UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
COINT - TECNOLOGIA EM SISTEMAS PARA INTERNET
CURSO DE TECNOLOGIA EM SISTEMAS PARA INTERNET

MICHAEL PACHECO VORNES

SEGURANÇA EM INTERNET DAS COISAS

PROJETO DE TRABALHO DE CONCLUSÃO DE CURSO

GUARAPUAVA
2017

MICHAEL PACHECO VORNES

SEGURANÇA EM INTERNET DAS COISAS

Projeto de Trabalho de Conclusão de Curso apresentado ao Curso de Tecnologia em Sistemas para Internet da Universidade Tecnológica Federal do Paraná, como requisito parcial para a obtenção do título de Tecnólogo.

Orientador: Prof. Hermano Pereira
Universidade Tecnológica Federal do Paraná

GUARAPUAVA
2017

RESUMO

VORNES, Michael. Segurança em Internet das Coisas. 2017. 18 f. Projeto de Trabalho de Conclusão de Curso – Curso de Tecnologia em Sistemas para Internet, Universidade Tecnológica Federal do Paraná. Guarapuava, 2017.

O aumento de objetos inteligentes fez com que o campo denominado Internet das Coisas, também conhecido pela sigla IoT (Internet of Things), recebesse atenção devido ao seu potencial de uso, proporcionando que objetos com diferentes recursos possam estar conectados, possibilitando o surgimento de novas aplicações. Assim, existem 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 são passíveis de receberem soluções de segurança convencionais. Porém, antes mesmo se pensar em um tratamento de segurança é necessário entender as características de tais dispositivos. Sendo assim, o objetivo do presente trabalho é propor um modelo de categorização para dispositivos de Internet das Coisas e um processo de governança voltado para segurança destes dispositivos.

Palavras-chave: Internet das Coisas, Classificação, Governança, Segurança.

ABSTRACT

VORNES, Michael. Internet of Things Security. 2017. 18 f. Projeto de Trabalho de Conclusão de Curso – Curso de Tecnologia em Sistemas para Internet, Universidade Tecnológica Federal do Paraná. Guarapuava, 2017.

The increase of intelligent objects made the field called Internet of Things, also known by the acronym IoT, receive attention due to its potential of use, providing that objects with different resources can be connected, allowing the appearance of new applications. Thus, there are some challenges such as the restrictions of these objects, limitations of operating system and specificity of communication protocols used, impacting on the security aspect. Therefore the importance of an appropriate treatment for the security of IoT devices, since such objects are often not capable of receiving conventional security solutions. However, before even thinking about a security treatment it is necessary to understand the characteristics of such devices. Therefore, the objective of the present work is to propose a categorization model for Internet of Things devices and a governance process focused on the security of these devices.

Keywords: Internet of Things, Classification, Governance, Security.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AC-DC	Alternate Current - Direct Current
CPS	CyberIphysical Systems
CPU	Central Processing Unit
GE	General Electric
IDC	International Data Group
IIoT	Industrial Internet of Things
IoT	Internet of Things
ISO	International Organization for Standardization
NI	National Instruments
SBRC	Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos

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, industrial, entre outros.

Assim como, também não é possível estabelecer de maneira tão simplória o que pode ser considerado um dispositivo de Internet das Coisas, pois mais uma vez, dependerá também do contexto e ambiente em que se está inserido. Além disto, a grande diversidade de dispositivos, com diferentes características, é um desafio para o estabelecimento de uma definição conceitual.

O campo de Internet das Coisas proporciona que objetos variados, com diferentes recursos, e até mesmo objetos do dia-a-dia, adaptados com capacidade computacional e de comunicação, possam estar conectados, possibilitando assim, o surgimento de novas aplicações nas mais diversas áreas.

Neste cenário, surgem diversos desafios, como por exemplo as restrições desses objetos em relação a processamento, memória e comunicação, suas limitações em âmbito de sistema operacional, visto que muitas vezes possuem sistemas operacionais simplificados e específicos para dispositivos com poucos recursos, bem como sua especificidade em relação aos protocolos de comunicação utilizados, o que impacta substancialmente a segurança dos referidos dispositivos.

