UNIVERSIDADE PAULISTA

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO

INTERNET DAS COISAS: ANÁLISE DAS QUESTÕES CHAVE DE APLICAÇÃO PÚBLICA NO BRASIL

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Paulista - UNIP, para obtenção do título de Mestre em Engenharia de Produção.

ALAN KILSON RIBEIRO ARAÚJO

SÃO PAULO

2017

UNIVERSIDADE PAULISTA

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO

INTERNET DAS COISAS: ANÁLISE DAS QUESTÕES CHAVE DE APLICAÇÃO PÚBLICA NO BRASIL

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Paulista - UNIP, para obtenção do título de Mestre em Engenharia de Produção.

Orientador: Dr. Rodrigo Franco Gonçalves

Área de concentração: Gestão de Sistemas de Operação

Linha de pesquisa: Redes de Empresas e Planejamento de Produção

ALAN KILSON RIBEIRO ARAÚJO

SÃO PAULO

2017

Araújo, Alan Kilson Ribeiro.
Internet das coisas: análise das questões chave de aplicação pública no Brasil / Alan KilsonRibeiro Araújo. - 2017.
84 f. : il. color. + CD-ROM.

Dissertação de Mestrado Apresentado ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Paulista, São Paulo, 2017.

Área de concentração: Gestão de Sistemas de Operação.
Orientador: Prof. Dr. Rodrigo Franco Gonçalves.

1. Internet das coisas. 2. Aplicação. 3. Gestão pública.
I. Gonçalves, Rodrigo Franco (orientador). II. Título.

ALAN KILSON RIBEIRO ARAÚJO

INTERNET DAS COISAS: ANÁLISE DAS QUESTÕES CHAVE DE APLICAÇÃO PÚBLICA NO BRASIL

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Paulista - UNIP, para obtenção do título de Mestre em Engenharia de Produção.

Aprovado em: _____

Banca Examinadora:

_____

Dr. Rodrigo Franco Gonçalves
Universidade Paulista - UNIP

_____

Dr. João Gilberto Mendes dos Reis
Universidade Paulista - UNIP

_____

Dr. Márcio Aurélio Carvalho de Morais
Instituto Federal do Piauí - IFPI

DEDICATÓRIA

Dedico este trabalho inicialmente a Deus, pela saúde, paciência, competência e sabedoria para sua realização. Ao Instituto Federal do Piauí e a Faculdade Santo Agostinho juntamente com a Universidade Paulista pela oportunidade e espaço para concretização. Ao meu orientador Rodrigo Franco Gonçalves pela confiança. A minha família, pela compreensão, e colegas de turma e trabalho, pelo companheirismo.

AGRADECIMENTOS

Agradeço a minha esposa Marcelya Chrystian Moura Rocha por entender a importância da concretização deste objetivo e ao meu filho José Henrique Rocha Ribeiro, que apesar da pouca idade compreendia perfeitamente os momentos de ausência e de estudos do pai. Aos meus pais Maria Auxiliadora de Sousa Ribeiro pelo legado educacional, moral e ético e José Maria de Araújo pelas boas conversas. Meus irmãos Luciana, Airton e Marina pela descontração. Seria injusto de minha parte não mencionar meus "compadres" pelos momentos de alegria e felicidade. Obrigado a todos.

EPÍGRAFE

"A Internet das Coisas irá conectar todas as coisas com todo o mundo numa rede global integrada."

Jeremy Rifkin

RESUMO

A primeira revolução de infraestrutura inteligente da história denomina-se Internet das Coisas. Conceituada como uma rede mundial de objetos interconectados, permitiu um enorme salto em produtividade. No entanto, verifica-se que os recursos escassos na Internet das Coisas ainda são os grandes limitadores para segurança das informações transmitidas. Diante disso, o objetivo geral do estudo foi realizar uma análise crítica acerca de questões chave para exploração das tecnologias associadas à Internet das Coisas, desde segurança, privacidade, interoperabilidade e padrões, regulamentação e legislação e aplicações ligadas ao desenvolvimento social. A metodologia aplicada neste trabalho foi a revisão bibliográfica, que permitiu identificar a utilização da Internet das Coisas em sua efetividade para a gestão pública no gerenciamento e enfretamento dos problemas sociais, comparar os instrumentos regulatórios da Internet das Coisas vigentes e descrever o papel das camadas de segurança utilizadas na estrutura da Internet das Coisas e a análise de cenário prospectivo para o uso da Internet das Coisas no âmbito educacional pelas instituições da administração pública. Concluiu-se que a aplicação da Internet das Coisas proporciona significativa contribuição para a gestão pública, melhorando suas práticas internas e a vida dos cidadãos. Também foi constatado que o Governo Federal já estuda a criação de um Plano Nacional da Internet das Coisas em busca da padronização; que o modelo de protocolo de arquitetura de segurança em cinco camadas deve ser adotado no Brasil a fim de se obter interoperabilidade entre os dispositivos na IoT, garantindo uma maior segurança dos dados e que a IoT é um campo promissor no cenário prospectivo brasileiro, inclusive no âmbito educacional.

Palavras-chaves: Internet das Coisas. Aplicação. Gestão pública.

ABSTRACT

The first intelligent infrastructure revolution in history is called Internet of Things, conceptualized as a worldwide network of interconnected objects, which allowed a huge jump in productivity. However, it turns out that scarce resources on the Internet of Things are still the major limiters for the security of transmitted information. Thus, the general objective of the study was to conduct a critical analysis on key issues for exploiting technologies associated with Internet of Things from security, privacy, interoperability and standards, regulation and legislation and applications related to social development. The methodology applied to this work was the bibliographic review that allowed to identify the use of the Internet of Things in its effectiveness for public management in the management and coping of social problems, to compare the regulatory instruments of the Internet of Things exiting and describe the role of security layers used in the Internet of Things structure and to analyze prospective scenario for the use of the Internet of Things in the educational field by public administration institutions. It was concluded that the application of the Internet of Things affords significant contribution to public management by improving their internal practices and the lives of citizens, it was also verified that the Federal Government is already studying the creation of a National Internet of Things Plan in search of standardization, the protocol model of five layer security architecture must be adopted in Brazil in order to achieve interoperability between devices in IoT, by ensuring greater data security and that IoT is a promising field in the Brazilian prospective scenario, including on the education field.

Keywords: Internet of things. Application. Public management.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

IoT – Internet of Things

DTLS – Datagram Transport Layer Security

TI – Tecnologia da Informação

RFID – Radio Frequency Identification

RSSF – Rede de Sensores Sem Fio

NIC – National Intelligence Council

EUA – Estados Unidos da América

TIC - Tecnologia de Informação e Comunicação

CoAP – Constrained Application Protocol

E2E – End to End

LLN – Low power and Lossy Networks

SUMÁRIO

1 CONSIDERAÇÕES INICIAIS

Este trabalho apresenta e discute os conceitos de Internet das Coisas *(Internet of Things)* aplicados na gestão pública, apresentando suas potencialidades e limitações de uso para contribuir na gestão pública, além de apresentar os instrumentos regulatórios criados e desenvolvidos em países chaves do mundo em análise comparativa com o que está sendo desenvolvido no Brasil. Além disso, apresenta uma análise crítica dos protocolos de segurança aplicados na IoT, seguindo os parâmetros seguidos no mundo de forma a fomentar o debate em torno da consolidação do campo de pesquisa e reflexão na área da segurança da Internet das Coisas, dando subsídios para os projetos de pesquisa e dissertações a serem desenvolvidos sobre esta temática.

1.1 Introdução

No limiar do século XX, a revolução industrial deu início a mudanças, com refinamento de processos, inovações tecnológicas, reorganização dos processos. Foi um século marcado pela busca de eficiência da manufatura. Essa passou a ser uma nova fronteira, período áureo de Produção em Massa com características bem definidas (REIS et al., 2015), onde as fábricas passaram a ser altamente automatizadas e com menores custos operacionais (RIFKIN et al., 2004).

A partir disto, a globalização do panorama mundial provocou um novo cenário econômico. Numa visão da situação de negócios das empresas ocorreu a transição de uma sociedade industrial para uma sociedade de informação, em que a capacidade de gerar, analisar, controlar e distribuir as informações passou a ser um ponto estratégico para as organizações (COSTA, 2007).

A primeira revolução de infraestrutura inteligente da história denomina-se Internet das Coisas. Esta permitiu um enorme salto em produtividade, haja vista que conecta cada equipamento, empresa, residência e veículo em uma rede inteligente composta por Internet das Comunicações, uma Internet de Energia e uma Internet do Transporte, todas embutidas em um único sistema operacional, ou seja, conectar todas as coisas em uma rede global integrada (RIFKIN, 2016).

Desta forma, observa-se que as organizações estão procurando cada vez mais se adaptar às constantes mudanças ambientais e das incertezas. Dentro dessa ótica, o planejamento estratégico representa uma ferramenta indispensável na gestão das organizações

a fim de precaverem-se das incertezas com técnicas e processos administrativos que permitam o planejamento de seu futuro, a elaboração de objetivos, estratégias, métodos e ações (REIS et al., 2011), o que não é diferente no que se refere a administração pública União, Estado e Município (COSTA; CANUTO, 2010).

No entanto, verifica-se que os recursos escassos na Internet das Coisas ainda são os grandes limitantes para possibilitar segurança das informações transmitidas, mas a falta de padronização na segurança para Internet das Coisas é um sério problema, já que por enquanto só existe o protocolo *Datagram Transport Layer Security* (DTLS) disponível. Alguns trabalhos propõem o uso desse protocolo com outros presentes nas outras camadas existentes, mas não analisam a excesso de protocolos nos principais cenários da Internet das Coisas (JESUS; KLEINSCHMIDT, 2015).

As plataformas de *middleware* especificamente voltadas para ambientes de Internet das Coisas (IoT) é uma área de pesquisa recente que tem atraído a atenção da indústria e da comunidade acadêmica, e são alguns exemplos de plataformas concebidas para endereçar alguns dos desafios anteriormente descritos, principalmente com relação à integração transparente de dispositivos heterogêneos e à provisão de mecanismos de alto nível para desenvolvimento de aplicações (ATZORI; IERA; MORABITO, 2010).

1.1.1 Problematização

O presente estudo aborda questões chave acerca da aplicação da Internet das Coisas: segurança, privacidade, interoperabilidade e padrões, instrumentos regulatórios e legislação e aplicações ligadas ao desenvolvimento social, com as seguintes questões norteadoras:

a) Qual a utilização da Internet das coisas em sua efetividade para a gestão pública no gerenciamento e enfretamento dos problemas sociais?
b) Como o Brasil se encontra quanto aos instrumentos regulatórios da IoT em relação aos países chaves do mundo ?
c) É possível definir um modelo de protocolo de segurança no Brasil de Internet das Coisas que atenda ao cenário internacional?

1.1.2 Motivação

A necessidade de discorrer sobre a temática abordada surgiu da atuação profissional do pesquisador, que uma vez servidor público de Instituto Federal de Educação, Ciência e

Tecnologia, ao observar em publicações de cunho científico e em geral o destaque e aplicação da Internet das Coisas em países desenvolvidos, despertou o interesse em analisar a importância das potencialidades de utilização da Internet das Coisas no âmbito da gestão pública, que enquanto fenômeno globalizado, estreita inclusive os canais de comunicação entre a sociedade civil e o governo. Desse modo, entende-se que a gestão pública demanda qualidade, rapidez e segurança na prestação de serviços. Para tanto, faz-se necessário desmistificar a burocratização relacionada à regulamentação e padronização da IoT, uma vez que essa ferramenta traz significativa contribuição para o gestor público melhorar suas práticas internas, facilitando a tomada de decisão e a vida dos cidadãos, acelerando respostas, economizando e gerando recursos.

Nesse sentido, a análise comparativa das propostas de regulamentação e padronização da IoT no Brasil em relação a alguns países do mundo foram fundamentais para investigar o que é desenvolvido no quesito segurança, considerado primordial.

1.1.3 Escopo

O trabalho busca analisar a maneira como o governo brasileiro vem trabalhando e regulamentando o uso da IoT por meio de seus órgãos oficias ao mesmo tempo em que verifica se a forma que a regulamentação é trabalhada no Brasil está de acordo com o que é realizado em alguns países do mundo. Além disso, aborda os problemas de segurança de IoT dentro das camadas apresentadas nos protocolos de segurança e o aproveitamento da Internet das Coisas pela gestão pública no âmbito político e social, por meio de uma análise de cenário no âmbito educacional.

1.2 Objetivos

1.2.1 Objetivo Geral

Investigar como a Internet das Coisas está sendo utilizada no âmbito da administração pública brasileira, principalmente pelas instituições ligadas a educação, visando contribuir para a promoção do interesse na área pelos órgãos governamentais no Brasil.

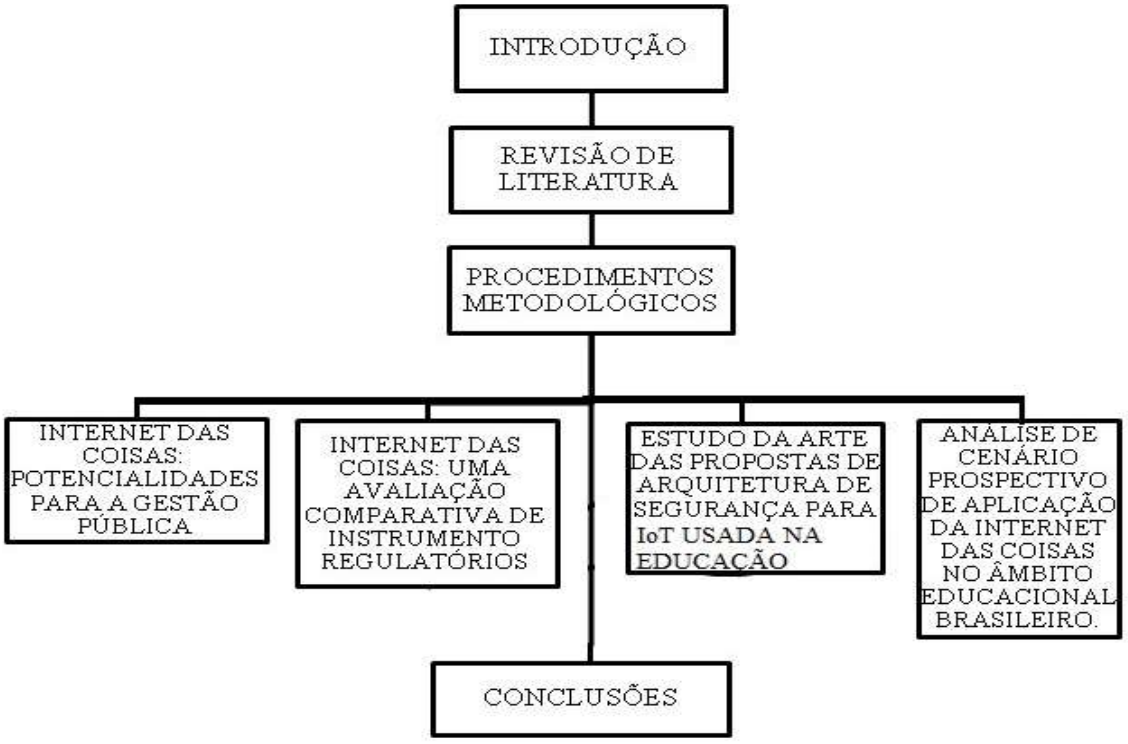
1.2.2 Objetivos Específicos

a) Realizar uma análise crítica acerca de questões chave para exploração das tecnologias associadas à Internet das Coisas desde segurança, privacidade, interoperabilidade e padrões, regulamentação e legislação e aplicações ligadas ao desenvolvimento social através da gestão pública.
b) Identificar a utilização da Internet das Coisas em sua efetividade para a gestão pública brasileira no gerenciamento e enfretamento dos problemas sociais.
c) Comparar os instrumentos regulatórios da Internet das Coisas vigentes.
d) Descrever o papel das camadas de segurança utilizadas na estrutura da Internet das Coisas.
e) Analisar cenários prospectivos de uso da Internet das Coisas no âmbito educacional pelas instituições da administração pública.

1.3 Organização do trabalho

O presente trabalho está organizado conforme demonstrado no organograma abaixo.

Organograma 1 – Estrutura da Dissertação



Fonte: O autor (2016).

A estrutura do trabalho inicia-se pela Introdução, onde é realizado o contexto da Internet das Coisas, apresentando sua relevância para o cenário atual de globalização. Assim é apresentada a problematização com a questões norteadoras abordadas no trabalho. Em seguida, apresenta-se a Motivação do trabalho com a importância e a justificativa da temática abordada. IoT requer estudo, levando em consideração as contribuições para a área do conhecimento e sociedade quanto ao alcance dos objetivos propostos, sendo estes: realizar análise crítica da arquitetura de segurança de IoT, contemplando sua aplicação no âmbito público que aborda sua regulamentação, e padronização no cenário brasileiro sendo mencionado nos resultados e conclusão.

Logo após inicia-se a revisão de literatura, abordando o processo histórico da globalização mundial, a utilização da Internet das Coisas em sua efetividade para a gestão pública no gerenciamento e enfretamento dos problemas sociais e modelo de segurança em três camadas na IoT.

Nos procedimentos metodológicos, além de apresentar a natureza da pesquisa, que é teórica, demonstra-se como a mesma foi realizada, a partir da pesquisa bibliográfica, análise de cenário prospectivo e da publicação dos artigos: “Internet das Coisas: potencialidades para a gestão pública”, “Internet das coisas: uma avaliação comparativa de instrumentos regulatórios” e “Estudo da Arte das propostas de arquitetura de segurança para IoT usada na Educação”, além do artigo desenvolvido “Análise de Cenário Prospectivo de aplicação da Internet das Coisas no âmbito educacional brasileiro”, contemplando assim o tópico dos resultados e discussões onde os mesmos são apresentados.

Por fim, nas conclusões confirma-se que a utilização da Internet das Coisas tem importância para a gestão pública, pois além de melhorar suas práticas internas e a vida dos cidadãos, acelera respostas e poupa ou gera recursos, e ressaltando também que o Governo Federal já realiza estudos da criação de um Plano Nacional da Internet das Coisas buscando padronização e regulamentação, que o modelo de protocolo de arquitetura de segurança em cinco camadas deve ser adotado no Brasil, a fim de se obter interoperabilidade entre os dispositivos na IoT por garantir uma maior segurança dos dados e que a IoT é um campo promissor nos cenários prospectivos inclusive no âmbito educacional brasileiro.

2 REVISÃO DE LITERATURA

2.1 Processo Histórico da Globalização Mundial

Nos primórdios da presença humana na Terra, as transformações que o homem produzia eram muito pequenas, sobretudo antes do desenvolvimento da atividade agrícola. No decorrer da história da humanidade, com o crescimento populacional e com o desenvolvimento de novas técnicas, o domínio de novas tecnologias e os novos instrumentos de produção, as intervenções nas paisagens foram sendo cada vez mais intensas e amplas (BRANCO, 2007).

Desta forma, compreende-se que nosso mundo está em constante evolução. Na história da humanidade, ocorreram inúmeros avanços durante milhões de anos, porém, quando se relaciona a indústria, destacam-se três momentos históricos, conhecidos como a primeira, segunda e terceira revolução industrial (SOARES, 2013).

A revolução industrial começou mais intensamente em meados do século XVIII na Inglaterra, de forma avassaladora, varrendo as organizações produtivas, sociais, familiares, políticas, as fronteiras do conhecimento, internacionais e de mercado, ou seja, teve como um dos principais acontecimentos a invenção da máquina a vapor e sua aplicação na produção têxtil, na fabricação de fios e tecidos (REIS et al., 2015; BRANCO, 2007).

Soares (2013) também ressalta que nesta época houve um grande crescimento nas cidades, logo a revolução espalhou-se para outros países europeus, atingindo também os EUA e o Japão, tendo a indústria têxtil como o principal setor em expansão desta primeira revolução.

Concorda-se que a mecanização se estendeu do setor têxtil para a metalurgia, para os transportes, para a agricultura e para outros os setores da economia. Diversos inventos revolucionaram as técnicas de produção e alteraram o sistema de poder econômico (TODA MATÉRIA, 2016).

Desta forma, a Primeira Revolução Industrial impulsionou a indústria de forma que propiciou um grande crescimento nas cidades. Porém, o anseio de crescimento e de criação de novas formas de facilitar a vida humana não parou e foi em meados de 1870 que surgiu a Segunda Revolução Industrial, também conhecida como segunda etapa da que ocorreu séculos antes.

