Alto	O dispositivo deve ser inviolável (não permitindo acesso aos componentes internos)	
Médio	Assegurar que o dispositivo tem possibilidade de desabilitar portas externas (USB)	Desabilitar portas USB caso elas não estejam sendo utilizadas na operação

Tabela 10 – Requisitos de Segurança para Segurança Física IoT.
Fonte: Elaborado pelo autor baseado nas regras originais da OWASP (2018).

Uma vez que estes requisitos foram definidos foi possível criar um modelo de classificação dos dispositivos em níveis de segurança. Os níveis de segurança definidos foram A, B, C e D.

Cada nível é definido pelo percentual de requisitos atendidos/aprovados. Sendo considerados Nível A dispositivos que atendem 100% dos requisitos de segurança. Nível B dispositivos que atendem acima de 90% dos requisitos. Nível C dispositivos que atendem entre 70% e 90% dos requisitos e Nível D dispositivos que atendem abaixo de 70% dos requisitos.

O cálculo para definição do percentual de requisitos atendidos se dá pela média ponderada dos requisitos avaliados, sendo desconsiderados do cálculo os requisitos considerados como *"Não Aplicável"*.

RESULTADO ANÁLISE	
Quantidade de Critérios Analisados	**46**
Quantidade de Critérios Atendidos	**46**
Percentual de Requisitos Atendidos	**100%**
Nível de Segurança do Dispositivo	**NÍVEL A**

Tabela 11 – Exemplo de Resultado de Análise.
Fonte: Elaborado pelo autor.

NÍVEIS DE SEGURANÇA	
NÍVEL A	**Sem Risco** Estes dispositivos atendem completamente aos requisitos de segurança - 100%
NÍVEL B	**Baixo Risco** Estes dispositivos atendem a grande maioria dos requisitos de segurança - Acima de 90%
NÍVEL C	**Médio Risco** Esses dispositivos atendem parcialmente aos requisitos de segurança - Entre 70% e 90%
NÍVEL D	**Alto Risco** Estes dispositivos antendem minimamente aos requisitos de segurança - Menos de 70%

Tabela 12 – Níveis de Segurança.
Fonte: Elaborado pelo autor.

4.6 PROCESSO DE GOVERNANÇA PARA DISPOSITIVOS IOT

Após todas as etapas de definições, coleta e análise de dados, bem como definições de requisitos, foi possível definir um processo de governança.

O processo de governança consistiu em entender que todos os dispositivos IoT deveriam passar por uma avaliação de nível de segurança, por meio da utilização do questionário/-framework contendo os requisitos de segurança a serem considerados, com intuito de se chegar ao nível de risco do dispositivo IoT.

Este processo de governança deve ser aplicado nos dispositivos já existentes dentro da organização, para avaliar o nível de risco atual e possibilitar ajustes e ações para mitigar estes riscos nos dispositivos que já estão conectados. O processo também deve ser utilizado para avaliação de novos dispositivos que estão sendo estudados para utilização em novos projetos.

Além de se verificar o nível de segurança do dispositivo também é possível avaliar o nível de criticidade que estará diretamente relacionado ao local onde o dispositivo será aplicado. De acordo com as políticas da empresa, chegou-se à conclusão que o nível de criticidade é baixo quando o dispositivo é aplicado em âmbito administrativo, mas que este nível aumenta quando a aplicação passa a ser em âmbito industrial pois o impacto de uma possível interrupção no parque industrial pode ser mais grave, e este nível de criticidade fica ainda maior quando se trata de uma aplicação no âmbito de produto, pois além de oferecer riscos para os clientes também impacta na credibilidade da empresa.

Levando em consideração esta característica evidenciada pela organização foi possível também adicionar ao processo de governança as prerrogativas de que para aplicação em produto final, apenas dispositivos com classificação nível A são permitimos, para aplicação no segmento indústria/produção, apenas dispositivos nível A e B são permitidos, e para aplicação

em segmentos administrativos podem ser usados além de dispositivos nível A e B, também dispositivos nível C desde que em ambiente controlado.

Figura 17 – Processo de Governança IoT
Fonte: Elaborado pelo autor.

5 CONSIDERAÇÕES FINAIS

O campo denominado Internet das Coisas vem crescendo e sendo bastante evidenciado à medida que surgem cada vez mais dispositivos e objetos inteligentes conectados. Neste cenário surgem alguns desafios em relação às características destes objetos, bem como, suas limitações. Evidencia-se então a importância de um tratamento de segurança adequado.