Sendo assim, fica clara a importância de um tratamento adequado no que se refere à segurança de dispositivos de IoT, principalmente devido às suas especificidades em relação à protocolos de comunicação e também devido suas limitações, pois muitas vezes tais objetos não são passíveis de receberem soluções de segurança convencionais.

Porém, antes mesmo de se estabelecer um tratamento adequado para a segurança dos referidos dispositivos, é necessário o conhecimento de suas principais características. Desta forma o objetivo do presente trabalho é propor um modelo de categorização de dispositivos de Internet das Coisas e um processo de governança voltado para segurança destes dispositivos.

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 um 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 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.

Antes mesmo de definir um processo de governança voltado para a segurança adequada de dispositivos de IoT é necessário conhecer as principais caraterísticas destes dispositivos, entender quais suas especificações e uma maneira de categorizá-los, pois ao se agrupar tais dispositivos em grandes grupos ou categorias, a utilização de um processo de governança por categorias se tornará mais fácil.

2.2 DIFERENTES DEFINIÇÕES PARA INTERNET DAS COISAS

Existem inúmeras definições para Internet das Coisas, partindo de diferentes perspectivas. Nesta seção serão apresentadas algumas definições estabelecidas por diferentes entidades, desde de grandes organizações atuantes no ramo da tecnologia, até mesmo consultorias e órgãos reguladores.

"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).

"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).

"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).

"The Internet of Things refers to the growing range of connected devices that send data across the Internet"(IBM, 2017).

"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).

"The IoT links objects to the Internet, enabling data and insights never available before"(CISCO, 2017).

"The land of networked devices and other objects embedded with electronics, sensors, and software"(SALESFORCE, 2017).

"A network of items—each embedded with sensors—which are connected to the Internet"(IEEE, 2017).

"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 co-operate each other to make the service better and accessible anytime, from anywhere"(IETF, 2017).

"CyberIphysical systems (CPS) sometimes referred to as the Internet of Things (IoT) – involves connecting smart devices and systems in diverse sectors like transportation, energy, manufacturing and healthcare in fundamentally new ways.Smart Cities/Communities are increasingly adopting CPS/IoT technologies to enhance the efficiency and sustainability of their operation and improve the quality of life.(NIST,"Global City Teams," 2014)" (NIST, 2017).

"L'Internet des objets, ou IoT (Internet of Things), est un scénario dans lequel les objets, les animaux et les personnes se voient attribuer des identifiants uniques, ainsi que la capacité de transférer des données sur un réseau sans nécessiter aucune interaction humain-à-humain ou humain-à-machine."(LEMAGIT, 2017).

"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).

"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).

"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).

Além das definições genéricas existem também outros termos derivados, que se referem a 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).

"The Industrial Internet of Things (IIoT) is the use of Internet of Things (IoT) technologies in manufacturing"(TECHTARGET, 2017).

"The IIoT can be characterized as a vast number of connected industrial systems that are communicating and coordinating their data analytics and actions to improve industrial performance and benefit society as a whole. Industrial systems that interface the digital world to the physical world through sensors and actuators that solve complex control problems are commonly known as cyber-physical systems. These systems are being combined with Big Analog Data solutions to gain deeper insight through data and analytics"(NI, 2017).

"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).

Além de se estabelecer uma definição conceitual é importante o entendimento dos aspectos relacionados aos dispositivos que compõem a Internet das coisas, como os aspectos de hardware, sistema operacional e forma de comunicação entre tais dispositivos.