Nesta etapa houve desenvolvimento da indústria química, elétrica, de petróleo e de aço; outros progressos essenciais nesse período incluem a introdução de navios de aço

movidos a vapor, o desenvolvimento do avião, a produção em massa de bens de consumo, o enlatamento de comidas, refrigeração mecânica e outras técnicas de preservação e a invenção do telefone eletromagnético (HOBSBAWM, 1999).

Logo após a Segunda Grande Guerra, na metade do século XX, a economia internacional começou a passar por profundas transformações, surgindo assim a Terceira Revolução Industrial, diferenciando-a das duas anteriores, uma vez que engloba mudanças que vão muito além das transformações industriais. Essa nova fase apresenta processos tecnológicos decorrentes de uma integração física entre ciência e produção, também chamada de revolução tecnocientífica.

Assim, entre 1989 e 1993, mais de 1 milhão de trabalhadores perderam seus empregos no setor industrial. Muitos deles vítimas da automação, tanto pelos empregadores americanos, quanto por empresas estrangeiras, cujas fábricas altamente automatizadas e com menores custos operacionais forçaram os fabricantes a reestruturar suas operações e demitir trabalhadores (RIFKIN, 2004).

Rifkin (2016) relata que na Primeira e Segunda Revolução Industrial ocorreram saltos em produtividade e crescimento atribuindo isto à matriz comunicação/energia/transporte e pela respectiva infraestrutura que compunha a plataforma tecnológica, às quais as empresas estavam conectadas.

Com isto, o perfil do trabalhador mudou, passando do operário para trabalhadores com nível de conhecimento mais elevado, os quais passaram a fazer parte de um grupo mais importante na equação econômica, onde os altos executivos e os investidores tiveram que compartilhar seu poder cada vez mais com os detentores da propriedade intelectual, em que abastecem a sociedade da informação da alta tecnologia (RIFKIN, 2004).

Desta forma, Costa (2007) cita a capacidade do ser humano de agir de maneira inteligente, abastecendo a alta tecnologia:

> A capacidade do ser humano em agir de maneira inteligente é frequentemente associada ao conhecimento construído ao longo do tempo e, dentro deste contexto, é intuitivo direcionar o pensamento ao fato de que a incorporação deste conhecimento para a construção de sistemas computacionais "inteligentes", conhecidos também por sistemas "especialistas" permite dar suporte ao processo de tomada de decisão. (COSTA, 2007, p. 387)

A Terceira Revolução Industrial teve como instrumento principal o uso da *internet*, que além de unir as pessoas em um único espaço virtual colaborativo e distribuído, une-os em

um espaço único, favorecendo mercados, uniões políticas continentais e a conectividade (RIFKIN, 2004).

As profundas implicações espaciais da internet só foram realmente registradas recentemente, começando a se espalhar pelos continentes, simultaneamente à criação de mercados continentais nascentes e de uniões continentais governantes (RIFKIN, 2012).

A complexidade tecnológica da era do conhecimento exige a articulação e cooperação, onde para inovar é preciso estar conectado a redes, sejam elas formais, informais, presenciais ou virtuais (REIS et al., 2015).

Costa e Canuto (2012) concordam que um dos campos onde as inovações têm surgido com mais intensidade na atualidade é o da TI (Tecnologia da Informação), sendo este um campo de conhecimento que abrange todas as informações criadas e utilizadas pelos negócios, bem como o grande espectro de tecnologias, cada vez mais convergentes e interligadas, que processam essas informações.

Desta forma, denota-se que o esgotamento da produção em massa, a personalização do produto, a valorização da opinião do cliente, a preocupação com o ambiente e a adoção da globalização econômica foram mudanças que facilitaram a junção das teorias de redes ao setor produtivo (REIS et al., 2015).

As companhias de TI do mundo estão trabalhando na estruturação da Internet das Coisas (IoT), tendo esta como objetivo conectar todas as coisas do mundo numa rede global integrada, composta pela Internet das Comunicações, Internet da Energia e Internet do Transporte, que funcionam juntas num sistema operacional único (RIFKIN, 2016).

Atzori, Iera e Morabito (2010) concordam que a Internet das Coisas é cenário da tecnologia sem fio moderna das telecomunicações, onde a ideia básica deste conceito é a presença generalizada em torno de nós de uma variedade de coisas ou objetos, como Radio-Frequency IDentification (RFID), tags, sensores, atuadores, telemóveis, que, através de esquemas de endereçamento único, são capazes de interagir uma com a outra e atingir objetivos comuns e inquestionavelmente, a principal força da ideia Internet das Coisas é o alto impacto que terá sobre vários aspectos do cotidiano da vida e o comportamento dos potenciais utilizadores.

Em última análise, os dispositivos da Internet das coisas será onipresente e permitirá a inteligência ambiente (ATZORI et al., 2012).

Rifkin (2012) conclui que a ligação em rede da comunicação, energia e comércio em rede, espalhados pelo planeta, invariavelmente dará lugar a uma governança em redes nos níveis continental e global.

2.2 Internet das Coisas no Gerenciamento e Enfretamento de Problemas Sociais

A próxima geração da Internet será a Internet das Coisas (IoT), que pode ser conceituada como uma rede mundial de objetos interconectados. Neste novo modelo, qualquer objeto que possua uma identificação exclusiva poderá se juntar à rede conhecida como a Internet. (JIANG; ZHANG; WANG, 2013).

Atzori, Iera e Morabito (2010) ressaltam que a Internet das Coisas é um paradigma do cenário moderno da comunicação sem fio. A ideia básica da Internet das Coisas é sua presença a nossa volta por meio de uma variedade de objetos, e que não precisa ser necessariamente implementada na forma de uma Rede de Sensores sem fio. Qualquer sistema de endereçamento único para os objetos que tenha uma estrutura similar à internet pode ser considerado uma implementação deste conceito, haja vista que para os objetos interagirem com outros, normalmente são utilizados tags RFID (Radio-Frequency IDentification), atuadores, sensores, celulares e até mesmo leitores de código de barra.

Segundo Zambarda (2014), a Internet das Coisas se refere a uma revolução tecnológica que em breve conectará equipamentos como eletrodomésticos, meios de transporte, roupas e maçanetas conectadas à Internet e a outros dispositivos, como computadores e smartphones.

Devido a importância da IoT, o Conselho Nacional de Inteligência dos EUA (NIC) a considera como uma das seis tecnologias civis mais promissoras e que mais impactarão a nação no futuro próximo. O NIC (2008) prevê que em 2025 todos os objetos do cotidiano (por exemplo, embalagens de alimento, documentos e móveis) poderão estar conectados à internet.

A Internet das coisas também é utilizada para criar cidades inteligentes; sensores medem vibrações e condições de materiais em prédios, pontes, estradas, e outras infraestruturas para avaliar a saúde estrutural da construção e apontar as necessidades de reparos; também tem sido aplicada em ritmo acelerado no meio ambiente para administrar os ecossistemas da Terra, onde sensores são usados em florestas para alertar os bombeiros sobre as condições de perigo que podem desencadear incêndios (RIFKIN, 2016).

Rifkin (2012) cita que a internet das coisas pode também ser utilizada para criar uma rede inteligente de energia em residências, escritórios, fábricas e veículos de comunicação contínua, compartilhando informações e energia ininterruptamente. O autor revela ainda que a invenção da Tecnologia da Informação (TI) para rede da segunda geração mudou a equação econômica, deslocando o equilíbrio do poder centralizado nas velhas energias de combustíveis fósseis e de urânio para novas energias renováveis, distribuídas.

Whitmore, Agarwal, Xu (2014) fazem referência a outras aplicabilidades da IoT, como as relações sociais em que se promove a interação social e atendem às necessidades das pessoas por meio de dispositivos com serviços de redes sociais, como Facebook ou Twitter. Isso é possível quando telefones habilitados podem se conectar diretamente a telefones móveis. No que se refere à segurança, a Internet das coisas é tipicamente sem fio e pode estar localizada em locais públicos, tornando-se mais segura através de criptografia, que é fundamental na garantia da segurança da informação, pois para ativá-la são necessários algoritmos e esquemas de distribuição-chave mais eficientes. Além da criptografia, o gerenciamento de identidade é um componente importante de qualquer modelo de segurança e identificadores originais são essenciais para os dispositivos da Internet das coisas, haja vista que esses identificadores podem ser usados para estabelecer as identidades pessoais em financeira, instituições, identificar a atividade ilegal e outras funções.

Contudo, Pagano, Chitinis e Lipare (2007) apontam que em sua maioria, as redes de sensores sem fio possuem recursos limitados, baixa confiabilidade em termos de nós individuais, arquitetura distribuída, comunicação sem fio e topologia de rede dinâmica. Essas características proporcionam desafios consideráveis a serem equacionados no desenvolvimento dessas novas classes de aplicações, que são “denominadas de segunda geração de aplicações de RSSF”.

Portanto, no contexto de criação de cidades inteligentes, Komninos et al. (2011) analisam que, embora se sustente em infraestruturas digitais, a cidade inteligente depende do desenvolvimento contínuo da capacidade de aprendizagem para a inovação e replicação nos processos de gestão da dinâmica urbana, utilizando as capacidades da cidade digital para implementar sistemas de informações que melhorem a disponibilidade e a qualidade das infraestruturas e serviços públicos, incrementando sua capacidade de crescimento e estimulando a inovação e o desenvolvimento sustentável. Isso significa que a cidade digital não é necessariamente inteligente, mas a cidade inteligente tem, obrigatoriamente, componentes digitais.

A cidade digital é caracterizada primordialmente pela capacidade de implementação de tecnologias de comunicação, promovendo o acesso amplo a ferramentas, conteúdos e sistemas de gestão, de forma a atender às necessidades do poder público e seus servidores, dos cidadãos e das organizações (YOVANOF; HAZAPIS, 2009).

Já a cidade inteligente emerge da cidade digital a visão de inteligência das cidades, que vem da convergência entre a sociedade do conhecimento, onde a informação e a criatividade têm grande ênfase e considera os capitais humano e social como seus mais

valiosos ativos (CASTELLS, 2012). A cidade digital faz extensivo uso de sistemas de telecomunicações e recursos da internet como meio para transformar significativamente as formas de relacionamento e de vida (COELHO, 2010).

As iniciativas para cidades inteligentes focalizam o uso das TIC's para transformar a vida e o trabalho dentro de uma região de forma significativa e fundamental, mais do que de forma incremental, explorando os recursos da cidade digital de maneira inovadora e colaborativa. Nesse sentido, a cidade digital não é necessariamente inteligente, mas a cidade inteligente tem, obrigatoriamente, componentes digitais (KOMNINOS et al., 2011; DUTTA, 2011).

Criar cidades inteligentes não se trata de uma revolução, de um conceito tecnológico ou de um fenômeno localizado particularmente. Trata-se, ao contrário, de uma evolução, de desenvolvimento socioeconômico e de um fenômeno global em que se busca a harmonização entre o mundo material e o mundo virtual, entre todos os subsistemas do sistema urbano, no melhor interesse dos atores que atuam nas cidades e respeitando suas características e vocações particulares (BOYKO et al., 2006; TOPPETA, 2010).

Desta forma, observa-se, de forma geral que, no que se refere a organizações privadas e administração pública União, Estado e Município, existe cada vez mais uma procura de adaptação às constantes mudanças ambientais e das incertezas, tendo como meio mediador e facilitador a aplicabilidade da Internet das Coisas.

2.3 Modelo de Segurança em Três Camadas da IoT

A miniaturização dos dispositivos computacionais e a diminuição do custo dos seus componentes possibilitaram a inserção destes dispositivos em diversos locais e em diferentes aplicações. Desta forma, as redes de sensores sem fio se beneficiaram com essa evolução, em que criou-se redes de sensores que possuíam uma organização similar à internet. Esta organização de elementos de forma similar à Internet foi chamada de Internet das Coisas (IoT). A partir do momento que se teve a necessidade de disponibilizar essa Internet das Coisas na *Web*, criou-se uma outra arquitetura, conhecida como Rede das Coisas (ATZORI; IERA; MORABITO, 2010).

De acordo com Miorandi et al. (2012), para o funcionamento eficiente de IoT é necessário que a estrutura de rede utilizada disponibilize alguns recursos chaves em nível de sistema, como: heterogeneidade dos dispositivos, escalabilidade, troca de dados entre tecnologias ubíquas sem fio, soluções otimizadas de energia, capacidade de rastreamento e

localização, capacidade de auto-organização, interoperabilidade semântica e gerenciamento de dados, segurança incorporada e mecanismos de preservação da privacidade.

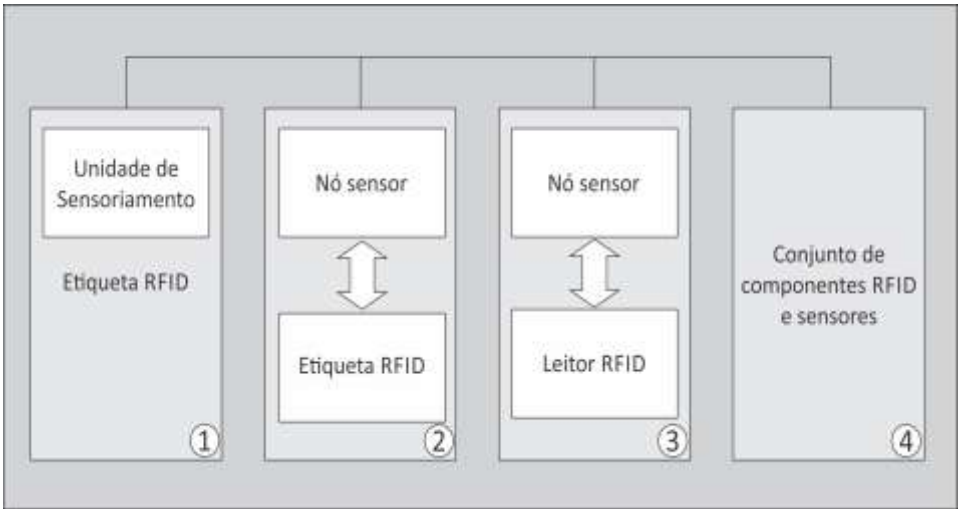
Entre as tecnologias mais promissoras para o paradigma de IoT estão a RFID (*Radio-Frequency IDentification*) e RSSF (Redes de Sensores Sem Fio). Os sistemas RFID são velozes e compatíveis para a identificação de objetos; já as RSSF são redes que podem cooperar para captar e distribuir dados (ATZORI; IERA; MORABITO, 2010).

Contudo, quando comparado com sistemas RFID ou RSSF individualmente, essas tecnologias integradas apresentam um potencial bastante promissor (WANG et al., 2014).

Mason et al. (2006) concordam ao afirmar que a integração das tecnologias de RFID e RSSF maximiza os seus benefícios, criando novas perspectivas para um maior número de aplicações, e aproximando o mundo real das pesquisas acadêmicas; isso ocorre porque o resultado dessa integração é uma tecnologia com capacidade estendida, escalável e portável com custos reduzidos.

No entanto, para Luo et al. (2011), o resultado desta integração pode trazer mais desafios técnicos, políticos e operacionais do que as tecnologias de RSSF e RFID já possuem de forma isolada, conforme apresentado na figura 01, que demonstra a tipos de integração entre essa tecnologias.

Figura 1 – Tipos de Integração RSSF e RFID



Fonte: Liu et al. (2008).

Outro aspecto importante para utilização da IoT é a sua segurança, fator fundamental para garantir a confidencialidade, autenticação e atualização de chaves entre duas entidades; as informações trocadas na rede devem ser protegidas de forma "*end-to-end*" (E2E); para isso, o CoAP identificou o protocolo "*Datagram Transport Layer Security*" (DTLS), como a

abordagem para proteger a comunicação CoAP em um *Low power and Lossy Networks* (LLN) ao nível da camada de transporte; a segurança "*end-to-end*" pode fornecer segurança mesmo se a infraestrutura de rede subjacente for apenas parcialmente sob o controle do utilizador (SILVA, 2013).

Atzori, Iera e Morabito (2010) confirmam que a comunicação automática entre os diversos dispositivos pessoais pode trazer alguns perigos, considerando que esse tipo de comunicação acaba se tornando uma espécie de vigilância na vida das pessoas. Isso porque será praticamente impossível realizar um controle da divulgação dos dados pessoais e de certa forma acaba gerando a falta de privacidade.

Jesus e Kleinschmidt (2015) especificam que o DTLS é um protocolo de segurança usado para proteger o tráfego de *datagramas* para aplicações cliente/servidor, automatizando o gerenciamento de chaves, a autenticação e a encriptação dos dados. É composto de um protocolo *Record* que carrega outros protocolos como o *Alert, Change Ciphe Spec, Handshake,* e *Data.*

Silva (2013) alerta que diversas aplicações de Redes de Sensores sem Fio necessitam de serviços de segurança e, devido às limitações dos dispositivos, os mecanismos de segurança causam efeitos indesejáveis na rede, como o aumento do consumo de energia e o atraso na comunicação, representando um problema para a implementação de mecanismos de segurança.

Vários pesquisadores vêm se questionando sobre soluções que esse novo campo irá trazer, bem como a inserção, tanto de novos dispositivos como novas redes, no período de 2015-2020, que serão semi-inteligentes e gradualmente obterão a compreensão ampla do meio e aspectos da vida social depois de 2020. Entretanto, outros desafios, são observados também no seu desenvolvimento, principalmente no campo da segurança, regulamentação e padronização (ZHAO; GE, 2013).

Referindo sobre o design da arquitetura de segurança observa-se que este vem sendo discutido na literatura, surgindo diversas propostas. Zhao e Ge (2013) apontam a estrutura do design da arquitetura de segurança, a qual divide-se geralmente em três camadas: *Perception Layer, Network Layer* e *Application Layer* e uma nova proposta de arquitetura genérica de Farooq et al. (2015) apresenta quatro camadas.

Já os autores Kahan et al. (2016) propõem um modelo com cinco camadas, que são descritos a seguir, destacando o papel de cada camada e o que motivou a criação de novas camadas a partir do modelo genérico de três camadas.

- **Camada de Percepção:** esta camada funciona como os cinco órgãos dos sentidos da IoT, com a principal tarefa de identificar e coletar informações. A *Perception Layer* inclui leitores de etiquetas de código de barra 2D, RFID, Câmera, GPS, sensores, terminais e sensores de rede.
- **Camada de Rede:** *Network Layer* é como uma rede neural e cerebral da IoT, sua principal função é transmitir e processar informações; devido à vasta quantidade de informações do mundo real que a Camada Perceptiva coleta, é necessário uma certa habilidade com o processamento e gerenciamento de informações.
- **Camada de Aplicação:** a principal tarefa da Camada de Aplicação é processar os dados de forma inteligente, então essa informação processada pode ser utilizada por nós. Desse modo, nós podemos obter informações importantes em real-time, que é a meta de desenvolvimento do IoT.

Quanto aos demais modelos, suas propostas baseiam-se na estrutura acima informada com a inclusão de uma ou mais camadas, abordando e discutindo assuntos com mais profundidade, não deixando essa abordagem a cargo de uma camada apenas. Como exemplo, devido ao grande fluxo de dados que a Camada de Percepção coleta, é muito importante e difícil armazenar essa grande quantidade de dados, pois incluem várias técnicas como, processamento inteligente, *cloud computing*, *ubiquitous computing*. Desta forma, a proposta para a Camada *Middleware* surgiu dessa observação e é descrita a seguir:

- **Camada *Middleware*:** esta camada consiste do sistema de processamento de informação, na qual toma ações automatizadas baseadas nos resultados dos dados processados e conecta o sistema com a base de dados, a qual fornece capacidade de armazenamento para os dados coletados.

A Camada de Negócios foi mencionada nas pesquisas de Kahan et al. (2016) e Wu et al. (2010) visando um desenvolvimento a longo prazo. Sem essa proposta viu-se que o sucesso não depende apenas da prioridade da tecnologia mas da inovação e do modelo de negócio, sendo descrita como se pode observar em seguida:

- **Camada de Negócios:** esta camada é a responsável pela gestão de todo o sistema da IoT, incluindo as aplicações e serviços. Ele constrói modelos de negócio, gráficos, fluxogramas, etc., com base nos dados recebidos da camada de aplicação. Com base na análise dos resultados, esta camada irá ajudar a determinar as futuras ações e estratégias de negócios.

3 PROCEDIMENTOS METODOLÓGICOS

Nesta seção são apresentados os procedimentos metodológicos que norteiam a pesquisa. Esta pesquisa utilizou-se da abordagem qualitativa porque melhor atende aos objetivos do estudo, como também, é uma abordagem apropriada para o entendimento de um fenômeno de natureza social e de caráter interpretativo. Conforme Sandín Esteban.