O presente trabalho objetivou contextualizar o termo Internet das Coisas, estabelecendo definições conceituais, além de propor um modelo de macro categorização para os dispositivos de Internet das Coisas, posteriormente abordando os aspectos de segurança e propondo um processo de governança com foco em segurança.

A pesquisa utilizou-se do modelo metodológico de estudo de caso, sendo realizada em indústria no estado do Paraná. O modelo metodológico escolhido teve o intuito de promover proximidade com o tema e oportunidade de coleta e análise de dados em campo, utilizando dados reais da indústria. Devido à aplicação ter sido feita na indústria, a maioria das análises contemplaram dispositivos IoT industriais.

Como resultados alcançados, foi possível chegar em uma definição coerente de o que deve ser considerado IoT dentro do contexto do estudo de caso para a organização. Além disso foi possível por meio de coleta de dados e observação, conhecer os principais dispositivos conectados à rede da empresa que poderiam estar sendo classificados como IoT. Com a identificação destes dispositivos foi possível propor um modelo de macro categorização, levando em consideração as características e aplicação dos dispositivos.

Uma outra etapa importante foi o estudo dos principais requisitos de segurança que deveriam ser considerados para dispositivos IoT. Estes requisitos foram levantados por meio de revisão de literatura e estudos já existentes, tendo sido gerado a partir deste levantamento, o questionário para avaliação de segurança e classificação de nível de segurança para um dispositivo IoT.

Por fim, foi possível fazer uma proposta inicial de modelo de governança que leva em consideração o entendimento do que pode ser considerado um IoT, como avaliar seus riscos com intuito de se estabelecer qual o nível de segurança do dispositivos e o entendimento de onde este dispositivo tem sua aplicação permitida de acordo com o nível de segurança que possui, com objetivo de evitar que dispositivos com baixo nível de segurança sejam utilizados e aplicados em áreas com maior criticidade dentro da empresa.

O objetivo geral do presente trabalho foi atingido, porém alguns objetivos específicos, como por exemplo a análise detalhada dos protocolos de comunicação dos dispositivos, não foram possíveis de serem exploradas devido à quantidade de dispositivos e dimensão do trabalho, ficando como sugestão para trabalhos futuros.

REFERÊNCIAS

AICHIKIKAI. **Warehouse AGV**. 2022. Disponível em: https://www.directindustry.com/prod/aichikikai-techno-system-co-ltd/product-234260-2350049.html. Acesso em: 15 de junho de 2022.

AL-SARAWI, S. *et al.* **Internet of Things (IoT) Communication Protocols: Review**. 2017. Disponível em: https://ieeexplore.ieee.org/document/7973477. Acesso em: 21 de agosto de 2017.

ALMEIDA, H. **Internet das Coisas**: Tudo conectado. 2015. Disponível em: http://sbc.org.br/images/flippingbook/computacaobrasil/computa_29_pdf/comp_brasil_2015_4.pdf. Acesso em: 12 de setembro de 2016.

AMAZON. **Internet of Things**. 2017. Disponível em: https://aws.amazon.com/iot/?nc1=H_ls. Acesso em: 21 de agosto de 2017.

CISCO. **Internet of Things Overview**. 2017. Disponível em: https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html. Acesso em: 21 de agosto de 2017.

CIVITECH. **Coletor de dados industrial**. 2022. Disponível em: https://www.civitech.com.br/coletor-dados-industrial. Acesso em: 15 de junho de 2022.

DACOM. **MOBILE COMPUTERS GENERAL PURPOSE COMPUTERS TC21 / TC26**. 2022. Disponível em: https://www.dacomaidc.com/en/products/tc21-tc26_PROD-TC21TC26.html. Acesso em: 15 de junho de 2022.

ELEKTRONICA. **Metal housing Raspberry**. 2022. Disponível em: https://elektronicavoorjou.nl/en/product/metal-aluminum-alloy-housing-for-raspberry-pi-3/. Acesso em: 15 de junho de 2022.

GARTNER. **Internet of Things**. 2017. Disponível em: http://www.gartner.com/it-glossary/internet-of-things/. Acesso em: 21 de agosto de 2017.

GARTNER. **Internet of Things: The Foundation of the Digital Business**. 2017. Disponível em: https://www.gartner.com/webinar/3179129. Acesso em: 21 de agosto de 2017.