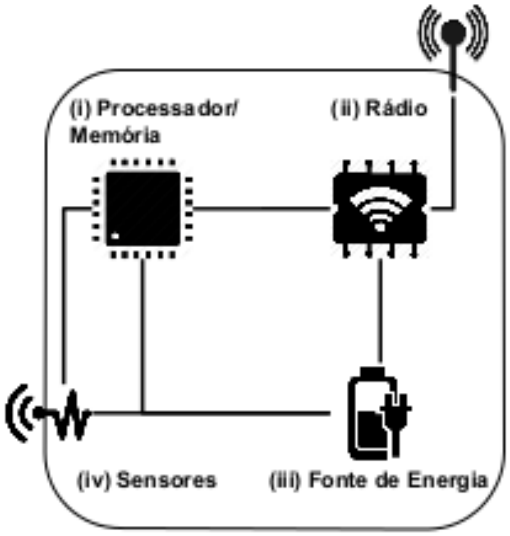
2.3 HARDWARE EM INTERNET DAS COISAS

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.

2.3.1 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.

Figura 1 – Arquitetura Básica de Objetos Inteligentes



Fonte: SBRC (2016)

A unidade de processamento/memória 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 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 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 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).

2.4 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 as limitações destes objetos inteligentes é necessário a utilização de sistemas operacionais específicos, com menor consumo de recursos. Existem diversos sistemas operacionais para IoT, sendo os mais conhecidos o CONTIKI, o TINYOS, o RIOT, o SNAPPY, o RASPBIAN, entre outros.

2.4.1 Comparativo entre Sistemas Operacionais

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

Figura 2 – Comparativo entre os Principais SOs para IoT

Sistema	Min. RAM	Min. ROM	Linguagem
Contiki	< 2 KB	< 30 KB	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

Fonte: SBRC (2016)

2.5 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.

2.6 GESTÃO DE DISPOSITIVOS DE INTERNET DAS COISAS

Fazer a gestão adequada dos dispositivos de Internet das Coisas pode se tornar uma tarefa difícil, principalmente quando se tem um grande número de dispositivos conectados, com diferentes características.

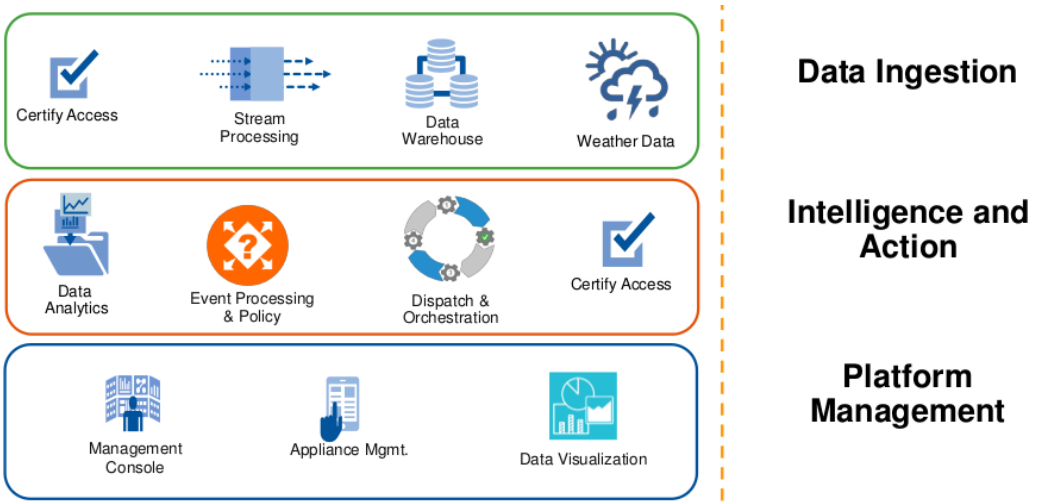
Para a gestão de tais dispositivos pode ser utilizado algum tipo de ferramenta ou plataforma, que pode ser uma solução proprietária desenvolvida pela própria organização para

administrar seus dispositivos, ou a utilização de uma plataforma de gestão de dispositivos já existente, oferecida por alguma entidade especializada. Atualmente existem diversas plataformas de gestão no mercado, desenvolvidas especificamente para dispositivos de Internet das Coisas.