> Pesquisa qualitativa é uma atividade sistemática orientada à compreensão em profundidade de fenômenos educativos e sociais, à transformação de práticas e cenários socioeducativos, à tomada de decisões e também ao descobrimento e desenvolvimento de um corpo organizado de conhecimentos. (SANDÍN ESTEBAN, 2010, p. 127).

De acordo com Minayo (2000, p. 21) a abordagem qualitativa ainda preocupa-se com um grau de realidade que não pode ser aferido, aos "[...] significados, motivos, aspirações, crenças, valores e atitudes, o que corresponde a um espaço mais profundo das relações, dos processos e dos fenômenos que não podem ser reduzidos à operacionalização de variáveis".

Corroborando acerca da abordagem qualitativa, Strauss e Cobin defendem:

> Que a pesquisa qualitativa produz resultados não alcançados através de procedimentos estatísticos ou de outros meios de quantificação, principalmente, quando se quer retratar experiências vividas, comportamentos, emoções e sentimentos. No entanto, ainda segundo os autores, numa pesquisa qualitativa alguns dados podem ser quantificados, mas o grosso da análise é interpretativa (STRAUSS; COBIN, 2008, p.23).

No âmbito da abordagem qualitativa, foram realizados os métodos: a) levantamento documental e bibliográfica e b) análise de cenário prospectivo.

Nesse sentido, Ludke e André (2007) ensinam que o levantamento bibliográfico pode se tornar uma técnica valiosa de abordagens qualitativas, primeiramente, em virtude da mesma conter as informações obtidas através de outras técnicas e, em segundo lugar, por que desvela aspectos novos de um tema ou problema.

Segundo Oliveira (2010, p. 69), "a principal finalidade da pesquisa bibliográfica é levar o pesquisador a entrar em contato direto com as obras, artigos ou documentos que tratam do tema em estudo". Nesse sentido, Gil (2010, p. 44) aponta que "a pesquisa bibliográfica é elaborada com base em material já publicado. Tradicionalmente, esta modalidade de pesquisa inclui material impresso como livros, revistas, jornais, teses, dissertações e anais de eventos científicos".

É válido aqui fazer inferências acerca dos métodos e técnicas utilizados para prospecção de futuro. Existem os métodos formais, informais e quantitativos, sendo os

métodos formais as entrevistas estruturadas, análises morfológicas, discussões organizadas sobre questões predeterminadas, Delphi, análise de impactos cruzados, construção e análise de cenários (CARDOSO et al., 2005). A importância de se trabalhar com cenários, é porque permitem "estimular a imaginação, reduzir as incoerências, criar uma linguagem comum e permitir a reflexão" (VALDEZ, 2007).

Particularmente, o método de cenários mereceu mais destaque entre aqueles desenvolvidos para auxiliar a reflexão estratégica e prospectiva. No seu sentido mais amplo, é uma ferramenta útil para análise prospectiva, o que por sua vez é de grande valia no processo de tomada de decisões.

De acordo com Sardenberg apud Grumbach (2002, p.12),

> Os estudos prospectivos são, com efeito, um mecanismo eficiente de planejamento, identificação de oportunidades e definição de ações. Devemos considerar a prospecção um processo continuado de pensar o futuro e de identificar elementos para a melhor tomada de decisão, levando em consideração aspectos econômicos, sociais, ambientais, científicos e tecnológicos. Não se trata, pois, de explorar faculdades divinatórias. Cenários não são predições sobre o que irá a acontecer. A premissa é de que o futuro não está, em larga margem, predeterminado e, portanto, pode ser moldado pela ação dos atores sociais.

Nesta pesquisa foi analisado o cenário de uso da IoT no âmbito educacional no Centro de Educação Professor Paulo Freire em Vitória da Conquista - BA por meio de utilização de etiquetas RFID para monitoramento da evasão escolar através do registro automático de entrada e saída dos alunos em alinhamento com os dispositivos de telefonia móvel dos pais que recebiam as devidas notificações dos registros.

No presente trabalho busca-se discutir sobre a Internet das Coisas: segurança, privacidade, interoperabilidade e padrões, regulamentação e legislação e aplicação pública ligadas ao desenvolvimento social. Conforme orientação do Programa de Pós-Graduação em Engenharia de produção da Universidade Paulista – UNIP, este trabalho é estruturado no formato de Dissertação por artigos.

O capítulo de Resultados e Discussões foi apresentado em forma de artigos, contemplando quatro artigos científicos que seguem o formato original de acordo com a publicação a qual foram submetidos e aprovados. O quarto artigo cujo título é "Análise de cenários prospectivos de aplicação de Internet das Coisas no âmbito educacional" ainda será submetido à revista científica.

O primeiro artigo foi elaborado com base em um levantamento de pesquisa bibliográfica e dados sobre a Internet das Coisas e potencialidades para a gestão. O referido

artigo explanou sobre o uso da Internet como meio de comunicação entre as pessoas, ressaltando sua forma mais avançada que chegou e estabelecendo a comunicação entre objetos e equipamentos eletrônicos capazes de processar dados e retornar informações aos seus usuários, a definida Internet das Coisas. Tem como objetivo de verificar a utilização da Internet das Coisas em sua efetividade para a gestão pública no gerenciamento e enfretamento dos problemas sociais. O estudo mostrou que a aplicação da Internet das Coisas já está presente no cotidiano das pessoas e a crescente utilização desta ferramenta pode trazer significativa contribuição para o gestor público melhorar suas práticas internas e a vida dos cidadãos, acelerando respostas e poupando ou gerando recursos.

O segundo artigo trata de uma avaliação comparativa de instrumentos regulatórios que analisa que a Internet das Coisas ainda é uma novidade e que sua utilização passa por um período de incerteza por não haver uma regulamentação no Brasil para seu funcionamento. O referido estudo apresentou como objetivo proposto realizar uma análise comparativa dos instrumentos regulatórios da IoT vigentes em países chaves do mundo com o que já existe e/ou está sendo trabalhado no Brasil, de forma a identificar barreiras burocráticas e se a proposta regulatória contempla a realidade mundial. Os resultados permitiram verificar que o Governo Federal já estuda a criação de um Plano Nacional da Internet das Coisas em busca da padronização, por meio de três etapas: normalização dentro do mercado, largura de banda e segurança de dados, temáticas essenciais voltadas para privacidade, segurança e direitos do consumidor, os quais, legalmente são assegurados pelo Marco Civil da Internet (Lei nº 12.965/2014).

O terceiro artigo aborda o estado da arte das propostas da arquitetura para IoT usada na educação, apontando que a Internet das Coisas permite captar, processar, armazenar e aplicar de maneira direta todos os dados gerados no dia a dia de maneira expansiva, gerenciados como um negócio. As etapas nas quais as informações se movimentam são chamadas de camadas, as aplicações mais comuns são: de percepção, de rede, de middleware, de aplicação, com estudos mais recentes apontando para uma quinta camada, referente à gerência das informações, a camada de negócios. O estudo referido teve como objetivo analisar o estado das artes propostas na arquitetura de segurança como sugestão de modelo de referência para ser adotado no Brasil de maneira a se adequar à realidade internacional. Com isso, chegou-se à conclusão de que o modelo de protocolo de arquitetura de segurança em cinco camadas deve ser adotado no Brasil a fim de se obter interoperabilidade entre os dispositivos na IoT, garantindo uma maior segurança dos dados, sejam eles em qualquer

camada que esteja sendo tratados, atendendo assim a realidade do cenário internacional e gerando intercomunicação onde quer que seja adotado.

O quarto artigo possui como objetivo central a análise dos cenários prospectivos de aplicação da Internet das Coisas no âmbito educacional brasileiro, por meio de um estudo de caso em uma escola em Vitória da Conquista - BA. Tal aplicação ocorreu mediante o monitoramento da entrada e saída dos alunos do Centro Municipal de Educação Professor Paulo Freire, que se daria por meio de etiquetas RFID colocadas no uniforme dos alunos, buscando a redução da evasão escolar por meio do controle da família, que recebia as informações diretamente no celular. O projeto, embora bastante promissor, apresentou controvérsias entre pedagogos, psicólogos, jornalistas, intelectuais, pais e alunos, além de falhas no sistema de operação e durabilidade das etiquetas. Apesar disso, compreende-se que a Internet das Coisas é um campo promissor nos cenários prospectivos de sua aplicação inclusive no âmbito educacional.

4 RESULTADOS E DISCUSSÕES

Os resultados e discussões desta dissertação são apresentados a seguir conforme artigos constantes na Tabela 1:

Tabela 1 – Lista de Artigos

ORDENAMENTO	PUBLICAÇÃO	TEMA	CONSTA
Artigo I	SODEBRAS - XXXIV International Sodebras Congress 07 a 09 de dezembro de 2015 – São Paulo – SP	INTERNET DAS COISAS: POTENCIALIDADES PARA A GESTÃO PÚBLICA	Resultados e Discussões
Artigo II	SODEBRAS - XXXIV International Sodebras Congress 07 a 09 de dezembro de 2015 – São Paulo – SP	INTERNET DAS COISAS: UMA AVALIAÇÃO COMPARATIVA DE INSTRUMENTOS REGULATÓRIOS	Resultados e Discussões
Artigo III	I Workshop Brasileiro sobre Internet das Coisas na Educação - 24 a 27 de outubro de 2016 – Uberlândia - MG	ESTUDO DA ARTE DAS PROPOSTAS DE ARQUITETURA DE SEGURANÇA PARA IoT.	Resultados e Discussões
Artigo IV	Não publicado	ANÁLISE DE CENÁRIO PROSPECTIVO DE APLICAÇÃO DA INTERNET DAS COISAS NO ÂMBITO EDUCACIONAL BRASILEIRO.	Resultados e Discussões

Fonte: O autor (2016).

4.1 Artigo I - INTERNET DAS COISAS: POTENCIALIDADES PARA A GESTÃO PÚBLICA

Esta seção apresenta o primeiro artigo intitulado de "Internet das Coisas: Potencialidades para a Gestão Pública", aprovado e apresentado no XXXIV International Sodebras Congress – São Paulo - SP – Brasil. O artigo mantém o padrão das configurações originais da Revista em que foi submetido

XXXIV International Sodebras Congress
07 a 09 de dezembro de 2015 – São Paulo – SP

INTERNET DAS COISAS: POTENCIALIDADES PARA A GESTÃO PÚBLICA

ALAN KILSON RIBEIRO ARAÚJO[1,2,3]; DANILO ALVES DO NASCIMENTO [3]; FÁBIO DE ARAÚJO LEITE[1,2]; RODRIGO FRANCO GONÇALVES[1]
1 – UNIVERSIDADE PAULISTA - UNIP/PPGEP; 2 – FACULDADE SANTO AGOSTINHO - FSA; 3 – INSTITUTO FEDERAL DO PIAUÍ - IFPI
alankilson@hotmail.com

***Resumo** - A utilização da internet para a comunicação entre pessoas é uma realidade consolidada, no entanto, a tendência aponta para a comunicação entre objetos e equipamentos eletrônicos capazes de processar dados e retornar informações aos seus usuários, denominada Internet das Coisas (IoT). O presente estudo teve como objetivo verificar a utilização da Internet das Coisas em sua efetividade para a gestão pública no gerenciamento e enfretamento dos problemas sociais. Os procedimentos metodológicos foram delineados pela pesquisa bibliográfica, a partir de uma revisão teórica dos principais conceitos e das diferentes visões sobre o assunto. O estudo mostrou que a aplicação da Internet das Coisas já está presente no dia a dia das pessoas e a crescente utilização desta ferramenta pode trazer significativa contribuição para o gestor público melhorar suas práticas internas e a vida dos cidadãos, acelerando respostas e poupando ou gerando recursos.*

***Palavras-chave:** Internet das Coisas. Efetividade. Gestão Pública.*

I. INTRODUÇÃO

É perceptível o aumento expressivo da utilização de tecnologias no cotidiano das pessoas: celulares, notebooks, tablets e outros. Na maioria dos casos esses dispositivos são conectados à internet possibilitando interação e comunicação entre pessoas em diferentes partes do mundo.

A rapidez na comunicação é uma característica dos tempos de hoje, informações estão disponíveis quase ao mesmo tempo em que acontecem. Toda essa informatização e interconectividade vêm alterando a forma de convívio social.

Até 2003 existiam mais pessoas conectadas à internet que dispositivos, este número veio ser revertido entre 2008 e 2009, onde o número de dispositivos conectados ultrapassou o número de pessoas conectadas à internet. É justamente neste momento que nasce a Internet das Coisas - IoT (EVANS, 2011).

Internet das Coisas vem da sigla IoT (*Internet of things*), é quando os dispositivos ficam conectados à internet e conseguem comunicar-se entre si sem intervenção das pessoas. Neste sentido, Mota e Batista (2013) afirmaram que as comunicações serão concebidas não apenas entre humanos, mas também entre humanos e coisas e entre coisas sem a interação com seres humanos.

A Internet das coisas (IoT) tem como objetivo ligar todos os equipamentos eletrônicos e objetos (coisas) que são usadas no dia a dia à internet com a utilização de redes de sensores, para processar essas informações e retornar benefícios aos seus usuários (BILINSKI, 2014).

Hoje um cidadão pode visualizar a rua da sua casa na tela do kit multimídia do carro, evitando assim uma ação surpresa e um possível assalto na sua chegada. É possível ligar a banheira de hidromassagem e decidir a temperatura do ar condicionado do quarto, mesmo estando no trânsito, voltando do trabalho. Isso é Internet das Coisas e é possível desde que dispositivos estejam conectados à internet.

Ainda neste sentido, Teixeira (2014) afirma que:

> A Internet das Coisas (IoT – Internet of Things) é uma infraestrutura de rede dinâmica e global com capacidades de autoconfiguração, baseada em protocolos de comunicação padronizados e interoperáveis, onde "coisas" físicas e virtuais tem identidades, atributos físicos e personalidades virtuais (TEIXEIRA, p.1, 2014).

Numa rede de Internet das Coisas (IoT), os elementos ou dispositivos que fazem parte desta rede são chamados de Objetos Inteligentes (OI), e é através desses objetos inteligentes que a rede se comunica e a interação entre usuários e "coisas" é efetivada. Os dispositivos ou objetos inteligentes precisam ocupar pouco espaço para que caibam nas "coisas" e também têm de ser baratos e com pouco consumo de energia elétrica. Esses objetos inteligentes, então, correspondem a sistemas computacionais embarcados, projetados para uma função específica (NASCIMENTO, CROCOMO e CANCIAN, 2015).

Na Internet das Coisas: as "coisas", objetos ou dispositivos devem se tornar participantes ativos em processos de negocio, informacionais e sociais, onde serão capazes de interagir e comunicar entre elas mesmas, trocar informações coletadas do ambiente, reagindo autonomamente aos eventos do mundo real, bem como influenciar esse contexto sem intervenção direta das pessoas (TEIXEIRA, 2014).

II. PROCEDIMENTOS

O presente estudo teve como objetivo verificar a utilização da Internet das Coisas e sua efetividade para a gestão pública no gerenciamento e enfretamento dos problemas sociais. A pesquisa adotou a perspectiva qualitativa e os dados foram obtidos através de pesquisa bibliográfica em livros, artigos, dissertações e teses.

ISSN 1809-3957

Os procedimentos técnicos foram delineados pela pesquisa bibliográfica, a partir de uma revisão teórica dos principais conceitos e das diferentes visões sobre o assunto.

A Figura 1 retrata o crescimento da população mundial comparando com o número de dispositivos conectados por pessoa. Já existem 3,47 dispositivos conectados por pessoa no mundo em 2015, são aproximadamente 25 bilhões de aparelhos, objetos ou coisas conectadas à internet (EVANS, 2011).

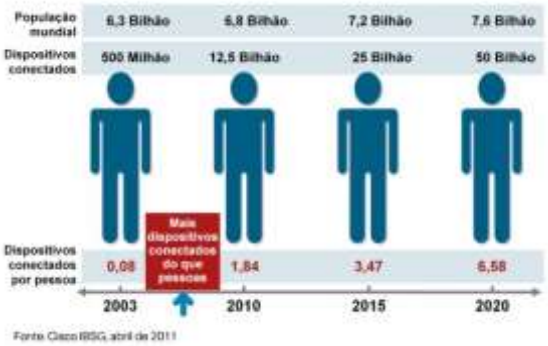


Figura 1 – Relação população por dispositivos conectados por pessoa. Fonte: EVANS, 2011.

Este número expressivo ao mesmo tempo em que facilita a comunicação e abre portas ao empreendedorismo, também cria problemas como o direito à privacidade da pessoa humana e outros. Ainda em relação à figura 1, está previsto que até 2020 o número de dispositivos conectados por pessoa dobre, chegando à marca de 50 bilhões de dispositivos, coisas ou objetos conectados à rede mundial de computadores.

A internet das coisas pode e deve ser utilizada para amenizar a falta de recursos no planeta, sistemas tecnológicos sustentáveis devem ser criados para auxiliar na redução de custos e insumos (água, energia e combustíveis).

Um fluxo contínuo e volumoso de dados poderá ser organizado, armazenado e manipulado a fim de gerar serviços de maior valor ao cidadão. Esse é o conceito do "Big Data". Os governos podem utilizar essa base de dados dinâmica e atualizada constantemente sobre a população para extrair informações e definir as suas políticas de saúde, trânsito, educação, etc. (PRODESP, 2012).

No agronegócio, sensores de rastreamento para o gado, que permitem aos pecuaristas monitorarem a saúde dos animais e acompanharem seus movimentos, garantindo um aumento na produção e na qualidade do alimento, que se torna mais saudável para o consumo (CIOLA, 2014).

Além disso, a Internet das coisas está se expandindo para locais que até agora eram inatingíveis. Pacientes estão ingerindo dispositivos conectados em seus próprios corpos para ajudar médicos a diagnosticar e determinar as causas de determinadas doenças. Sensores muito pequenos podem ser colocados em plantas, animais, bem como em recursos geológicos e, em seguida, serem conectados à Internet (EVANS, 2011).

Este estudo teve como objetivo detectar a parcela de contribuição da Internet das Coisas para o gerenciamento e enfrentamento dos problemas sociais, como a gestão pública pode se utilizar destes sistemas para efetivar políticas públicas que venham a melhorar e facilitar a vida das pessoas.

III. RESULTADOS

São muitas as áreas onde a Internet das Coisas pode intervir: Educação, saúde, logística, ambiental, segurança, mobilidade urbana, sustentabilidade e etc. O presente estudo buscou exemplos de iniciativas já colocadas em prática no Brasil.

A tecnologia por trás da Internet das coisas pode ser aplicada em uma série de situações, inclusive na manufatura, logística e distribuição, proporcionando mais visibilidade, rastreamento e sincronização de cadeia de suprimentos, com total segurança. Dessa forma, tal aplicabilidade mostra-se relevante, quando por sua vez, essa implementação ocorre também na área de segurança (HESSEL, 2011).

Uma das áreas que mais preocupam os gestores brasileiros é a segurança pública, são crescentes os índices de violência em todo país. Especialistas afirmam que só a repressão não soluciona o problema, é preciso que a polícia seja aparelhada e tenha um forte serviço de inteligência, neste exato momento se faz necessária a tecnologia da Internet das Coisas.

Na Copa das Confederações o governo utilizou o caminhão CiCCM (Centro integrado de Comando e Controle Móvel). Trata-se de um veículo equipado com computadores de última geração, servidores, câmeras de vídeo, telas, sistema de captação de áudio e softwares de integração e análise de dados. O CiCCM é integrado às polícias civil, militar, federal, Bombeiros e SAMU, e pode identificar desde carros estacionados de forma irregular à venda de produtos piratas, ou mesmo evitar ataques terroristas e tumultos em geral (BARCELLOS, 2013).

Ainda nas áreas de segurança pública e mobilidade urbana, os chamados ITS (Intelligent Transportation Systems) utilizam recursos avançados de informática no sistema de transporte para reorganizar e monitorar o trânsito, além de fornecer informações aos motoristas. O ITS possui sensores e câmeras que contam a quantidade de veículos em movimento e identificam carros em direção perigosa, gerando um alarme para os agentes de trânsito. Esse sistema já se encontra em operação no Túnel Rebouças, no Rio de Janeiro (BARCELLOS, 2013).

Figura 2 – Centro integrado de Comando e Controle Móvel utilizado na copa das confederações. Fonte: BARCELLOS, 2013.