GE. **What is the Industrial Internet of Things**. 2017. Disponível em: https://www.ge.com/digital/blog/everything-you-need-know-about-industrial-internet-things. Acesso em: 21 de agosto de 2017.

GOOGLE. **Internet of Things Overview**. 2017. Disponível em: https://cloud.google.com/solutions/iot-overview. Acesso em: 21 de agosto de 2017.

IBM. **What is IoT**. 2017. Disponível em: https://www.ibm.com/internet-of-things/resources/library/what-is-iot/. Acesso em: 21 de agosto de 2017.

IDC. **Connecting the IoT: The Road to Success**. 2017. Disponível em: https://www.idc.com/infographics/IoT. Acesso em: 21 de agosto de 2017.

IEEE. **Internet of Things**. 2017. Disponível em: https://iot.ieee.org/images/_les/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf. Acesso em: 21 de agosto de 2017.

IETF. **Internet of Things**. 2017. Disponível em: https://iot.ieee.org/images/_les/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf. Acesso em: 21 de agosto de 2017.

INFRAKOM. **Production display boards**. 2022. Disponível em: https://www.exportersindia.com/product-detail/220v-production-display-boards-2721347.htm. Acesso em: 15 de junho de 2022.

INTEL. **Internet of Things Overview**. 2017. Disponível em: https://www.intel.com/content/www/us/en/internet-of-things/overview.html. Acesso em: 21 de agosto de 2017.

ISO. **Internet of Things Overview**. 2014. Disponível em: https://www.iso.org/_les/live/sites/isoorg/_les/developing_standards/docs/en/internet_of_things_report-jtc1.pdf. Acesso em: 21 de agosto de 2017.

ISUB. **Industrial Printer**. 2022. Disponível em: https://www.i-sub.co.uk/digital-textile-printing/dye-sublimation-printers/homer/homer-hm3200r-hybrid. Acesso em: 15 de junho de 2022.

JN. **Câmera PTZ industrial, para inspeção visual Pan Tilt**. 2022. Disponível em: https://jnrepresentacao.com.br/camera-ptz-industrial-baker-hughes/. Acesso em: 15 de junho de 2022.

KALATEC. **Robôs Industriais**. 2022. Disponível em: https://blog.kalatec.com.br/robos-industriais/. Acesso em: 15 de junho de 2022.

MMCALL. **Sistema Industrial Andon**. 2022. Disponível em: https://mmcallus.com/pt/industrial/sistema-andon. Acesso em: 15 de junho de 2022.

OWASP. **IoT Attack Surface Areas Project**. 2018. Disponível em: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Attack_Surface_Areas. Acesso em: 21 de abril de 2018.

SALESFORCE. **Internet of Things**. 2017. Disponível em: https://trailhead.salesforce.com/en/modules/iot_basics/units/iot_get_to_know_iot_cloud_unit. Acesso em: 21 de agosto de 2017.

SAP. **SAP Leonardo**. 2017. Disponível em: http://news.sap.com/brazil/2017/03/24/o-que-e-sap-leonardo/. Acesso em: 21 de agosto de 2017.

SAS. **What is the Internet of Things (IoT)**. 2017. Disponível em: https://www.sas.com/en_us/insights/big-data/internet-of-things.html. Acesso em: 21 de agosto de 2017.

SBRC. **Internet das Coisas**: da teoria à prática. 2016. Disponível em: http://www.sbrc2016.ufba.br/downloads/anais/MinicursosSBRC2016.pdf. Acesso em: 12 de setembro de 2016.

SECTIGO. **Evolution of IoT Attacks: An Interactive Infographic**. 2020. Disponível em: https://sectigo.com/uploads/resources/Evolution-of-IoT-Attacks-Interactive-IG_May2020.pdf. Acesso em: 21 de agosto de 2020.

SIEMENS. **CLP SIMATIC S7-1500**. 2022. Disponível em: https://new.siemens.com/br/pt/produtos/automacao/controladores/simatic-s7-1500.html. Acesso em: 15 de junho de 2022.

SIEMENS. **Tablet SIMATIC ITP1000**. 2022. Disponível em: https://www.directindustry.com/pt/prod/siemens-pc-based-industrial-automation/product-30335-2153999.html. Acesso em: 15 de junho de 2022.

SURGE. **Maleta Surge Test**. 2022. Disponível em: http://surgetestbrasil.com.br/. Acesso em: 15 de junho de 2022.