2.6.1 Plataformas para Gestão de Internet das Coisas

Uma plataforma IoT precisa disponibilizar diversos recursos para gerenciamento de variados dispositivos. Basicamente é composta por 3 camadas: Data Ingestion, Intelligence and Action, Management (GARTNER, 2017b).

Figura 3 – Arquitetura de Referência para uma Plataforma IoT



Fonte: Gartner (2017b)

2.6.2 Requisitos para uma Plataformas de Internet das Coisas

Ao se analisar uma plataforma, se deve levar em consideração alguns requisitos para finalidade de comparações e verificação de qual plataforma atende melhor ao cenário que se pretende utilizar.

Figura 4 – Requisitos para uma Plataforma IoT

Requirement	Description
Architecture	Point vs. Modular vs. Suite
Deployment Models	Cloud vs. On-Premises
Sensor Management	Edge Device Management
Data xForm	Ingest Any Type of Data Construct
Data Warehouse	Data Storage Location
RT Stream Processing	Performs In-Stream Analytics for Immediate Decisions
Analytics	Post-Ingestion Data and Trend Analysis
Event Handling	Ability to Trigger/Send Events to Applications
Policy/Dispatching	Determine if a Threshold Has Been Exceeded and Take Action
Security/IAM	Authenticate IoT Devices, Secure Communications
IoT Admin Console	Platform Administration
IoT Visualization	Visualize Data and Trends From Warehouse
IoT Data Marketplace	Pull/Mashup Data From External Sources

Fonte: Gartner (2017b)

2.6.3 Principais Plataformas para Gestão de Internet das Coisas

Atualmente existem diversas plataformas de gerenciamento de IoT, visto que a maioria das grandes entidades do segmento de tecnologia possuem suas versões de plataformas IoT.

Figura 5 – Plataformas IoT Atuais

PLATAFORMA	**VENDOR**
AWS IoT	Amazon
Cloud Platform	Google
Watson IoT Platform	IBM
Azure IoT Suite	Microsoft
Fortinet Security Fabric	Fortinet
Predix	GE
Intel IoT Platform	Intel
Cisco Kinetic	Cisco
Oracle's Internet of Things Platform	Oracle
Samsung ARTIK	Samsung
SAP Leonardo	SAP
Plataforma EUGENIO	Logicalis
Bosch IoT Suite	Bosch
Salesforce IoT Cloud	Salesforce
ThingWorx IoT Technology Platform	ThingWorx
MindSphere	Siemens
Universal Internet of Things IoT Platform	HPE
KAA	Kaa IoT Technologies
Ayla IoT Platform	Ayla Networks

Fonte: Elaborado pelo autor

2.6.4 Comparativo entre Plataformas de Internet das Coisas

Cada plataforma fornece recursos e serviços específicos, sendo necessário o entendimento do seu ambiente para escolha da melhor plataforma. Levando em consideração os requisitos de uma plataforma é possível o comparativo destas, conforme exemplo a seguir.

Figura 6 – Comparativos entre Principais Plataformas IoT

Requirement	AWS	Google	IBM	Microsoft
Architecture	Modular	Modular	PaaS Suite	Suite
Sensor Mgmt.	No	No	Yes	IoT Hub (future)
Data xForm	Data Pipeline	No	Bluemix Cloud Integration/DataWorks	BizTalk Services
Data Warehouse	DynamoDB, Redshift	Cloud SQL, Cloud Storage	Cloudant/dashDB	SQL Data Warehouse
RT Stream	Kinesis	Cloud Dataflow	MQ Light/TimeSeries	Event Hubs
Analytics	Redshift, EMR, Mobile Analytics, Amazon ML	Big Query	Analytics Suite	Azure ML/ Stream Analytics/HDInsight
Event Handling	Lambda	Cloud Pub/Sub	MQ Light	Azure Service Bus
Policy/Dispatching	Lambda, SNS	No	MQ Light, Node-RED, IBM Lotus Workflow	BizTalk Services/Azure Service Bus
Security/IAM	AWS IAM, Cognito	Google Cloud IAM	Security AppScan/IBM SSO	Azure AD
IoT Admin Console	No	No	Node-RED	No
IoT Visualization	No	No	SPSS Predictive Modeler	Power BI
IoT Data Marketplace	No	No	No	No

Fonte: Gartner (2017b)

2.7 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.