ISSN 1809-3957

Na educação do município de Vitória da Conquista, no interior da Bahia, etiquetas de rádio frequência instaladas nos uniformes escolares monitoram mais de 20 mil estudantes do ensino básico da rede municipal de educação. As etiquetas tem o objetivo de registrar a entrada dos estudantes na escola e, em caso de falta, autorizar o envio de mensagens SMS para os celulares dos pais dos alunos ausentes (SINGER, 2012).

Figura 3 – Uniforme com chip da Rede Municipal de Educação do Município de Vitória da Conquista. Fonte: FERREIRA, 2012.

O Governo Federal estuda a criação de um Plano Nacional de Comunicação entre Máquinas (M2M *Machine to Machine*) e Internet das Coisas. Entre os objetivos estão o fomento à padronização de sistemas de IoT; a criação de uma regulamentação para tratar de temas como privacidade, segurança e direitos do consumidor em serviços de IoT; o lançamento de programas de financiamento de soluções de IoT, provavelmente com recursos do Funttel; e o estímulo à adoção de soluções de IoT pelo setor público (PAIVA, 2015).

Em Santo Amaro, distrito da zona sul da cidade de São Paulo, são instalados dispositivos de transmissão de dados ao lado do hidrômetro do imóvel, a transmissão de dados é feita ininterruptamente, 24 horas por dia, sete dias por semana. Dessa maneira, o consumidor pode acompanhar seu consumo de água em tempo real, o sistema traz ainda outras vantagens, como visualização das informações em gráficos e tabelas e envio de alerta pré-configurável no e-mail ou celular em caso de alteração no padrão de consumo. O acesso é controlado por senha, garantindo a segurança e a confiabilidade das informações (FECOMERCIO, 2010).

IV. CONCLUSÃO

A partir dos resultados desse estudo, ficou bastante clara a influência da tecnologia nos dias de hoje e como ela pode ser melhor utilizada. A Internet das Coisas está presente no dia a dia das pessoas, mas sistemas mais integrados são necessários para produzir um número cada vez maior de informações e benefícios.

Conclui-se dessa forma que a Internet das Coisas (IoT) pode sim contribuir de forma efetiva para o enfretamento das demandas e problemas sociais. Os resultados mostraram vários exemplos sucedidos onde tal tecnologia foi empregada poupando recursos humanos e acelerando respostas.

V. REFERÊNCIAS BIBLIOGRÁFICAS

BARCELLOS, Marco. **A Internet de Todas as Coisas já está chegando ao Brasil**. Canaltech. Disponível em: http://corporate.canaltech.com.br/coluna/internet/A-Internet-de-Todas-as-Coisas-ja-esta-chegando-ao-Brasil/. Acesso em 02.09.2013

BILINSKI, Fernando Rodrigo. **Internet das coisas.** Curitiba, 2014. Disponível em: http://www.inf.ufpr.br/aldri/disc/artigos/2014/fernando_f1.pdf. Acesso em 10.09.2015.

CIOLA, Felipe. **Boletim Internet das Coisas**. Sebrae, 2014. Disponível em: http://www.sebrae2014.com.br/Sebrae/Sebrae%202014/Boletins/2014_08_13_BO_Julho_TIC_InternetdasCoisas_pdf.pdf. Acesso em 09.10.2015.

EVANS, Dave. **A Internet das Coisas Como a próxima evolução da Internet está mudando tudo**. Cisco Internet Business Solutions Group (IBSG). 2011. Disponível em: http://www.cisco.com/web/BR/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf. Acesso em 15 out 2015.

FECOMERCIO. **O Uso Racional da Água no Comércio.** São Paulo, 2010. Disponível em: http://site.sabesp.com.br/uploads/file/asabesp_doctos/cartilha_fecomercio.pdf. Acesso em: 12.10.2015.

FERREIRA, Porto. **Vitória da Conquista vai monitorar presença em aula através de chip em uniforme**. 2012. Disponível em: http://www.portoferreirahoje.com.br/noticia/2012/03/27/vitoria-da-conquista-vai-monitorar-presenca-em-aula-atraves-de-chip-em-uniforme/.Acesso em 18.10.2015.

HESSEL, Fabian et al. **Implementando RFID na cadeia de negócios: Tecnologia a Serviço da Excelência.** Porto Alegre, 2011.

MOTA, Rafael Perazzo Barbosa; BATISTA, Daniel Macedo. **Um mecanismo para garantia de QoS na Internet das Coisas com RFID**. São Paulo, 2013. Disponível em: http://ccsl.ime.usp.br/files/sbrc_artigo.pdf. Acesso em 13.09.2015.

NASCIMENTO, Ercílio G.; CROCOMO, Bruno M.; CANCIAN, Rafael L. **Geração Automática de GUIs para Objetos Inteligentes em Dispositivos Móveis.** Florianópolis, 2015. Disponível em: http://siaiweb06.univali.br/seer/index.php/acotb/article/view/7035. Acesso em 18.10.2015.

PAIVA, Fernando. **Governo Federal estuda criação de Plano Nacional da Internet das** Coisas. Brasília, 2015. Disponível em: http://convergecom.com.br/teletime/23/06/2015/governo-federal-estuda-criacao-de-plano-nacional-da-internet-das-coisas-2/. Acesso em 14.10.2015.

ISSN 1809-3957

PRODESP. **Informativo Tecnológico da Prodesp**. 4ª edição. Outubro de 2012, Disponível em: http://www.prodesp.sp.gov.br/clientes/pdf_tendencias/INFORMATIVO_TENDENCIAS_OUT_2012.pdf. Acesso em 09.10.2015.

SINGER, Talyta. **Tudo Conectado: Conceitos e Representações da Internet das Coisas**. Simpósio em Tecnologias Digitais e Sociabilidade. Salvador, 2012. Disponível em: http://gitsufba.net/anais/wp-content/uploads/2013/09/n1_tudo_44965.pdf. Acesso em 19.10.2015.

TEIXEIRA, Fernando A. et al. **Siot: defendendo a internet das coisas contra exploits**. Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC), Florianópolis, 2014. Disponível em: http://sbrc2014.ufsc.br/anais/files/trilha/ST14-1.pdf. Acesso em 13.09.2015.

VI. COPYRIGHT

ISSN 1809-3957

4.2 Artigo II - INTERNET DAS COISAS: UMA AVALIAÇÃO COMPARATIVA DE INSTRUMENTOS REGULATÓRIOS

Esta seção apresenta o segundo artigo intitulado de "Internet das Coisas: Uma Avaliação Comparativa de Instrumentos Regulatórios", aprovado e apresentado no XXXIV International Sodebras Congress – São Paulo - SP – Brasil. O artigo mantém o padrão das configurações originais da Revista em que foi submetido.

XXXIV International Sodebras Congress
07 a 09 de dezembro de 2015 – São Paulo - SP

INTERNET DAS COISAS: UMA AVALIAÇÃO COMPARATIVA DE INSTRUMENTOS REGULATÓRIOS

ALAN KILSON RIBEIRO ARAÚJO[1,2,3]; FÁBIO DE ARAÚJO LEITE[1,2]; DANILO ALVES DO NASCIMENTO [3]; RODRIGO FRANCO GONÇALVES[1]
1 – UNIVERSIDADE PAULISTA - UNIP/PPGEP; 2 – FACULDADE SANTO AGOSTINHO - FSA;
3 – INSTITUTO FEDERAL DO PIAUÍ - IFPI
alankilson@hotmail.com

Resumo** - A Internet das Coisas (IoT) é considerada ainda uma novidade e sua utilização atravessa um período de incerteza por não haver uma regulamentação no Brasil para padronização do seu funcionamento. Em face desta problemática, este estudo objetiva realizar uma análise comparativa dos instrumentos regulatórios da IoT vigentes em países chaves do mundo com o que já existe e ou está sendo trabalhado no Brasil, de forma a identificar barreiras burocráticas e se a proposta regulatória contempla a realidade mundial. Os procedimentos metodológicos basearam-se em revisão bibliográfica. Assim, foi analisado que o Governo Federal já estuda a criação de um Plano Nacional da Internet das Coisas em busca da tão esperada padronização, por meio de três etapas: normalização dentro do mercado, largura de banda e segurança de dados, temáticas essenciais voltadas para privacidade, segurança e direitos do consumidor, os quais, legalmente são assegurados pelo Marco Civil da Internet (Lei nº 12.965/2014).

Palavras-chave:** Internet das Coisas. Regulamentação. Padronização.

I. INTRODUÇÃO

A Internet das Coisas, ou, em inglês, Internet of Things (IoT) é algo relativamente novo que se acreditava tratar de um novo tipo de Internet, contudo, abrange uma maneira diferente de utilizá-la com uma menor intervenção do homem, uma vez que não é exigida uma pessoa em frente a máquina. A IoT provém de uma rede formada com todos os tipo de coisas (sejam animados ou inanimados) conectadas e trocando informações constantemente pela internet.

Neste sentido Maeda (2015) explica que:

> A Internet das Coisas nada mais é do que a continuação do movimento de digitalização, de transformação digital. É a internet entrando no mundo físico, conectando todas as coisas. (MAEDA, F. C.,2015).

O termo surgiu em 1999 durante uma palestra na Procter & Gamble (P&G) por meio do executivo Kevin Ashton que pesquisava formas de gerenciamento logístico dos produtos da empresa através de uma conexão das embalagens com a Internet, de tal forma a saber a localização exata de um produto desde sua saída da fábrica até seu consumidor final, surgindo assim, uma parceria para pesquisa com o Massachusstts Institute of Technology (MIT), onde foi desenvolvida a tecnologia das etiquetas RFID (identificação por rádio-frequência), aplicada nos produtos que respondem ou enviam sinais que são lidos por uma base (ASHTON, 2009).

Em 2008, foi publicado The Internet of Things de Rob Van Kranenburg, livro abordando um novo paradigma no qual objetos produzem informação, abrangendo questões sobre os ambientes que processam informação de forma autônoma, levando em consideração preocupações sobre a vigilâncias que as coisas conectadas podem exercer e a necessidade de se apropriar dessa tecnologia, tornando-se assim uma das maiores referências quando se trata de IoT (KRANENBURG, 2008). A Figura 1 representa os termos envolvidos quando se trata de IoT.

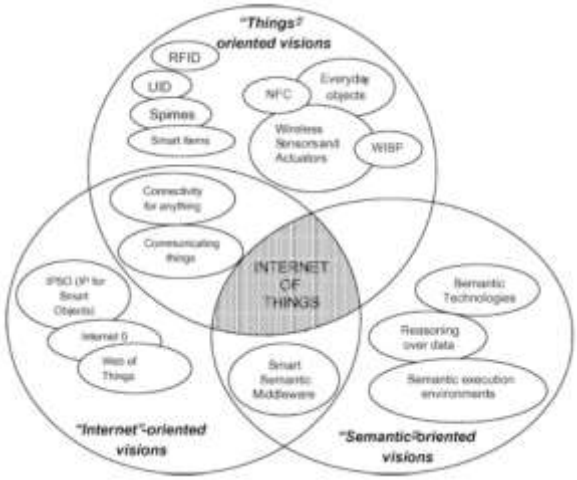


Figura 1: O paradigma da Internet das Coisas. Fonte: ATZORI (et al, 2010, p.2).

Dezesseis anos depois, podemos dizer que as possibilidades de utilização da IoT são infinitas por conta da constante interação e da imensa troca de dados (MAEDA, F. C.,2015). Uma geladeira, por exemplo, pode identificar a falta de algum produto e sinalizar o fornecedor para a realização do devido abastecimento, assim como smartphones solicitando táxis por meio de aplicativos ou máquinas solicitando assistência técnica automaticamente.

Ainda neste sentido Maeda (2015) afirma que:

ISSN 1809-3957

> No consumo, as maiores mudanças estarão nos "wearables" (tecnologias vestíveis), na casa e nos carros conectados. Coisas que vão aumentar a conveniência, facilitar a vida das pessoas. Com as coisas conectadas, vamos ter perfis muito claros dos clientes. Saber exatamente o que querem, como usam os produtos, que tipo de café prefere etc. (MAEDA, F. C., 2015).

A utilização da IoT ainda atravessa um período de incerteza, por falta de estrutura e de uma regulamentação que padronize seu funcionamento. Para que a IoT realmente funcione é necessário que as coisas tenham de fato acesso à Internet, independente do tipo de conexão e também que elas se comunique em uma linguagem padronizada ou regulamentada (CANALTECH, 2014). Outro aspecto também importante a mencionar, trata-se da privacidade, uma vez que tantos acessos aos dados e necessidades dos usuários podem gerar cenário de insegurança. A Figura 2 representa a utilização da IoT em residências.

Figura 2: Modelo Internet das Coisas implementado em casas.
Fonte: INNOVATION, 2015

II. PROCEDIMENTOS

Este trabalho tem como objetivo realizar uma análise comparativa dos instrumentos regulatórios da IoT vigentes em países chaves do mundo com o que já existe e ou está sendo trabalhado no Brasil, buscando identificar barreiras burocráticas e se a proposta regulatória contempla à realidade mundial.

Com os eventos que colaboraram para criar a Internet das Coisas, podemos observar que pela existência de diferentes significados, novos termo que derivavam de contextos diferentes surgiram: computação ubíqua, machine-to-machine (M2M), web das coisas, internet do futuro e cidades inteligentes (ATZORI et al, 2010; KRANENBURG et al, 2011; UCKELMANN et al, 2011), levando aos questionamentos sobre privacidade e até debates públicos sobre segurança e transparência.

Este aumento das novas tecnologias iniciaram as discussões sobre a criação de padrões internacionais que permitam que a existência de uma rede autônoma de objetos conectados. O ITU (International Telecommunication Union) das Nações Unidas, vem desde o ano de 2011 reunindo especialistas para a criação e consolidação do padrão global, já em março de 2012, a União Europeia realizou uma consulta pública buscando que os cidadãos apresentassem suas necessidades e inseguranças sobre a IoT e em 16 e 17 de junho, Londres sediou a 1ª Open IoT Assembly, onde as pessoas livremente discutiram e colaboraram para a criação de um documento com os princípios de transparência e bom uso das informações na IoT.

O trabalho possui natureza teórica e exploratória, realizada a partir de revisão bibliográfica sobre políticas, programas, regulamentos e leis vigentes, bem como trabalhos relacionados a IoT tanto no âmbito nacional como internacional.III. RESULTADOS

A Internet, como atual modeladora de costumes e culturas, tem sua importância e usabilidade crescentes, mostrando-se assim a importância de legislação específica que garanta não apenas o combate a cibercrimes, mas também a proteção, direitos e deveres de seus usuários e provedores, e estimule o compartilhamento de ideias e capital intelectual.

De acordo com Segurado (et al, 2014), existem três categorias fundamentais para análise na regulamentação da Internet, sendo elas a Neutralidade de rede, que pressupõe que todas as informações devem ser tratadas de forma isonômica, o Direito à privacidade dos cidadãos internautas e as questões relacionadas à vigilância e à segurança, e, por último, a Discussão dos direitos autorais sob a lógica da propriedade intelectual; para a padronização da Internet das Coisas, mais especificamente, serão necessárias três etapas: normalização dentro do mercado, largura de banda larga e segurança de dados. No Reino Unido, a Ofcom (Office of Communications), agência reguladora de comunicações do Reino Unido, realizou uma consulta pública para basear suas medidas visando investimento e pesquisa nos sistemas de IoT, principalmente nos quesitos de definição, demanda espectral, protocolos e segurança – sendo o último o que recebe mais ênfase devido a quantidade de informações que podem ser armazenadas e manuseadas por um sistema IoT (MOBILE, 2014).

São exatamente os critérios de segurança e privacidade que geram preocupação e resistência nos usuários: em um estudo feito pela F-Secure, 80% dos entrevistados tinham receio quanto o ataque de hackers às informações armazenadas nos dispositivos inteligentes, enquanto 79% estavam preocupados com sua privacidade (ABRANET, 2015). Justificando essa preocupação tem-se o caso Ashley Madison, em que usuários de um site de relacionamentos extraconjugais tiveram suas contas hackeadas e os invasores ameaçaram divulgar suas informações. Esse é apenas um caso de roubo de dados, mas se torna mais preocupante quando relacionado à IoT devido o controle e integração de objetos entre si: usando um sistema que usa a rede de celular, pesquisadores puderam tomar controle do sistema de entretenimento de um carro e reescrever o firmware (instruções operacionais programadas diretamente no hardware de um equipamento eletrônico) para enviar comandos a sistemas críticos, como freio, volante e transmissão (ESTES, 2015).

Alguns países são modelos quanto às atitudes relacionadas à regulamentação dessa ferramenta; listados abaixo estão alguns deles e as medidas tomadas abrangendo essa temática:

ISSN 1809-3957

a. Estados Unidos:

Após os ataques de 11 de Setembro de 2001, os Estados Unidos aumentaram a vigilância e a rigidez relacionadas ao tráfico de informações nacionais e internacionais – fato que gerou inimizades com outros países depois das denúncias de espionagem feitas por Edward Snowden.

CALEA (Communications for Law Enforcement Act): 1994 – lei de auxílio das comunicações para a aplicação do direito; ampliou a capacidade de vigilância das agências do Estado de modo que as operadoras de telefonia e os fabricantes projetassem seu equipamento para facilitar a instalação de grampos.

FISA (Foreign Intelligence Surveillance): 1978 – lei de vigilância de inteligência estrangeira; regras de vigilância com o intuito de recolher informações de potências e agentes estrangeiros, incluindo cidadãos americanos.

Patriotic Act ("Lei Patriota"): 2011 – lei que rege as investigações secretas.

b. Brasil:

Assumindo um papel de importância, o Brasil aprovou a lei chamada de Marco Civil da Internet, consolidando a posição de país que apoia e exerce a democracia:

MCI (Marco Civil da Internet) – Lei 12.965 de 2014: Princípios, direitos e deveres para internautas e provedores no país.

De acordo com Segurado (et al, 2014):

> O Marco Civil da Internet é uma iniciativa da Secretaria de Assuntos Legislativos do Ministério da Justiça em parceria com o Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas (FGV) do Rio de Janeiro. Trata-se da primeira proposta de marco civil do mundo, uma espécie de "constituição da internet" que regulamenta direitos, deveres e garantias do uso da rede de computadores no país. O principal objetivo é garantir os interesses dos usuários e promover a cidadania. Por essa razão, foi elaborado de forma colaborativa com a participação de diversos segmentos da sociedade civil (SEGURADO, p. 10, 2014).

Lei 12.737/2012 – Apelidada de "Lei Carolina Dieckmann", dispõe sobre a tipificação criminal dos delitos informáticos, como a invasão de dispositivo informático, a interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou informação de utilidade pública, a falsificação de documento particular e a falsificação de cartão.

c. Espanha:

A lei que teve como contexto os desdobramentos da crise financeira, conhecida como Lei Sinde-Wert. Foi promulgada em 2010, mas entrou em vigor apenas em 2012, permite o fechamento de sites sem a necessidade de uma ordem judicial, com o objetivo de se opor à pirataria.

d. Reino Unido:

A Ofcom (Office of Communications), agência reguladora de comunicações do Reino Unido, realizou uma consulta pública para basear suas medidas visando investimento e pesquisa nos sistemas de IoT, principalmente nos quesitos de definição, demanda espectral, protocolos e segurança – sendo o último o que recebe mais ênfase devido a quantidade de informações que podem ser armazenadas e manuseadas por um sistema IoT (MOBILE, 2014).

Vale ressaltar ainda que a aplicabilidade da tecnologia de Internet das Coisas abrange mais do que aumentar o conforto e praticidade no dia-a-dia dos usuários, sendo que pesquisas apontam a usabilidade das IoT no auxílio e cuidado de idosos e pacientes.

Segundo José Bruzadin (2015), diretor de Desenvolvimento de Mercado da Intel Pró-Saúde para a América Latina:

> "O grande beneficiário das tecnologias da Internet das Coisas, sem dúvida, será a saúde. E a Intel já estuda três áreas para usar: na telemedicina; no monitoramento de pacientes em casa; e na mudança de hábitos – me referindo ao incentivo das pessoas mudarem para hábitos mais saudáveis, usando objetos ligados à internet que auxiliem, por exemplo, em corridas (CIPRIANO, 2015)."