2.7.1 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 estima que serão aproximadamente 25 bilhões de dispositivos conectados até 2020 (GARTNER, 2017b). Já a IDC estima que para esta data serão aproximadamente 30 bilhões de dispositivos (IDC, 2015).

2.7.2 Ataques em Internet das Coisas

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.

Estudar as características dos ataques já ocorridos pode contribuir para o entendimento das vulnerabilidades e garantir a segurança relacionada a alguns elementos.

Um dos grandes ataques ocorridos em dispositivos de Internet das Coisas foi o ataque conhecido como MIRAI, ocorrido em 2016 que atingiu um grande número de dispositivos de Internet das Coisas, sendo que suas principais características eram utilizar usuário e senhas padrões para acessar e controlar dispositivos.

3 PROCEDIMENTOS METODOLÓGICOS

Inicialmente será 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.

Desta forma será possível propor um modelo de categorização para tais dispositivos, com intuito de facilitar a criação de regras de governança baseadas em categorias ou grupos de dispositivos.

Posteriormente será feito um levantamento dos principais protocolos de comunicação utilizados por dispositivos de IoT objetivando uma análise dos aspectos técnicos destes protocolos. Por fim, será feita uma abordagem sobre os aspectos de segurança envolvendo tais protocolos e será proposto um processo de governança voltado para segurança de tais dispositivos.

4 RESULTADOS ESPERADOS

Esta seção descreve os principais resultados que se espera obter com o presente trabalho, resultados estes, diretamente ligados aos objetivos estabelecidos.

4.1 MODELO DE CATEGORIZAÇÃO DE DISPOSITIVOS DE INTERNET DAS COISAS

Conhecer todas 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 contribuirá para este melhor entendimento é estabelecer uma categorização para tais dispositivos, o que facilitará o estudo de características específicas de acordo com cada categoria de dispositivo, visto que, seria inviável estudar características específicas para cada dispositivo, devido à grande gama de dispositivos existentes.

4.2 PROCESSO DE GOVERNANÇA PARA DISPOSITIVOS DE INTERNET DAS COISAS

Após o estabelecimento de um método de categorização para os dispositivos de Internet das Coisas será possível estudar em maior nível de detalhes as características e especificações de cada categoria ou grupo de dispositivos, com isto, será possível também se estabelecerem regras de governança diretamente ligadas às características de cada categoria de dispositivo.

5 CONSIDERAÇÕES FINAIS

O campo denominado Internet das Coisas vem crescendo e sendo bastante evidenciado â 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.

Desta forma, o presente trabalho objetiva contextualizar o termo Internet das Coisas, estabelecendo definições conceituais, propondo um modelo de categorização para os dispositivos de Internet das Coisas e posteriormente analisar características técnicas relacionadas aos protocolos de comunicação prioritariamente utilizados, abordar também os aspectos de segurança e propor um processo de governança com enfoque em segurança.

6 PLANEJAMENTO DO TRABALHO

O planejamento do presente trabalho está descrito no crSonograma da Quadro 1. Neste cronograma constam todas as atividades com seus respectivos prazos para o cumprimento.

Quadro 1 – Cronograma de Atividades.