Pesquisa da empresa Internacional Data Corp, o IDC aponta, que a Internet das Coisas pode se tornar uma grande impulsionadora do PIB mundial nos próximos 15 anos, sendo que o Brasil está na 17ª colocação entre os países que dispõem incentivos para o desenvolvimento dessa tecnologia, com os Estados Unidos ocupando o 1º lugar do ranking (IBRACE, 2015). No entanto, para que essa previsão se torne realidade, serão necessários investimentos governamentais e das empresas para ampliar a adoção dessa tecnologia e que as empresas formulem estratégias para o crescimento desse ramo (ITFORUM365, 2015). Para subir de colocação, o Brasil deverá investir em infraestrutura adequada, instituições de pesquisa e mão de obra qualificada, oferecendo também incentivos para que esses profissionais permaneçam no país, evitando o fenômeno *brain drain* (fuga de cérebros).

O ideal é que se aproveite a exploração crescente dos sistemas de Internet das Coisas para a criação de padronização e legislação visando o controle do fornecimento dos serviços, e segurança, direitos e deveres dos usuários, de modo que essas medidas sejam preventivas, e não um método de correção de possíveis falhas de segurança e invasão de privacidade dos usuários dessa ferramenta.

IV. CONCLUSÃO

Por meio da técnica aplicada neste trabalho podemos concluir que os países em desenvolvimento levados em consideração neste estudo estão se mobilizando e também mostram-se bastante preocupados com a questão da padronização e regulamentação da IoT, uma vez que ataques cibernéticos aos produtos detentores desta tecnologia estão cada vez mais comuns e também o aumento do número de empresas trabalhando em dispositivos que utilizam a Internet das Coisas.

A mobilização não ocorre somente do ponto de vista público, mas principalmente do privado, envolvendo

ISSN 1809-3957

organizações cada vez mais preocupadas com os fatores de privacidade e segurança de dados, chegando até formar consórcios na busca pela padronização da IoT, uma delas é a General Eletric, que está liderando o Consórcio de Internet Industrial dos Estados Unidos, temos também na Alemanha, onde existe a chamada Indústria 4.0, iniciativa governamental para fomentar a fabricação de produtos que usam a IoT (CANALTECH, 2014).

Quanto ao Brasil, a IoT ainda é muito simplória, pois exige uma necessidade de superar os obstáculos técnicos, organizacionais e regulatórios, além de se criar e mudar a concepção sobre a Internet das Coisas principalmente quanto ao fator privacidade.

Porém o Governo Federal realiza estudos voltados para a criação de um Plano Nacional de Comunicação entre Máquinas e Internet das Coisas, buscando com isso a sonhada padronização de sistemas de IoT e a criação de uma regulamentação levando em consideração: privacidade, segurança e direitos do consumidor em serviços de IoT (PAIVA, 2015). Dessa forma, se busca promover o desenvolvimento de programas de financiamento de soluções de IoT, com recursos originados provavelmente do Funttel e por consequencia o estímulo à adoção de soluções de IoT pelo setor público. Dessa forma, o Governo irá evitar problemas de interoperabilidade, criados pelo surgimento de ilhas de desenvolvimento de M2M e IoT no Brasil, apresentando e desenvolvendo sistemas que não conversam entre si.

V. REFERÊNCIAS BIBLIOGRÁFICAS

ABRANET, **Internet das Coisas avança, mas aumenta medo dos ataques dos hackers.** Disponível em: <http://www.abranet.org.br/Noticias/Internet-das-Coisas-avanca,-mas-aumenta-medo-dos-ataques-hackers-867.html#.Vi8NidKrRdg>. Acesso em: 17 de outubro de 2015.

ASHTON, Kevin. **That 'Internet of Things' thing**. Publicado no RFID Journal, 2009. Disponível em <http://www.rfidjournal.com/article/view/4986>. Acesso em: 10 outubro de 2015.

ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. **The Internet of Things: a survey**. Computer Networks, 2010.

CANALTECH, **Gartner: Internet das coisas passará por padronização em 2015**. Disponível em: <http://canaltech.com.br/noticia/internet/Gartner-Internet-das-Coisas-passara-por-padronizacao-em-2015/#ixzz3p1uRnZhx>. Acesso em: 17 de outubro de 2015.

CIPRIANO, Leonardo**. Estudo aponta que Internet das Coisas beneficiará principalmente a saúde em 2025.** Publicado no Neitec, disponível em: <http://neitec.com/inovacao-tecnologica/estudo-aponta-que-internet-das-coisas-beneficiara-principalmente-a-saude-em-2025/>. Acesso em: 15 de outubro de 2015.

ESTES, Adam**. Hackers podem controlar quase meio milhão de veículos Chrysler à distância**. Publicado no Gizmodo, disponível em: <http://gizmodo.uol.com.br/hackers-podem-controlar-quase-meio-milhao-de-veiculos-chrysler-a-distancia/>. Acesso em: 10 de outubro de 2015.

IBRACE, **Brasil ocupa 17ª lugar entre os países mais preparados para usar a IoT na indústria.** Disponível em: <http://www.grupoibrace-icbr.org.br/brasil-ocupa-17o-lugar-entre-os-paises-mais-preparados-usar-iot-na-industria/>. Acesso em: 10 de outubro de 2015.

INNOVATION, **Internet das coisas deixará a publicidade muito mais inteligente.** Disponível em: <http://innovationinsider.com.br/internet-das-coisas-deixara-a-publicidade-muito-mais-inteligente/>. Acesso em: 15 de outubro de 2015.

ITFORUM365, **IoT precisa de apoio do governo e empresas para se tornar realidade, diz Accenture.** Disponível em: <http://itforum365.com.br/noticias/detalhe/114844/iot-precisa-do-apoio-do-governo-e-empresas-para-se-tornar-realidade-diz-accenture>. Acesso em: 27 de outubro de 2015.

KRANENBURG, R. **The Internet of Things**: a critique ambient technology and the all-seeing network of RFID. Amsterdã: Institute of Networks Culture, 2008.

KRANENBURG, R.; ANZELMO, E.; BASSI, A.; CAPRIO, D.; DODSON, S.; RATTO, M. **The Internet of Things**. 1st Berlin Symposium on the Internet and Society. Outubro de 2011. Disponível em: <http://www.network cultures.org/uploads/notebook2_theinternetofthings.pdf>. Acesso em 26 jun. 2012.

MAEDA, F. C.. **Verbete Draft: o que é Internet das Coisas no Projeto DRAFT, 2015**.Disponível em: <http://projetodraft.com/verbete-draft-o-que-e-internet-das-coisas/>. Acesso em 09 outubro de 2015.

MOBILE, **Agência do Reino Unido realiza consulta pública para definir IoT**. Disponível em: <http://www.mobiletime.com.br/25/07/2014/agencia-do-reino-unido-realiza-consulta-publica-para-definir-iot/385099/news.aspx>. Acesso em: 24 de outubro de 2015.

PAIVA, Fernando**. Governo Federal estuda criação de Plano Nacional da Internet das Coisas**. Publicado no Convergecom, disponível em: <http://convergecom.com.br/teletime/23/06/2015/governo-federal-estuda-criacao-de-plano-nacional-da-internet-das-coisas-2/>. Acesso em: 17 de outubro de 2015.

UCKELMANN, D; HARRISON, M.; MICHAHELLES, F. (Orgs). **Architecting the Internet of Things**. Springer: Nova Iorque, Dordrecht, Heidelberg, Londres, 2011.

SEGURADO, Rosemary; et al. **Regulamentação da internet: perspectiva comparada entre Brasil, Chile, Espanha, EUA e França**. História, Ciências, Saúde – Manguinhos. Rio de Janeiro. 21 p. 2014.

VI. COPYRIGHT

ISSN 1809-3957

4.3 Artigo III - ESTUDO DA ARTE DAS PROPOSTAS DE ARQUITETURA DE SEGURANÇA PARA IoT USADA NA EDUCAÇÃO

Esta seção apresenta o terceiro artigo intitulado de "Estudo da Arte das Propostas de Arquitetura de Segurança para IoT usada na Educação", que foi aprovado no I Workshop Brasileiro sobre Internet das Coisas na Educação – Uberlândia - MG – Brasil. O artigo mantém o padrão das configurações originais do evento em que foi submetido.

Estudo da Arte das Propostas da Arquitetura de Segurança para IoT usada na Educação

Alan K. R. Araújo[1], Rodrigo F. Gonçalves[1], Guilherme I. R. Silva[2], Ricardo G. Queiroz[2]

[1]Departamento de Pós Graduação em Engenharia de Produção - Universidade Paulista (UNIP) – Campus Indianapolis

Rua Doutor Bacelar, nº 1212 - Vila Clementino, CEP - 04026-002, São Paulo - SP – Brasil

[2]Departamento de Pós Graduação em Redes de Computadores – Faculdade Santo Agostinho (FSA)

Avenida Valter Alencar, nº 665 - São Pedro, CEP - 64019-625, Teresina – PI – Brasil

alankilson@hotmail.com, rofranco@osite.com.br, guilhermisaac@gmail.com, rgqueiroz@gmail.com

Abstract. *The Internet of Things absorbs all the data generated on a daily basis massive way. The present study aimed to carry out a critical analysis of the security architecture in IoT, to be consolidated as a reference model or even as a standard adopted in Brazil in order to suit the international reality. The methodological procedures were outlined by literature from a theoretical review. The study concluded that the model of security architecture protocol in five layers should be adopted in Brazil to obtain interoperability between devices in the IoT, ensuring greater data security, thus meeting the international scene and generating intercommunication wherever it is adopted.*

Resumo. *A Internet das Coisas absorve todos os dados gerados no dia a dia de maneira massiva. O estudo apresentado teve como objetivo realizar uma análise crítica da arquitetura de segurança em IoT, para serem consolidadas como um modelo de referência ou mesmo como um padrão adotado no Brasil de maneira a se adequar a realidade internacional. Os procedimentos metodológicos foram delineados pela pesquisa bibliográfica. O estudo concluiu que o modelo de protocolo de arquitetura de segurança em cinco de camadas deve ser adotado no Brasil fim de se obter interoperabilidade entre os dispositivos na IoT, garantindo uma maior segurança dos dados, atendendo o cenário internacional e gerando intercomunicação onde quer que seja adotado.*

1. Introdução

O ambiente que nos cerca está saturado com informações (temperatura, umidade, presença, códigos de barra, sons etc.) que podem ou não ser lidas, interpretadas, utilizadas e armazenadas. A presença de sensores capazes de lerem tais informações, os protocolos utilizados na intercomunicação e no que as informações obtidas podem implicar são a área de estudo que compõem a noção de IoT (Internet of Things).

O termo Internet das Coisas (IoT) está entre os tópicos mais discutidos no meio acadêmico de tecnologia da última década. Com uma proposta de ser uma rede ubíqua, que pode ser acessada "a qualquer hora, em qualquer lugar, por qualquer um e qualquer coisa" [Itu, 2005]. Interconectando dispositivos entre si e esses tendo, com base em dados colhidos por sensores equipados com: Identificação de Rádio Frequência (RFID), sensores de infravermelho, leitores de código de barras, etc., sendo esses dados inteligentemente processados, tornando-se assim dispositivos inteligentes capazes de captar e tomar decisões sem interferência humana, abrindo portas para uma nova era da computação.

Sensores, câmeras, smartphones, cada um com peculiaridades na operação, captação e transmissão de dados são os componentes da IoT. A padronização da maneira com que os dados obtidos serão processados, transmitidos, utilizados e armazenados, além do aumento da eficiência no uso de recursos (bateria, processamento e banda de dados) é o foco dos estudos realizados em diferentes centros tecnológicos, que acaba por criar protocolos de comunicação e propostas de arquiteturas dissonantes.

No que diz respeito ao design da arquitetura de segurança e que vem sendo muito discutida na literatura, tem surgido diversas propostas. A estrutura é dividida geralmente em três camadas, que é composta como segue: Camada de Percepção, Camada de Rede e Camada de Aplicação [Zhao; Ge, 2013]. Uma nova proposta de arquitetura genérica com quatro camadas foi adotada, incluindo a Camada de Middleware [Farooq; Waseem; Khairi; Mazhar, 2015]. Já a literatura mais atual [Rafiullah; Sarmad; Zaheer; Khan, 2012] propõe um modelo com cinco camadas, incluindo a Camada de Negócios ao modelo de quatro camadas. Na figura abaixo é possível conferir o layout de cada um dos modelos mencionados acima oriundos do modelo genérico de três camadas.

Figura 01 – Layout Modelos de Camadas de Segurança IoT.

Fonte: O autor (2016).

A utilização de dados obtidos de maneira massiva com sensores pode ser feita em diferentes áreas do conhecimento, através da utilização de sistemas especialistas que interpretam os dados obtidos, gerando resultados úteis e de grande valor em diversas áreas do conhecimento, como planejamento de sistemas de transporte ou estimativas em sistemas logísticos.

2. Procedimentos Metodológicos

Por não haver apenas um modelo de referência, um estudo crítico dos trabalhos existentes e o levantamento das falhas nas camadas estudadas (Percepção, Rede, Middleware, Aplicação e Negócios) se faz necessário, assim como a proporção de soluções para as falhas identificadas e aperfeiçoamentos referentes a sua utilização na educação.

Através desse estudo bibliográfico das propostas em estado da arte, pode-se restringir as informações de maior valor e direcioná-las a aplicações otimizadas ao cenário brasileiro, permitindo uma padronização que preza pela eficiência, considerando as características, problemas e peculiaridades do nosso território.

Dentre os modelos levantados, foi adotado o de cinco camadas, pois verificou-se que este atende a maioria das menções acima citadas. Sendo as camadas distribuídas de uma forma que cada uma delas fica mais evidenciada em relação aos outros modelos de três e quatro níveis, brevemente mencionados, além de inseridas novas propostas que satisfazem com maior robustez a proposta adotada para esse trabalho.

Será descrita a arquitetura adotada para este trabalho, detalhando as respectivas funções de cada camada, além de elencar os problemas de segurança que afetam cada camada. O modelo foi escolhido seguindo alguns critérios que procurem atender o cenário brasileiro, sem deixar de existir interoperabilidade com o cenário internacional, gerando intercomunicação onde quer que seja adotado, visto que se utilizaram artigos que foram publicados em fontes de respaldo no meio científico. Observou-se a forma como estão divididas as funções dos respectivos níveis, deixando bastante claro o serviço que cada camada está designada a oferecer.

3. Problemas que afetam a IoT

Quando um sistema especialista é implementado há uma necessidade de informações diversas, que muitas vezes não parecem estar ligadas, mas que quando correlacionadas e tomadas as orientações corretas, podem indicar uma resposta. Nem sempre os dados iniciais aparentam ser importantes, mas quando combinados podem fornecer respostas cruciais a resolução de problemas e automatização de processos outrora ineficientes.

Durante a etapa de captação e movimentação de informações, um percentual significativo dos pacotes de dados trafega carregando informações sensíveis, que podem prejudicar, revelar informações confidenciais ou constranger o usuário, e está sujeito a interceptações maliciosas, assim, é necessário utilizar-se de uma série de medidas e regras que regulamentem a maneira com que essas informações são manipuladas e que estas possam garantir segurança, a fim de minimizar ao máximo os danos que possam vir a afetar o sistema e consequentemente o usuário.

Assim nesta nova era é necessário que haja um consenso de um modelo de Arquitetura e que o mesmo possa englobar robustez, velocidade, interoperabilidade e acima de tudo, segurança, no caso do último citado é um dos itens que se tem que olhar com bastante atenção. Além disso, é importantíssimo que essa adoção deixe um campo aberto para futuras inovações.

3.1. Camada de Percepção

Esta camada representa os cinco órgãos dos sentidos da IoT. O principal objetivo da mesma é a coleta profunda de todos os tipos de informação de todos os dispositivos em termos de propriedades, condições do meio, etc [Vikas, 2015]. A Camada de Percepção inclui leitores de etiquetas de código de barra 2D, RFID, câmera, GPS, terminais e sensores de rede. Segundo [Weizhe; Baosheng, 2013], usualmente essa camada constrói uma *Rede AD HOC* (significa "para esta finalidade" ou "com este objetivo") com uma distribuição dinâmica, dando recursos limitados ao nó, mudanças dinâmicas na topologia da rede e na estrutura distribuída.

Abaixo são descritos os problemas de segurança que essa camada enfrenta.

Captura Física: Como esses nós estarão distribuídos em um meio, podem ser facilmente capturados por um terceiro, que pode ter acesso as informações do usuário, podendo comprometê-las.

Acesso não Autorizado as Etiquetas: Devido a falta de um mecanismo adequado de autenticação em um grande número de sistemas RFID, essas etiquetas podem ser acessadas por alguém sem autorização. O atacante pode, não apenas ler os dados, mas os dados podem ser modificados ou até mesmos apagados [Uttarkar; Kulkarni, 2014].

Clone de Etiquetas Não Autorizado: Estes são os ataques de integridade em que um atacante consegue capturar informações de identificação de uma etiqueta. Novamente estes ataques são exacerbados pelo facto de que as etiquetas podem ser manipuladas por leitores invasores. A capacidade para criar clones de etiquetas pode ser usada como um meio de superar proteção falsa (por exemplo, em passaportes e etiquetas de droga) e como um passo de preparação de uma esquema de roubo em grande escala. Mais uma vez, ele expõe as empresas a novas vulnerabilidades se RFID’s são utilizados para automatizar as etapas de verificação para simplificar os procedimentos de segurança [Burmester; Medeiros, 2016].

Os desafios de segurança que essa camada enfrenta são discutidos abaixo:

Ataque de Força Bruta: Devido a pouca capacidade de armazenamento e o reduzido poder computacional desses dispositivos, é um alvo fácil para sofrer um ataque de força bruta.

Clone de Nós: Dada a simples estrutura dos nós, torna-se fácil a cópia por parte do atacante [Weizhe; Baosheng, 2013]. Tendo acesso a esses dispositivos e os meios para clonálos.

Ataque DoS: Como o nó tem capacidade limitada de processamento, atacantes podem usar o ataque de negação de serviço (DoS) para parar os serviços na rede [Vikas, 2015].

Interferência e Bloqueio: Os sinais de rádio podem sofrer interferência ou serem bloqueados, o que faz com que a mensagem seja corrompida ou perdida [Karygiannis; Owens, 2002] [Nichols; Lekkas, 2002]. Se o atacante tem um transmissor poderoso, um sinal pode ser gerado que será forte o suficiente para superar os sinais específicos e perturbar as comunicações. O mais comum tipos desta forma de bloqueio de sinal são ruídos aleatórios e pulso. Além disso, os ataques de congestionamento podem ser elaborados a partir de um local remoto para as redes alvo [Wu; Chen; Wu; Cardei, 2007].

3.2 Camada de Rede

A Camada de Rede desempenha um papel importante nas transferências de forma segura, mantendo a informações confidenciais. Podendo se utilizar das seguintes tecnologias para o seu trabalho: 3G, 4G, UMTS, Wi-FI, WiMAX, Bluetooth, infravermelho, satélite, etc. Por isso, esta camada é a principal responsável pela transferência da informação da Camada de Percepção para a camada superior [Surapon; Tuwanut, 2015].

A seguir são apresentadas as vulnerabilidades que esta camada enfrenta.

Ataque Shinkhole: É um ataque interno como se um intruso comprometesse um nó dentro da rede, e a partir desse lança um ataque. Em seguida, o nó comprometido tenta atrair todo o tráfego dos nós vizinhos com base na métrica de roteamento utilizado no protocolo de roteamento. Quando se consegue alcançar isso, ele lança um ataque. Devido ao padrão de comunicação da rede de sensores sem fio de muitos para um, a comunicação onde cada nó envia dados para a estação base, faz com que este WSN fique vulnerável a ataques shinkhole [Ngai; Liu; Lyu, 2007].

Ataque Sybil: No ataque Sybil, um nó malicioso se comporta como se fosse um número maior de nós, por exemplo através da personificação de outros nós ou simplesmente por reivindicando identidades falsas. No pior dos casos, um intruso pode gerar um número arbitrário de identidades, nó adicional, utilizando apenas um dispositivo físico [Newsome; Shi; Song; Perrig, 2004].

Ataque Consumo de Recursos: Este é também conhecido como ataque de privação do sono. Um atacante ou um nó comprometido pode tentar consumir a vida da bateria, solicitando descoberta excessiva de rota, ou através do envio de pacotes desnecessários para o nó vítima [Wu; Chen; Wu; Cardei, 2007].

3.3 Camada Middleware

Devido ao grande fluxo de dados que a Camada de Percepção coleta, além de ser muito importante acaba sendo difícil armazenar essa grande quantidade de informações que serão utilizadas pelas aplicações da Camada de Aplicação. Essa camada engloba várias técnicas como: *cloudcomputing, ubiquitouscomputing*. Esta consiste de um sistema de processamento de dados, ou seja, fica encarregada de processar os dados que são repassados da Camada de Rede, podendo tomar ações baseadas nos resultados computacionais, logo depois se conecta

com a base de dados, a qual fornece capacidade de armazenamento para os dados coletados e que ficam a disposição das aplicações que rodam na Camada de Aplicação.

Abaixo é mencionada a principal ameaça de segurança que assola a Camada Middleware.

Acesso não autorizado: A camada Middleware fornece interfaces diferentes para as aplicações e instalações de armazenamento de dados [Farooq; Waseem; Khairi; Mazhar, 2015]. O atacante pode facilmente causar enormes danos ao sistema, proibindo o acesso aos serviços relacionados à IoT ou apagar os dados existentes.

3.4 Camada de Aplicação

A principal tarefa da Camada de Aplicação é se utilizar das informações armazenadas pela Camada Middleware, então essa informação processada pode ser utilizada pelo usuário final.

Abaixo são elencados os problemas de segurança relatados para essa camada.

Vulnerabilidades de aplicações: Programadores que escrevem códigos não padronizados tornam-se uma brecha para a exploração de vulnerabilidades que possam existir no software. Hackers podem utilizar para explorar essas falhar para um propósito [Zhao; Ge, 2013].

Ataque DDoS: ataque DDoS e interrupção do serviço. Este tipo de ataque pode impedir que usuários normais visitem serviços de nuvem, tornando alguns serviços que estão na nuvem, críticos. Consomem uma grande quantidade de recursos do sistema, desde processos, memória, espaço em disco e banda de rede, o que leva a resposta do servidor de nuvem tornam-se extremamente lenta ou completamente indiferente [Wu; Chen; Wu; Cardei, 2007].

Vazamento de informações confidenciais: Nesta camada pode ter o controle de informações de suma importância em tempo real, o que pode ser utilizado para propósitos diversos, à bem entender de quem possui posse dessas informações.

Engenharia Social: Os usuários são o elo mais fraco, caso não tenha uma boa política de segurança, hackers podem utilizar dessa técnica para tomar posse de dados extremo valor para os negócios.

3.5 Camada de Negócios

A Camada de Negócios visa um desenvolvimento em longo prazo. Sem essa proposta se viu que o sucesso não depende apenas da prioridade da tecnologia, mas da inovação e do modelo de negócio. Essa camada é a responsável pela gestão de todo o sistema da IoT, incluindo as aplicações e serviços. Sendo responsável por construir modelos de negócio, gráficos, fluxogramas, etc.

A camada de negócios não só gerencia o lançamento e cobrança de várias aplicações, mas também a pesquisa sobre modelo de negócio e modelo de lucro. O sucesso de uma tecnologia não só depende da prioridade na tecnologia, mas também a inovação e razoabilidade de modelo de negócio. Tendo isso como ponto de partida, a Internet das Coisas não pode ter um desenvolvimento eficaz e de longo prazo, sem a pesquisa em modelo de negócio [Wu; Lu; Ling; Sun; Du, 2010].

Dentre os problemas de segurança pelo qual essa camada pode enfrentar o problema abaixo requer maior atenção:

Informações alteradas: Como as informações correm o risco de serem alteradas, podem-se gerar modelos de negócio, gráficos, fluxogramas, etc., com informações que podem não condizer com a realidade da coleta das mesmas.

4. Resultados

Diante de todas os levantamentos feitos em cada um dos níveis da Arquitetura de Segurança da IoT, se faz necessário uma proposta para incrementar ainda mais o nível de segurança do modelo adotado para esse trabalho, visando minimizar os danos que as ameaças possam vir a afetar em quaisquer uma das camadas, causando qualquer tipo de percepção ou indisponibilidade por parte do usuário, que é sempre o mais afetado.

Partindo desse pressuposto, abaixo será descrita a proposta de melhoria, detalhando cada aspecto das soluções apresentadas, visando assim uma melhor compreensão dessas medidas.

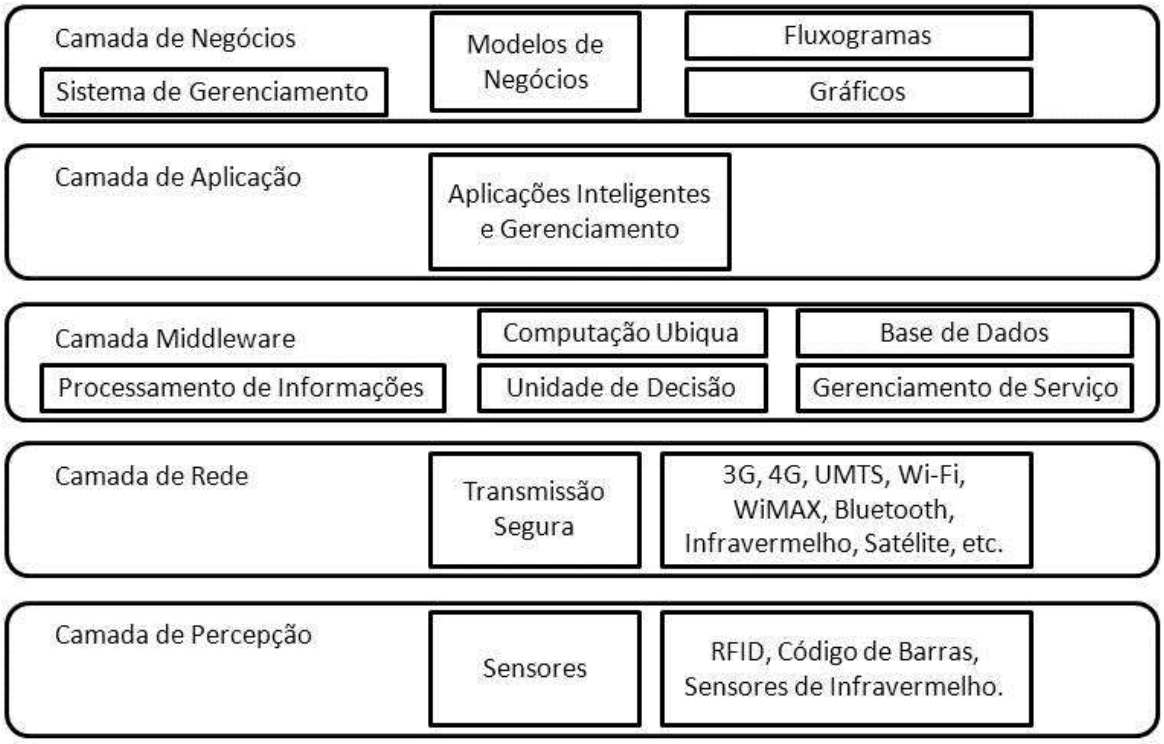


Figura 2: Layout da Arquitetura de Segurança proposta para a IoT

Fonte: O Autor (2016).

Criptografia: A utilização de criptografias assimétricas são bastante caras. Torna-se uma alternativa a utilização de criptografia simétrica. O SPIN (Sensor Protocols for Information via Negotiation) foi proposto. Foram construídos dois blocos seguros que compõem o SPIN: são eles SNEP (Sensor Network EncriptyProtocol) e µTESLA.

SNEP (Secure Network ProtocolEncryption): Fornece confidencialidade de dados, autenticação de dados e atualização de dados. Ele protege os canais de confidencialidade, fazendo o uso de autenticação. μTESLA (Microcronometrada, eficiente e streaming, possui perda tolerante e protocolo de autenticação) fornece autenticação ampla para ambientes que dispõem de dispositivos com capacidades limitadas. Ele usa transmissão autenticada assimétrica para fornecer autenticação [Gonçalves; Costa, 2015].

Ataques DoS: Segundo informa [Albarakati, 2015], a defesa contra o ataque DoS é o uso de códigos de correção de erros.

Gerenciamento de Chaves: Como o gerenciamento de chave é uma das bases mais importantes do mecanismo de segurança, é sempre a área de pesquisa que está sempre em evidência. Ela ainda é o aspecto mais difícil de segurança criptográfica. Atualmente, os pesquisadores não encontrar soluções ideais, algoritmos criptográficos leves ou de tenham desempenho elevado do nó sensor, que não estão sendo aplicados. Até agora, a rede de sensores em grande escala é dificilmente posta em prática. Os problemas de segurança de rede serão pagos com mais atenção ao se tornarem pontos chaves e as dificuldades da investigação neste ambiente de rede.

Solução para Ataques Shikhole: É apresentado um algoritmo que consiste em dois passos, sendo que a primeira etapa é de localização de uma lista de nós suspeitos, o qual é verificado a consistência dos dados, identificando em seguida o intruso na lista através de uma análise das informações de fluxo de rede [Ngai; Liu; Lyu, 2007]. Além disso, foi apresentada uma série de melhorias para lidar com nós maliciosos em trabalho conjunto que interferem o algoritmo de detecção e tentativa de esconder o intruso real.

Solução para Ataque Sybil: Para a solução do problema nesse cenário, o método mais promissor dentre os que puderam ser verificados foi o de pré-distribuição de chave aleatória, que consiste em associar chaves de um nó com a sua identidade [Newsome; Shi; Song; Perrig, 2004].

IDS (Sistema de Detecção de Intrusos): Essa é uma ferramenta de software que é utilizada para detectar acessos não autorizados a um sistema de computador ou rede. Ele pode detectar todos os tipos de tráfego de rede malicioso, que inclui: ataques de rede contra serviços vulneráveis, ataques impulsionando dados relativos aos pedidos, os ataques baseados em host (elevação de privilégios, logins não autorizados e acesso a arquivos sensíveis e malware). Um sistema de detecção de intrusão é uma entidade de monitoramento dinâmico, que complementa as capacidades de monitoramento estáticas de um firewall. Um sistema de detecção de intrusão monitora o tráfego na rede em modo promíscuo, muito parecido com um *sniffer* de rede (ferramentas que interceptam e analisam o trafego de uma rede). Os pacotes de rede que são recolhidos são analisados por violações de regras por um algoritmo de reconhecimento de padrões. Quando são detectadas violações de regras, o sistema de detecção de intrusão alerta o administrador.

5. CONCLUSÃO

Após a descrição a arquitetura adotada para este trabalho e detalhamento das respectivas funções de cada camada seguida da apresentação dos principais problemas de segurança que afetam cada camada, o estudo pode concluir que o modelo de protocolo de arquitetura de segurança em cinco de camadas deve ser adotado no Brasil a fim de se obter

interoperabilidade entre os dispositivos na IoT, pois além de garantir uma maior segurança dos dados, independentemente da camada em que estejam sendo tratados, atendem plenamente a realidade do cenário internacional, gerando intercomunicação onde quer que seja adotado.

Referências

Albarakati, A. J. A Study on Underwater based Wireless Sensor Networks. International Journal of Computer Applications (0975 – 8887). Volume 119, nº.12, June 2015.

Bartariya, S.; Rastogi, A. Security in Wireless Sensor Networks: Attacks and Solutions. In: International Journal of Advanced Research in Computer and Communication Engineering. Vol. 5, Issue 3, March 2016.

Wu, B.; Chen, J.; Wu, J.; Cardei, M. A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. In: XIAO, Yang; SHEN, Xuemin Sherman; DU, Ding-Zhu. Wireless Network Security. [S.l.]: Springer, 2007.

Burmester, M.; Medeiros, B. RFID Security: Attacks, Countermeasures and Challenges. Florida: Computer Science Department, 2016. Disponível em: >https://www.cs.fsu.edu/~burmeste/133.pdf< Acesso em: 25 jul.2016.

Gonçalves, D. O.; Costa, D.G. A Survey of Image Security in Wireless Sensor Networks. [S.l]: J. Imaging, 2015.

Itu by Internet Reports Series. The Internet of Things. Geneva: ITU, 2005

Karygiannis, T.; Owens, L. Wireless Network Security-802.11, Bluetooth and Handheld Devices. National Institute of Standards and Technology. U.S: Technology Administration, Department of Commerce, Special Publication p.800-848, 2002.

Zhao, K.; Ge, L. A Survey on the Internet of Things Security. In: Ninth International Conference on Computational Intelligence and Security. [S.l.: s.n.], 2013.

Wu, M.; Lu, Ting-lie; Ling, Fei-Yang; Sun, Jing; Du, Hui-Ying. Research on the Architecture of Internet of Things.[S.l]: ICACTE, 2010.

Mohammadi, S.; Jadidoleslamy, H. A Comparison of Physical Attacks on Wireless Sensor Networks. International Journal of Peer to Peer Networks (IJP2P). Vol.2, nº.2, Issue 11, November 2014. April 2011.

Farooq, M. U.; Waseem, M.; Khairi, A.; Mazhar, S. A Critical Analysis on the Security Concerns of Internet of Things (IoT). In: International Journal of Computer Applications. [S.l: s.n], 2015.

Newsome, J.; Shi, e.; Song, D.; Perrig, A. The Sybil Attack in Sensor Networks: Analysis & Defenses. [S.l: s.n], 2004.

Ngai, E.; Liu, J.; Lyu, M. An efficient intruder detection algorithm against sinkhole attack in wireless sensor network. In: Computer Communications, [S.l: s.n], 2007.

Nichols, R.; Lekkas, P. Wireless Security-Models, Threats, and Solutions, McGraw-Hill. [S.l]: Chapter, 2002.

Rafiullah, K.; Sarmad, U. K.; Zaheer, R.; Khan, S. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. In: 10th International Conference on Frontiers of Information Technology. [S.l: s.n], 2012.

Stallings, William – Criptografia e Segurança de Redes – Princípios e Práticas, 5ª Edição, Prentice-Hall, 2013.

Surapon, Kraijak, Tuwanut, Panwit. A Survey on Internet of Things Architecture, Protocols, Possible Applications, Security, Privacy, Real-World Implementation and Future Trends. In: Proceedings of ICCT2015. [S.l: s.n], 2015.

Uttarkar, R.; Kulkarni, R. Internet of Things: Architecture and Security. In: International Journal of Computer Application, Volume 3, Issue 4, 2014.

Vikas, B. O. Internet of Things (IoT): A Survey on Privaçy Issues and Security. [S.l: s.n], 2015.

Weizhe, Z.; Baosheng, q. Security Architecture of the Internet of Things Oriented to Perceptual Layer. In: International Journal on Computer, Consumer and Control (IJ3C). [S.l: s.n], Vol. 2, nº.2, 2013.

4.4 Artigo IV - ANÁLISE DE CENÁRIO PROSPECTIVO DE APLICAÇÃO DA INTERNET DAS COISAS NO ÂMBITO EDUCACIONAL BRASILEIRO

Esta seção apresenta o quarto artigo intitulado de " Análise de Cenário Prospectivo de Aplicação da Internet das Coisas no Âmbito Educacional Brasileiro ", que não será publicado. O artigo mantém o padrão proposto pela Associação Brasileira de Normas Técnicas - ABNT.

ANÁLISE DE CENÁRIO PROSPECTIVO DE APLICAÇÃO DA INTERNET DAS COISAS NO ÂMBITO EDUCACIONAL BRASILEIRO

Alan Kilson Ribeiro Araújo[1]
Rodrigo Franco Gonçalves[2][1]

Resumo

A Internet das Coisas (IoT) é resultado da convergência de diversas tecnologias, em primeiro lugar, a miniaturização e popularização de sensores que viabilizam a coleta e transmissão de dados, o cenário prospectivo da IoT também é contemplado no âmbito educacional, ao apoiar, melhorar e garantir processos educacionais inovadores. Desta forma, o objetivo do presente estudo é realizar a análise de cenários prospectivos de aplicação da internet das coisas no âmbito educacional brasileiro realizando um estudo de caso em uma escola em Vitória da Conquista - BA. A metodologia aplicada é o método análise de cenário e estudo de caso e a abordagem qualitativa. Concluiu-se que o projeto de implantação da Internet das Coisas no âmbito educacional em Vitória da Conquista com a utilização de chip nos uniformes, não evoluiu devido às falhas no sistema de operação e durabilidade do chip após lavagem das roupas evidenciando um estudo mais aprofundando na busca de melhorias na efetividade do projeto e depois assim reativá-lo.

Palavras-chave: Internet das Coisas; Educação; Projeto em Vitória da Conquista.

Abstract

The Internet of Things (IoT) is the result of the convergence of several technologies, in the first place, the miniaturization and popularization of sensors that make possible the collection and transmission of data, the IoT prospective scenario is also contemplated in the educational scope, by supporting, improving And ensure innovative educational processes. Thus, the objective of the present study is to perform the analysis of prospective scenarios of Internet application of things in the brazilian educational context by carrying out a case study in a school in Vitória da Conquista - BA. The applied methodology is the method of scenario analysis and case study and the qualitative approach. It was concluded that the project of implantation of Internet of Things in the educational scope in Vitória da Conquista with the use of chip in the uniforms, did not evolve due to the failures In the system of operation and durability of the chip after washing of the clothes evidencing a study more in depth in the search of improvements in the effectiveness of the project and after this reactivate it.

Keywords: Internet of things; Education; Project in Vitória da Conquista.

[1] Administrador e Mestrando em Engenharia de Produção pela Universidade Paulista - UNIP
[2] Professor Doutor do Programa de Pós Graduação em Engenharia de Produção da Universidade Paulista - UNIP

Introdução

A evolução tecnológica proporcionou em larga escala mudanças significativas no contexto informacional, assim, ao longo dos anos foram desenvolvidos cada vez mais mecanismos complexos e eficientes que aumentaram a eficiência para a busca, localização, recuperação, uso e divulgação da informação (CARVALHO; SOUZA, 2015).

Com isto, pode-se atribuir tais características tecnológicas a Internet das Coisas, que, de acordo com Mattos Filha (2013, p.77), pode ser "considerada como uma espécie de rede de objetos inteligentes, formados por pequenos dispositivos que possibilita, através de um identificador único, conter um pequeno repositório com dados e informações que podem ser comunicados através de um dispositivo externo". Sendo a Internet das coisas a evolução tecnológica da comunicação e da computação, sua inovação, que se dará por meio de fatores importantes como sensores, *Wireless* e nanotecnologia. Isso promoverá a possibilidade de objetos de uso comum no dia-a-dia serem conectados à rede favorecendo a interação entre objetos e pessoas.

Uma das propostas da IoT é permitir, com o uso de tecnologias de rastreamento, identificação e troca de informações, que numerosos objetos comuniquem-se automaticamente e a distância, estudo este que poderá permitir diversas utilizações (MOLINA, 2012).

Assim a satisfação atual com a Internet das Coisas (IoT) é resultado da convergência de diversas tecnologias, em primeiro lugar, a miniaturização e popularização de sensores que viabilizam a coleta e transmissão de dados, com estimativa de mais de 40 bilhões de dispositivos conectados em 2020. Tal conectividade é viabilizada pelo avanço das redes sem fio, tornando onipresente o acesso e a transmissão dos dados para a Internet (ALMEIDA, 2015).

Observa-se também que o termo Internet das Coisas (IoT) está entre os tópicos mais discutidos no meio acadêmico de tecnologia da última década, com uma proposta de ser uma rede ubíqua, que pode ser acessada "a qualquer hora, em qualquer lugar, por qualquer um e qualquer coisa" interconectando dispositivos entre si e esses tendo, com base em dados colhidos por sensores equipados com: Identificação de Rádio Frequência (RFID), sensores de infravermelho e leitores de código de barras; sendo esses dados inteligentemente processados, se tornando assim, dispositivos inteligentes capazes de captar e tomar decisões sem interferência humana, abrindo portas para uma nova era da computação (ARAÚJO et al., 2016).

Entendendo a Internet das Coisas um fenômeno atual de grande significado técnico, social e econômico, ocorre um processo de convergência onde produtos de consumo, bens duráveis, componentes industriais e de utilidade pública, sensores e outros objetos do cotidiano estão sendo combinados com a conectividade da Internet e com capacidades analíticas de dados poderosas que prometem transformar a forma como nós trabalhamos, vivemos e nos divertimos (POETAS.IT, 2016).

Desta forma, surge o interesse pelo conhecimento do futuro, que está biologicamente associado ao homem, já que é relacionado ao seu instinto de sobrevivência. Nas organizações é fundamental esse conhecimento, pois pode diminuir ou mesmo eliminar a variável de risco. Uma das formas de responder a pergunta sobre como será o futuro sem que isso se constitua meio de adivinhação é mediante a utilização de cenários prospectivos (CARVALHO; SOUZA, 2015).

A importância de se trabalhar com cenários permite “estimular a imaginação, reduzir as incoerências, criar uma linguagem comum e permitir a reflexão” (VALDEZ, 2007).