Atividades	**Ago**	**Set**	**Out**	**Nov**	**Dez**	**Jan**	**Fev**	**Mar**	**Abr**	**Mai**
1. Pesquisa sobre Estado da Arte	C	C								
2. Elaboração da Proposta de TCC	C	C								
3. Defesa da Proposta de TCC		C								
4. Revisão dos Apontamentos da Banca para a Proposta de TCC		C								
5. Revisão da Literatura			C	C	A	A	A	A	A	
6. Redação do Projeto de TCC			C	C						
7. Defesa do Projeto de TCC					C					
8. Revisão dos Apontamentos da Banca para o Projeto de TCC					C					
9. Escrita da Monografia de TCC					A	A	A	A	A	A
10. Elaboração da apresentação final										N
11. Defesa final do TCC										N
12. Revisão dos Apontamentos da Banca para a Monografia										N

Status:

C - Concluída

A - Em Andamento

N - Ainda Não Realizada

REFERÊNCIAS

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. Citado na página 3.

AMAZON. **Internet of Things**. 2017. Disponível em: <https://aws.amazon.com/iot/?nc1=h_ls>. Acesso em: 21 de agosto de 2017. Citado na página 3.

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. Citado na página 4.

CONTIKI. **Contiki: The Open Source OS for the Internet of Things**. 2016. Disponível em: <http://www.contiki-os.org/index.html>. Acesso em: 20 de setembro de 2016. Citado na página 7.

GARTNER. **Internet of Things**. 2017. Disponível em: <http://www.gartner.com/it-glossary/internet-of-things/>. Acesso em: 21 de agosto de 2017. Citado na página 3.

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. Citado 3 vezes nas páginas 8, 9 e 11.

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. Citado na página 5.

GOOGLE. **Internet of Things Overview**. 2017. Disponível em: <https://cloud.google.com/solutions/iot-overview>. Acesso em: 21 de agosto de 2017. Citado na página 3.

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. Citado na página 3.

IDC. **Connecting the IoT: The Road to Success**. 2015. Disponível em: <https://www.idc.com/infographics/IoT>. Acesso em: 21 de agosto de 2017. Citado na página 11.

IEEE. **Internet of Things**. 2017. Disponível em: <https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf>. Acesso em: 21 de agosto de 2017. Citado na página 4.

IETF. **Internet of Things**. 2017. Disponível em: <https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf>. Acesso em: 21 de agosto de 2017. Citado na página 4.

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. Citado na página 4.

ISO. **Internet of Things (IoT) - Preliminary Report**. 2014. Disponível em: <https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/internet_of_things_report-jtc1.pdf>. Acesso em: 21 de agosto de 2017. Citado na página 4.

LEMAGIT. **Internet des Objets IoT**. 2017. Disponível em: <http://www.lemagit.fr/definition/Internet-des-objets-IoT>. Acesso em: 21 de agosto de 2017. Citado na página 4.

NI. **The Industrial Internet of Things**. 2017. Disponível em: <http://www.ni.com/pdf/company/en/Trend_Watch_IIOT.pdf>. Acesso em: 21 de agosto de 2017. Citado na página 5.

NIST. **Internet of Things**. 2017. Disponível em: <https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf>. Acesso em: 21 de agosto de 2017. Citado na página 4.

RASPBIAN. **Welcome to Raspbian**. 2016. Disponível em: <https://www.raspbian.org/>. Acesso em: 20 de setembro de 2016. Citado na página 7.

RIOT. **RIOT: The friendly Operating System for the Internet of Things**. 2016. Disponível em: <https://riot-os.org/>. Acesso em: 20 de setembro de 2016. Citado na página 7.

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. Citado na página 4.

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. Citado na página 4.

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. Citado na página 4.

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. Citado 2 vezes nas páginas 6 e 7.

SNAPPY. **Snappy Ubuntu Core**. 2016. Disponível em: <https://www.ubuntu.com/core>. Acesso em: 20 de setembro de 2016. Citado na página 7.

TECHTARGET. **Industrial Internet of Things (IIoT)**. 2017. Disponível em: <http://internetofthingsagenda.techtarget.com/definition/Industrial-Internet-of-Things-IIoT>. Acesso em: 21 de agosto de 2017. Citado na página 5.

TINYOS. **TinyOS Home Page - Berkeley WEBS**. 2016. Disponível em: <http://webs.cs.berkeley.edu/tos/>. Acesso em: 20 de setembro de 2016. Citado na página 7.