A prospectiva visa avaliar o futuro para explicar o presente, sua postura é marcadamente pró-ativa e não encara o futuro apenas como prolongamento do passado, pois o futuro está aberto às ações de múltiplos atores que agem, hoje, em função dos seus projetos para o futuro (CARVALHO; SOUZA, 2015).

Desta forma, o cenário prospectivo da IoT também é contemplado no âmbito educacional, ao apoiar, melhorar e garantir processos educacionais inovadores, sendo exemplos de aplicações: a aprendizagem móvel, que permite que conteúdos curriculares possam ser acessados, compartilhados além disso, discutidos fora da sala de aula e a acessibilidade de alunos com necessidades especiais através do uso de cartões (TEC.EDU., 2016).

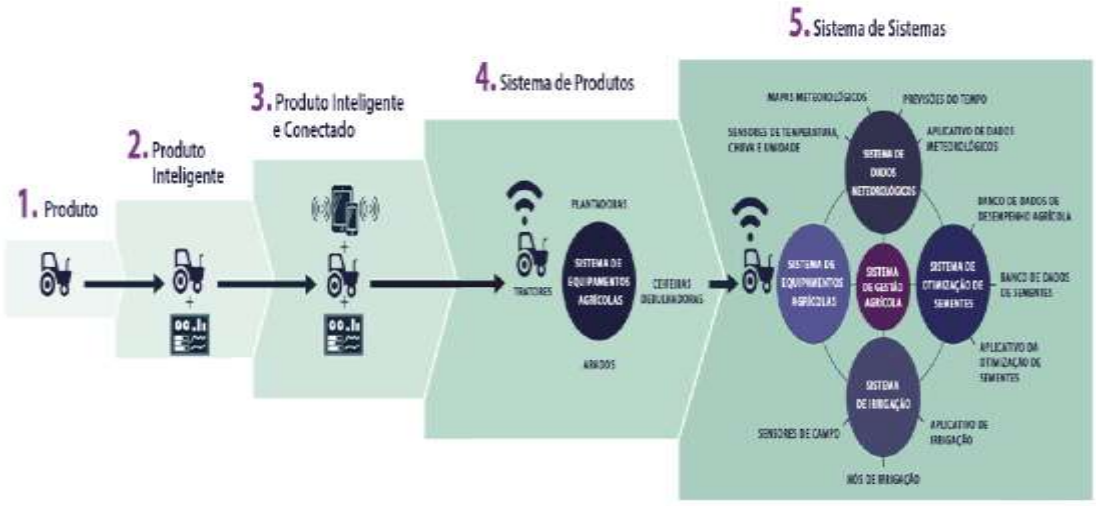
Diante disto, o presente estudo realiza um estudo de caso com enfoque na análise de cenários prospectivos de aplicação da Internet das Coisas no âmbito educacional em Vitória da Conquista.

Referencial Teórico

A Internet das Coisas é uma infraestrutura de rede global dinâmica, baseada em protocolos de comunicação onde coisas físicas e virtuais têm identidades, atributos físicos e personalidades virtuais, utilizando interfaces inteligentes e integradas às redes telemáticas. Para que haja a Internet das Coisas é preciso o desenvolvimento de ações que utilizam

softwares para a construção dos objetos que se utilizam sensores ou outros dispositivos conectados, conforme demonstra a figura 01 abaixo (SUNDMAEKER et al., 2010).

Figura 01 - Produtos Inteligentes Conectados



Fonte: Poetas.It (2016).

Desta forma, surge o interesse pelo conhecimento do futuro, que está diretamente relacionado à aplicabilidade da Internet das Coisas em vários segmentos, inclusive no âmbito educacional, onde uma das formas de responder ao questionamento de como será o futuro de sua aplicação é através da utilização de cenários prospectivos (CARVALHO; SOUZA, 2015; TEC.EDUC, 2016).

Para Franco (2007) cenário é "a existência de mais de uma solução é condição básica para a tomada de decisão e uma das bases do planejamento estratégico".

O planejamento prospectivo é, portanto, "um processo estruturado e coordenado, que tem como função a formulação de estratégias para se atingirem objetivos" (CARDOSO et al., 2005).

Dahis (2008) define cenários prospectivos como configurações de imagens de futuro condicionadas e fundamentadas em jogos coerentes de hipóteses sobre os prováveis comportamentos das variáveis determinantes do objeto de planejamento.

Os cenários prospectivos têm o objetivo de se perscrutar o futuro e preparar sociedades e instituições para se ajustarem às conjunturas então previstas ou previsíveis (futuros alternativos) (COUTEAU-BÉGARIE, 2007).

Para a efetivação de cenários prospectivos, há uma grande quantidade de métodos e técnicas utilizados para prospecção de futuro, existem os métodos formais, informais e quantitativos; os métodos formais são entrevistas estruturadas, análises morfológicas, discussões organizadas sobre questões predeterminadas, Delphi, análise de impactos cruzados, construção e análise de cenários (CARDOSO et al., 2005).

A utilização da análise prospectiva vem se difundido principalmente na Europa, empresas como: BASF, DaimlerChrysler, Èletricité de France, Elf, Renault, Schne ider, Shell aplicam este ferramental para a construção de cenários que embasam o planejamento estratégico da mesma forma as empresas médias começam a perceber a lógica do processo de planejamento baseado em cenários (VILELA; MAIA, 2016).

Carvalho e Souza (2015) afirmam que em relação ao futuro da Internet das Coisas, atualmente existem 36 plataformas tecnológicas européias (PTE) e cinco iniciativas tecnológicas conjuntas (ITC) abrangendo as áreas tecnológicas mais importantes que se conectam a milhares de empresas européias, institutos de pesquisas e tomadores de decisões políticas e que 10 dessas PTE se tornaram importantes para a Comissão Européia em termos de desenvolvimento de agendas estratégicas de pesquisa e definição das tecnologias necessárias para a implementação do futuro da internet.

Jafarey (2015) prevê uma análise prospectiva da Internet das Coisas em relação as empresas, verificando que possivelmente o futuro das empresas dependerá da forma como as companhias abordarão as possibilidades de Internet das Coisas. Os departamentos mais inovadores verão o conceito como um grande horizonte cheio de possibilidades para criar novas formas de negócio e atuarem de forma mais preditiva na relação com o mercado e os clientes.

> CINCO DIMENSÕES estruturais para serem estudadas em detalhe quando se discute a Internet das Coisas no Brasil e o que deveríamos fazer para que a IoT fosse importante para o país. Tais dimensões são as de COMPLEXIDADE do Problema e do Fenômeno Econômico, PRODUTOS INTENSIVOS em SERVIÇOS, ECOSSISTEMAS EMPRESARIAS e ORGANIZACIONAIS e GOVERNANÇA necessárias para o desenvolvimento econômico, social e sustentado da Internet das Coisas no Brasil. Vale salientar, e tratamos com destaque, que nada será possível se não desenvolvermos as competências humanas e de relação com o mercado demandadas neste contexto (POETAS.IT, 2016, p. 8).

O cenário prospectivo da IoT também é contemplado no âmbito educacional, ao promover processos educacionais inovadores, facilitando o acesso e desempenho dos alunos (TEC.EDU., 2016).

Metodologia

A pesquisa desenvolvida é a do tipo bibliográfica, realizada com base em material já elaborado, constituído principalmente de livros e artigos científicos e com utilização do método análise de cenário, que enquadra-se na abordagem qualitativa. Este procedimento permite adquirir conhecimento do fenômeno estudado a partir da exploração intensa de um único caso (GIL, 2010).

Diante disto, aborda-se a análise de cenário prospectivo de aplicação da Internet das Coisas dentro de um estudo de caso no âmbito educacional em Vitória da Conquista - BA.

Resultados e Discussões

Um cenário prospectivo da IoT no âmbito educacional é citado por Lemos (2016). Tratou-se de um projeto revolucionário no Brasil, que teve como objetivo monitorar a entrada e a saída de alunos do Centro Municipal de Educação Professor Paulo Freire (CAIC), em Vitória da Conquista – BA. A Prefeitura investiu cerca 1,2 milhão de reais no projeto, com o objetivo de atender 25 escolas e mais de 20 mil alunos da rede municipal da cidade no ano de 2012, tendo como meta que em 2013, todos os 43 mil estudantes da rede pública da cidade, entre 4 e 14 anos, já possuíssem uniformes com a tecnologia RFID. Toda etiqueta RFID tem um código universal e é cadastrada no sistema da instituição com os dados do estudante e o número do telefone celular de seus pais ou responsáveis que seriam os recebedores das informações de entrada e saída do aluno da escola, também foi instalado um leitor na portaria da escola, de modo que quando o aluno vestido no uniforme passe pela portaria, o leitor ativa a etiqueta nesse exato momento, produzindo essa informação de entrada e saída de aluno.

Entretanto, de acordo com o autor supracitado o projeto suscitou em diversas controvérsias entre pedagogos, psicólogos, jornalista, intelectuais, pais e alunos. Esse caso de aplicação de IoT é interessante para mostrar como as controvérsias expressam o magma social, isto é, o social antes de estabilizações e caixas-pretas.

Não bastasse as diversas discussões sobre o projeto, o sistema não apresentou funcionalidade efetiva envolvendo falhas técnicas, que de acordo com o relato de mães transcreve-se: "as informações da minha filha nunca chegaram", "as do menino vinham, mas só de vez em quando". Também houve vários relatos de problemas com a durabilidade das peças, que não teriam resistido às lavagens constantes dos uniformes. Além disso, os resultados obtidos com o sistema foram tímidos e, de acordo com a Secretaria Municipal de

Educação, após a adoção dos uniformes com chip, a redução da evasão escolar nas unidades foi de apenas 2% (DÉCIMO, 2013).

Alguns autores como Carvalho e Souza (2015) sugerem outras utilizações da IoT no âmbito educacional, como em bibliotecas, em que entre as possibilidades vislumbradas, destacam-se: localização do material no acervo por meio de sensores que indicariam onde está inserido o item na estante, controle de incêndio, enchentes ou outros problemas ambientais, timidamente pode-se considerar o inventário eletrônico como um dos usos com a Internet das coisas, a partir do momento em que a leitura do código de barras é feita diretamente de um mecanismo nas etiquetas do livro, sem a necessidade de retirá-los das estantes, ressalta-se ainda as etiquetas magnéticas anti-furtos inseridas nos livros, que são detectadas por portão eletrônico.

Sundmaeker et al. (2010) comentam que com a Internet das Coisas no âmbito educacional, os livros inteligentes do futuro irão interagir com o sistema de entretenimento, tais como multimídia, hipertexto; e na tela da TV poderão constar informações adicionais sobre o tema que se está lendo em tempo real.

Trazendo para dentro dos portões da escola a Internet das Coisas, Claro (2016) também sugere exemplos simples, como transformar o celular dos alunos em um mecanismo valioso de acompanhamento da vida escolar, em que ao conectar diferentes espaços e objetos da escola, um aluno poderia utilizar o seu celular para acessar laboratórios, verificar a disponibilidade de livros na biblioteca, marcar reuniões ou até comprar lanches; tudo isso ficaria registrado, ao mesmo tempo em que sensores no material escolar poderiam contabilizar faltas ou acompanhar o seu trajeto de volta para casa, haja vista que a integração desses objetos à internet permite registrar as preferências dos alunos e reunir um grande volume de dados, como a quantidade de vezes que ele comprou doces na cantina ou chegou atrasado na escola.

A Internet das Coisas pode ser também utilizada para fins de segurança nas escolas, sendo que estas podem criar alavancas ou botões em toda a escola que, quando acionados, iniciam um sistema de bloqueio personalizado, que pode incluir, entre outras funcionalidades, perímetro de segurança automático, notificação imediata das autoridades e transmissão de vídeo para a polícia, onde possam monitorar a atividade do intruso (EDUCADORES INOVADORES, 2014).

Considerações Finais

Atendendo ao objetivo central do referido artigo, a análise dos cenários prospectivos de aplicação da Internet das Coisas no âmbito educacional brasileiro, por meio de um estudo de caso em uma escola de Vitória da Conquista-BA, verificou-se que o projeto de implantação da Internet das Coisas no âmbito educacional em Vitória da Conquista com a utilização de etiquetas RFID nos uniformes com objetivos de levar informações aos pais ou responsáveis sobre a entrada e saída de alunos da escola não evoluiu devido às falhas no sistema de operação e durabilidade do chip após lavagem das roupas, evidenciando um estudo mais aprofundando na busca de melhorias na efetividade do projeto e depois, assim, reativá-lo.

Assim como há uma nítida evolução tecnológica ao lado do desenvolvimento do homem, existe também uma nítida vulnerabilidade do país com relação a estes avanços tecnológicos. Por ser um sistema complexo, necessária seria uma combinação com a estrutura econômica do país, considerando que os avanços tecnológicos traduzem os avanços econômicos.

Devido IoT estar ainda em fase ainda de construção e potencial de externalidades para a economia e bem estar no Brasil, para muitos países e regiões tornou-se um problema estratégico de grande interesse, por causa de seus potenciais impactos econômicos e sociais.

Neste sentido, se a Internet das Coisas é uma infraestrutura de rede global dinâmica que necessita do desenvolvimento de ações que utilizem softwares, a mesma está intimamente ligada ao crescimento econômico.

Além do mais, se o cenário prospectivo da Internet das Coisas induz a um processo estruturado e coordenado visando uma conjuntura futura, se torna, no mínimo, relevante o projeto de monitoramento, por meio da IoT no sistema educacional.

O referido projeto, embora complexo e ainda carente de aprimoramento, aduz a um crescimento significativo do cenário educacional, tendo em vista que o conhecimento pelo futuro está ligado à aplicabilidade da Internet, pois como dito, a população se consagra, hoje, por meio dos avanços tecnológicos.

Observou-se também outras sugestões de aplicabilidade da Internet das Coisas no âmbito educacional, como em bibliotecas, livros inteligentes, uso do celular para acessar laboratórios, livros, comprar lanches e também utilidade no quesito segurança dos alunos. Compreende-se, desta forma, que ainda assim a Internet das Coisas é um campo promissor nos cenários prospectivos inclusive no âmbito educacional.

Referências Bibliográficas

ALMEIDA, H. Internet das Coisas: Nós, as cidades, os robôs, os carros, tudo conectado. **Revista da sociedade brasileira**. Porto Alegre. 2015.

BRANCO, A. L. **Revoluções industriais: Primeira, segunda e terceira revoluções**. 2007. Disponível em: http://educacao. uol. com. br/ disciplinas/ geografia/ revolucoes-industriais-primeira-segunda-e-terceira-revolucoes.htm Acesso em: 02/12/2016.

CARDOSO, L. R. A. et al. Prospecção de futuro e Método Delphi: uma aplicação para a cadeia produtiva da construção habitacional. **Ambiente Construído**, Porto Alegre, v. 5, n. 3, p. 63-78, jul./set. 2005.

CARVALHO, T.; SOUZA, T. L. Internet das Coisas e Sua Aplicação em Bibliotecas. **Revista Gestão**. Org. v.13. ed. Especial. 2015. p.264-270.

CLARO, M. **Como a Internet das Coisas pode entrar nas escolas**. 2016.Disponível em: https:// www. moodlelivre. com. br/ noticias/ 1481 como–a–internet -das- coisas-pode entrar-na-escola acesso em: 02/01/2017.

COUTEAU-BÉGARIE, H. **Os Grandes Desafios Estratégicos do século XXI**, palestra in VI Encontro Nacional de Estudos Estratégicos. EGN. Rio de Janeiro. 2007.

DÉCIMO, T. **Chip será retirado de uniforme em Vitória da Conquista.** 2013. Disponível em: http:// www. estadao. com. br/ noticias/ geral, chip-sera-retirado-de-uniforme-em-vitoria-da-conquista,1091860 acesso em 02/01/2017.

EDUCADORES INOVADORES. **Internet das Coisas traz uma nova era para a educação.** 2014. Disponível em: http:// www. blogeducadoresinovadores. com.br /2014/ 12/ 01/internet-das-coisas-traz-uma-nova-era-para-a-educacao/ acesso em 02/01/2017.

FRANCO, F. L. **Prospectiva estratégica:** Uma metodologia para a construção do futuro. 2007. 240 f. Tese (Doutorado em Engenharia). Programa de Pós-Graduação de Engenharia, Universidade Federal do Rio de Janeiro, RJ, 2007.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa**. 5ª Ed. Atlas: São Paulo. 2010.

GRISI, C. C. H.; BRITTO, R. P. **Técnica de Cenários e o Método Delphi: uma aplicação para o ambiente brasileiro**. In: SEMINÁRIOS EM ADMINISTRAÇÃO FEA-USP, 6., 2003, São Paulo.

HOBSBAWN, E. J. **Industry and Empire: From 1750 to the Present Day**, rev. and updated with Chris Wrigley, 2nd ed., New York: New Press, 1999.

JARAFEY, A. **Capacidade explorar IoT definirá o futuro da tecnologia e do CIO**. 2015. Disponível em: http://computerworld.com.br/capacidade-explorar-iot-definira-o-futuro-da-tecnologia-e-do-cio. Acesso em: 10/12/2016.

LEMOS, A. **A comunicação das coisas, Internet das coisas e teoria Ator-Rede Etiquetas de radiofrequência em uniformes escolares na Bahia**. Disponível em: http://www.seminariosmv.org.br/textos/Andre%20Lemos.pdf Acesso em: 10/12/2016.

MATTOS FILHA, M. H. F. **A biblioteca universitária e a educação superior a distância: estudo do planejamento dos serviços, compartilhamento da informação e do conhecimento nas universidades no Estado do Rio de Janeiro**. Dissertação (Mestrado em Ciência da Informação). Programa de Pós-Graduação em Ciência da Informação, Universidade Federal Fluminense, 2013.

MOLINA, F. **USP desenvolve ligados à Internet das Coisas.** 2012. Disponível em: http://www5.usp.br/14645/usp-desenvolve-projetos-ligados-a-internet-das-coisas/ acesso em 02/01/2017.

POETAS.IT. **IoT - Uma Estratégia para o Brasil / Consolidação de uma visão unificada para orientação e proposição de políticas públicas sobre Internet das Coisas no Brasil v.1.2.** 2016. Creative Commons. Disponível em: www.cesar.org.br/poetas.it/visionstatement Acesso em: 05/12/2016

REVISTA TEC. EDUC. **Internet das Coisas na Educação: aplicações e benefícios**. 2016. Disponível em: http://www.positivoteceduc.com.br/giro-te/internet-das-coisas-na-educacao-aplicacao-e-beneficios/ Acesso em: 05/12/2016.

SOARES, F. **Primeira, segunda e terceira revolução industrial.** 2013. Disponível em: http: // www. geografiaopinativa. com. Br /2013 /12/ primeira- segunda -e- terceira-revolucao. html Acesso em 9/12/2016.

SUNDMAEKER, H. et al. Vision and Challenges for Realising the Internet of Things. In: **Cluster of European Research Projects on the Internet of Things.** European Commission-Information Society and Media DG, Brussels, Mar. 2010. p. 230.

VALDEZ, Tomás Alves de Só. **Regionalização e Integração Sistêmica:** cenários para a reforma do Sistema de Saúde de Cabo Verde. 2007. 240 f. Dissertação (Mestrado em Saúde Pública). Fundação Oswaldo Cruz - FIOCRUZ. Escola Nacional de Saúde Pública Sérgio Arouca. Rio de Janeiro, 2007.

VILELA, L. E.; MAIA,S.W. **Utilização da análise prospectiva e da metodologia de planejamento para a construção de cenários norteadores do planejamento estratégico em empresas de médio porte - O caso da Brazshipping Marítima LTDA**. Disponível em: http: //www. anpad. org. br/ diversos/ trabalhos/ 3Es/ 3es_2003/ 2003_3ES40.pdf Acesso em: 07/12/2016.

5 CONSIDERAÇÕES FINAIS

5.1 Conclusões

Ao atender o objetivo central deste trabalho de investigar como a Internet das Coisas está sendo utilizada no âmbito da administração pública brasileira buscando identificar sua utilização de maneira efetiva para o gerenciamento e enfretamento dos problemas sociais, conclui-se que o estudo da IoT é resultado de um processo evolutivo da Revolução Industrial, que se caracteriza por ser um cenário de tecnologia sem fio moderna das telecomunicações, tendo como ideia básica deste conceito a presença generalizada em torno das pessoas e de uma variedade de coisas ou objetos, que são interconectados, facilitando as atividades cotidianas.

Sendo que a IoT, mesmo em fase de construção, já evidencia seu processo de expansão mundial, despertando assim, interesse para muitos países e regiões, uma vez que apresenta papel estratégico para o desenvolvimento técnico, social e econômico, incluindo o Brasil, que em seu contexto enxerga uma forma de gerar valor agregado localmente, além de ganhos de produtividade e a inserção global do país no cenário de tecnologia.

Além disso, a utilização da IoT tem importância significativa na gestão pública, haja vista que melhora suas práticas internas e a vida dos cidadãos, acelerando respostas e poupando ou gerando recursos.

Em atendimento ao objetivo de análise das questões chave de exploração da IoT desde segurança, privacidade, interoperabilidade e padrões, regulamentação e legislação e aplicações ligadas ao desenvolvimento social através da gestão pública, conclui-se que existe uma necessidade de uma gestão estratégica ligada ao seu desenvolvimento, principalmente em um país como o Brasil, na qual a IoT adquire uma complexidade sistêmica ou complexidade envolvendo múltiplos sistemas analíticos e que poucas vezes foi enfrentada nos domínios tanto da intervenção privada quanto da intervenção pública, quando se aborda políticas públicas baseadas ou habilitadas por tecnologia.

Desde 1995, quando foi criado o Comitê Gestor da Internet no Brasil observa-se uma experiência positiva de governança da Internet tradicional, visando à produção de novos conhecimentos, a inovação tecnológica e o desenvolvimento econômico, a partir da experiência dos laboratórios de Ciência da Computação de algumas de suas principais universidades, de algumas lideranças na área de inovação e a colaboração de instituições de ciência e tecnologia dos governos federal e estadual, contando também com a participação da

iniciativa privada nacional, ficando então evidenciado o esforço do Governo e de iniciativas privadas, para criar um ambiente de negócio mais inovador.

Quanto ao objetivo de comparar os instrumentos regulatórios vigentes da Internet das Coisas concluiu-se que o Governo Federal já estuda a criação de um Plano Nacional da Internet das Coisas em busca da padronização, por meio de três etapas: normalização dentro do mercado, largura de banda e segurança de dados, temáticas essenciais voltadas para privacidade, segurança e direitos do consumidor, os quais legalmente são assegurados pelo Marco Civil da Internet (Lei nº 12.965/2014).

Em quesitos fundamentais como privacidade e segurança, ficam evidenciados, que o sistema regulatório brasileiro precisa ajustar-se rapidamente ao cenário de implementação da IoT no mundo, pois ainda não há uma regulação específica adequada na área ou para proteção de dados pessoais e privacidade no Brasil, sendo que as propostas em discussão foram elaboradas quando a IoT ainda não era uma realidade, assim os assuntos regulatórios devem voltar-se para leis que protejam os direitos individuais e favoreçam a inovação, com o objetivo de definir um modelo para o cenário de IoT com foco na proteção dos direitos constitucionais dos usuários e em consonância com as políticas de inovação e desenvolvimento, utilizando modelos internacionais como base para construir soluções nacionais que garantam a segurança e a privacidade .

Quanto ao objetivo de descrever o papel das camadas de segurança utilizadas na estrutura da Internet das Coisas, conclui-se que o modelo de protocolo de arquitetura de segurança em cinco camadas deve ser adotado no Brasil, a fim de se obter interoperabilidade entre os dispositivos na IoT, pricipalmente os utilizados na educação, garantindo uma maior segurança dos dados, sejam eles em qualquer camada que estejam sendo tratados, atendendo assim à realidade do cenário internacional e gerando intercomunicação onde quer que seja adotado.

Ao se analisar cenários prospectivos de uso da Internet das Coisas no âmbito educacional pelas instituições da administração pública conclui-se que embora seja uma sistemática complexa e ainda carente de aprimoramento, aduz a um crescimento significativo do cenário educacional, tendo em vista que o conhecimento pelo futuro está ligado à aplicabilidade da Internet, pois como dito, a população se consagra, hoje, por meio dos avanços tecnológicos.

Observou-se também outras sugestões de aplicabilidade da Internet das Coisas no âmbito educacional, como em bibliotecas, livros inteligentes, uso do celular para acessar laboratórios, livros, comprar lanches e também utilidade no quesito segurança dos alunos.

Compreende-se, desta forma, que ainda assim a Internet das Coisas é um campo promissor nos cenários prospectivos inclusive no âmbito educacional.

Uma política nacional de Internet das Coisas deve levar em conta a experiência brasileira de governança da Internet tradicional, atentando-se aos erros que foram cometidos no passado e buscando evitá-los nesta nova implementação, levando em conta também problemas como formação de capital humano, a criação de negócios, desenvolvimento de capacidades e soluções ligadas a inovação, em níveis de volume e qualidade global, gerando oportunidades para o Brasil dentro do mercado mundial, no qual, mesmo em um cenário de recessão econômica, torna-se uma oportunidade em potencial para guiar uma recuperação.

Uma vez que o Estado tem um papel indutor no desenvolvimento da IoT, no Brasil, espera-se que contribua para que a IoT assuma a experiência positiva de impacto social e para as boas práticas da gestão pública, preparando os cidadãos brasileiros para compreender como a tecnologia impacta na sociabilidade, não apenas delineando políticas eficientes, mas buscando com que a IoT se torne um mecanismo de empoderamento digital.

5.2 Recomendações de Trabalhos Futuros

Como trabalhos futuros, propõe-se:

1. Aplicar a Internet das Coisas no âmbito público, especificamente na área da educação, onde sejam analisados sua viabilidade, os resultados alcançados, a efetividade na prestação dos serviços educacionais, contribuindo para o gestor educacional melhorar suas práticas internas, facilitando a tomada de decisão e a relação entre pais e a escola, acelerando respostas, economizando e gerando recursos.
2. Avaliar os impactos no quesito segurança na prestação de serviços de IoT prestados no âmbito público.
3. Comparar o que já foi realizado na aplicação da IoT na educação pública no Brasil com o que está sendo aplicado em países desenvolvidos no mundo em apresentação dos resultados alcançados.

REFERÊNCIAS

ATZORI, L.; IERA, A.; MORABITO, G. The internet of things: A survey. **Elsevier**. Computer Networks, p. 1-19, 31 mai. 2010,

ATZORI, L.; IERA, A; MORABITO, G.; NITTI, M. The Social Internet of Things (SIoT) When Social Networks meet the Internet of Things: Concept, Architecture and Network Characterization I. **Elsevier**. Computer Networks. v.56, n. 16, p. 3594-3608, 14 nov. 2012,.

BOYKO, C. T.; COOPER, R.; DAVEY, C. L.; WOOTTON, A. B. et al. Addressing sustainability early in the urban design process. **Management of Environmental Quality: an International Journal**, v.17, n.6, p. 689-706, 2006.

CARDOSO, L. R. A. et al. **Prospecção de futuro e Método Delphi: uma aplicação para a cadeia produtiva da construção habitacional.** Ambiente Construído, Porto Alegre, v. 5, n. 3, p. 63-78, jul./set. 2005.

CASTELLS, M. **A sociedade em rede**. 6ª ed. São Paulo: Paz e Terra, 2012.

COELHO, F. D. Desenvolvimento local e sociedade da informação. In: L. DOWLOR; POCHMANN, M. (Org.), **Políticas para o desenvolvimento local.** São Paulo: Fundação Perseu Abramo, p. 337-365, 2010.

COSTA, P. L. O. C. **Qualidade e competência nas decisões**. 1ª ed. Blucher: São Paulo. 2007.

COSTA, P. L. O. C; CANUTO, S. A. **Administração com qualidade-Conhecimentos para a gestão moderna**. Blucher. São Paulo, 2010.

DUTTA, S. (Ed.). **The Global Innovation Index 2011: accelerating growth and development.** Fontainebleau: INSEAD. 2011.

FAROOQ, M. U; WASEEM, M.; KHAIRI,A.; MAZHAR, S. A Critical Analysis on the Security Concerns of Internet of Things (IoT). **International Journal of Computer Applications** (0975 8887)**,** v. 111, n. 7, p. 1-6, fev. 2015

GIL, A. C. **Como Elaborar Projetos de Pesquisa**. 5ª Ed. Atlas: São Paulo. 2010.

GRUMBACH, Raul José dos Santos. **Cenários Prospectivos:** Como construir um futuro melhor. Rio de Janeiro: FGV, 2002.

JESUS, D. F.; KLEINSCHMIDT, J. H. Estudo do Consumo de Energia do Protocolo DTLS para Internet das Coisas. Resumo estendido. **Computer on the Beach**, p. 504-506, 2015.

JIANG, Y.; ZHANG, L.; WANG, L. Wireless Sensor Networks and the Internet of Things. **International Journal of Distributed Sensor Networks.** Research Center for Mobile

Computing, Tsinghua University, Institute of Microelectronics, Tsinghua University, China, p. 1-7, 2013.

KHAN. R. **Future Internet:** The Internet of Things Architecture, Possible Applications and Key Challenges. 2012. Disponível em: <http://ieeexplore.ieee.org/stamp/ stamp.jsp?arnumber=6424332>. Acesso em: 06 jul. 2016.

KOMNINOS, N. et al. Developing a policy roadmap for smart cities and the future internet. In: **Echallenges Conference Proceedings Thessalonik:** URENIO - Urban and Regional Innovation Research, p.1-8, 2011.

LIU, H; BOLIC, M; NAYAK, A.; STOJMENOVIC, I. Taxonomy and challenges of the integration of rfid and wireless sensor networks. **IEEE Network**, IEEE, v. 22, n. 6, p. 926-935, 2008.

LUDKE, Menga; ANDRÉ, Marli E. D. **Pesquisa em educação:** abordagens qualitativas. 10. reimp. São Paulo: EPU, 2007.

LUO, Z. et al. An information-upload approach with low power consumption for a rfid-wsn smart node system. In: IEEE. **7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM).** [S.l.], p. 1–4, 2011.

MARCIAL, E. C.; GRUMBACH, R. J. S. **Cenários Prospectivos – Como Construir um Futuro Melhor**. Rio de Janeiro: Ed. FGV, 2002.

MASON, A; SHAW, A.; AL-SHAMMAAAM, A.; WELSBY,T. Rfid and wireless sensor integration for intelligent tracking systems. In: **Proceedings of 2nd GERI Annual Research Symposium GARS**, 2006.

MINAYO, M. C. S. (Org.). **Pesquisa social: teoria, método e criatividade.** Petrópolis: Vozes, 2000.

MIORANDI, D; SICARI, S.; PELLEGRINI, F.; CHLAMTAC, I. **Internet of things: Vision, applications and research challenges.** Ad Hoc Networks.v.10 n.7, p. 1497-1516, 2012.

NIC - National Intelligence Council), Disruptive Civil Technologies. Six Technologies with Potential Impacts on US Interests Out to 2025. **CONFERENCE REPORT CR.** April 2008-07, 2008.

OLIVEIRA, M.. M. **Como fazer Pesquisa Qualitativa**. Petrópolis: Vozes, v. 1000. 181 p, 2007.

PAGANO, P.; CHITINIS, M.; LIPARE, G. **Real-time applications in wirelles sensor networks.** Retis. Lab. Scuela Superiore Santa'ana Pisa. Italy. Dez. 2007.

POETAS.IT. **IoT - Uma Estratégia para o Brasil / Consolidação de uma visão unificada para orientação e proposição de políticas públicas sobre Internet das Coisas no Brasil v.1.2.** 2016. Creative Commons. Disponível em: www.cesar.org.br/poetas.it/visionstatement Acesso em: 05/12/2016

RIFKIN, J. **O fim dos empregos - O contínuo crescimento do desemprego em todo o mundo.** M. Books do Brasil Editora: São Paulo. 2004.

_____. **A Terceira Revolução Industrial - Como o poder lateral está transformando a energia, a economia e o mundo**. M. Books do Brasil Editora: São Paulo. 2012.

_____. **Sociedade com custo marginal zero - Internet das coisas, os bens comuns colaborativos e o eclipse do capitalismo**. M. Books do Brasil Editora. São Paulo, 2016.

REIS, J. G. M. et al. **Qualidade em redes de suprimentos - A qualidade aplicada ao supply chain management**. Atlas: São Paulo, 2015.

SARDENBERG, Ronaldo M. **Brasil 2020**: Parcerias Estratégicas, Brasília, nº10, março 2001. p.18-35.

SANDÍN, E., MARIA, P. **Investigación Cualitativa en Educación. Fundamentos y Tradiciones.** Madrid. Mc Graw and Hill Interamericana, 2003.

SILVA. M. C. **Segurança em aplicações de redes de sensores com IPv6.** Dissertação (Mestrado em Engenharia da Informática). Departamento de engenharia informática. Faculdade de ciências e tecnologia da Universidade de Coimbra, 2013.

STRAUSS, A.; CORBIN, J. **Pesquisa qualitativa: técnicas e procedimentos para o desenvolvimento de teoria fundamentada.** 2. ed. Porto Alegre: Artmed, 2008.

TOPPETA, D. **The smart city vision: how innovation and ICT can build smart, "livable", sustainable cities**. Milão: The Innovation Knowledge Foundation. 2010.

VALDEZ, T. A. S. **Regionalização e Integração Sistêmica:** cenários para a reforma do Sistema de Saúde de Cabo Verde. 2007. 240 f. Dissertação (Mestrado em Saúde Pública). Fundação Oswaldo Cruz - FIOCRUZ. Escola Nacional de Saúde Pública Sérgio Arouca. Rio de Janeiro, 2007.

WANG, L; XU, L.D; BI, Z.; XU, Y. Data cleaning for rfid and wsn integration. **IEEE Transactions on Industrial Informatics,** IEEE, v. 10, n. 1, 2014, p. 408-418, 2014.

WHITMORE, A. AGARWAL, A. XU, L. D. The Internet of Things - A survey of topics and trends.**Springer Science+Business Media**. New York, 2014.

WU, M. et al. Research on the architecture of Internet of things**. International Conference on Advanced Computer Theory and Engineering (ICACTE)**, 2010.

YOVANOF, G. S., HAZAPIS, G. N. **An architectural framework and enabling wireless technologies for digital cities and intelligent urban environments.** Wireless Personal Communications, v. 49, n. 3, p. 445-463, 2009.

ZAMBARDA, P. **'Internet das Coisas': entenda o conceito e o que muda com a tecnologia'.** 2014 Disponível em: <http://www.techtudo.com.br/noticias/noticia/2014/08/internet-das-coisas-entenda-o-conceito-e-o-que-muda-com-tecnologia.html>. Acesso em: 02 jul. 2016.

ZHAO, K.; GE, L. **A Survey on the Internet of Things Security.** Ninth International Conference on Computational Intelligence and Security, 2013.

ANEXOS

CONSULTA PÚBLICA - PLANO NACIONAL DE IoT

1. PESQUISA E DESENVOLVIMENTO

Objetivo: mapear o ecossistema de comunicação M2M e IoT no que diz respeito à pesquisa e desenvolvimento, vislumbrando possíveis ações de estímulo ao seu desenvolvimento tecnológico.

1 - Quais as atuais ações e instrumentos adotados pelo Estado Brasileiro para incentivar a pesquisa, o desenvolvimento e a inovação tecnológica para os setores relacionados à comunicação M2M e IoT?

2 - Existem ações não adotadas ainda pelo Estado Brasileiro, mas que poderiam impulsionar ainda mais PD&I nos setores relacionados à comunicação M2M e IoT?

3 - O Brasil aparece no Relatório do Índice Global de Inovação 2015 (Cornell University, INSEAD, e WIPO) na posição 70 de 141 países. O estudo aponta um cenário preocupante com relação ao percentual de graduações em ciência e engenharia em relação ao total de graduações, ocupando a posição 94. Os impactos do conhecimento e das tecnologias geradas (que incluem patentes, papers e citações) posicionam o país em 72º lugar. Já Índice Global de Talento Competitivo 2015-2016 (INSEAD, ADECCO and HCLI) coloca o Brasil em 67º lugar entre 109 países, com o subíndice de quantidade equivalente de pesquisadores em tempo integral por milhões de habitantes na posição 53. Quais os principais motivos para a atual atratividade dos cursos nas áreas de ciência e engenharia? Que iniciativas poderiam melhorar este cenário?

4 - Quais as oportunidades e barreiras existentes nas políticas públicas atuais de incentivo à PD&I, no âmbito do ecossistema de IoT?

5 - Existem problemas para a formação de redes de pesquisa e o fortalecimento dos vínculos entre os atores da produção de conhecimentos técnicos e científicos (universidades, institutos de pesquisa, parques tecnológicos, etc.), considerando-se as distintas camadas da arquitetura de IoT?

6 - Existem problemas na relação entre indústrias e provedores incumbentes de soluções e serviços de TICs, no que tange suas relações com o ecossistema de startups no Brasil? Que medidas devem ser consideradas para aproximar esses atores, aproveitando-se suas principais forças, isto é, capacidade de inovação das Startups em setores dinâmicos como IoT e capacidade de atuar em escala da indústria e provedores de serviços incumbentes?

7 - Há demanda para linhas de financiamento de pesquisa para P&D de produtos e aplicações para soluções de comunicação M2M e Internet das Coisas? Em que áreas? Cite necessidades e oportunidades de P&D.

8 - Quais as instituições de pesquisa nacionais que possuem estudos relacionados ao ecossistema de Internet das Coisas de forma relevante?

9 - Como poderia ser realizado o incentivo à criação de um ecossistema de empresas nascentes (startups) com elevado grau de inovação em IoT, através de apoio estatal (p.ex., o financiamento dos projetos ou simplificação das obrigações sobre tais empresas), reduzindo o risco à inovação?

10 - Considerando iniciativas e o ambiente de pesquisa e desenvolvimento, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

2. RECURSOS HUMANOS

Objetivo: mapear a capacidade técnica e as principais lacunas na mão-de-obra brasileira, para atuar nos diversos setores que envolvem soluções de comunicação M2M e IoT.

1 - A Comunicação M2M e a Internet das Coisas afetarão a educação em sentido amplo. As aplicações dessas tecnologias em diversas áreas dependerão de habilidades profissionais variadas e nos obriga a revisitar os processos educacionais de maneira holística e questioná-los do ponto de vista da melhoria que essas tecnologias podem representar. Considerando este contexto:

- Aponte qual(is) o(s) perfil(is) de profissional que será(ão) mais demandado(s) para o desenvolvimento do ecossistema de IoT;
- Quais são as principais barreiras do nosso atual processo educacional para a formação de novos profissionais para o mercado de IoT.

2 - Qual o impacto (positivo ou negativo) que a IoT pode provocar na força de trabalho?

3 - Quais os potenciais benefícios da IoT para empregados e/ou empregadores?

4 - Considerando aspectos relacionados a força de trabalho dedicada ao ecossistema de IoT, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

5 - O atual arranjo entre governo, universidade e empresas é adequado para a capacitação e formação de mão de obra aplicável à IoT?

3. OFERTA TECNOLÓGICA E COMPOSIÇÃO DE ECOSSISTEMAS

Objetivo: identificar qual o contexto atual da indústria brasileira de TIC, mapeando suas competências e oportunidades para o desenvolvimento do setor aplicado a IoT no Brasil.

1 - Considerando o setor de TICs no Brasil, que empresas apresentam produtos ou serviços que podem ser utilizados no desenvolvimento ou formação de um ecossistema local de IoT?

2 - Que instituições de pesquisa, no Brasil, desenvolvem tecnologias ou soluções que poderão ser relevantes na constituição do ecossistema de IoT no Brasil?

3 - Avaliando o potencial das entidades brasileiras de suprir às futuras demandas de IoT, quais são as ofertas de tecnologias, produtos e serviços que poderão contribuir para disseminação de IoT nos diversos segmentos econômicos brasileiros?

4 - Que alianças internacionais, no contexto da IoT, são relevantes para o desenvolvimento da IoT no Brasil?

5 - Identifique quais são os subsetores da cadeia de TIC mais relevantes para o desenvolvimento de IoT.

6 - Que nichos de mercado apresentam potencial para desenvolvimento de players locais?

7 - Em quais aplicações o Brasil pode ser competitivo em semicondutores?

8 - Em quais nichos de equipamentos eletrônicos o Brasil pode desenvolver tecnologia local em hardware/software embarcada?

9 - Em que área o Brasil pode desenvolver softwares de maior valor agregado, como software-ferramentas e/ou com elevado potencial de exportação?

10 - Considerando a oferta tecnológica e a composição do ecossistema de IoT, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

4. INVESTIMENTO, FINANCIAMENTO E FOMENTO

Objetivo: mapear fontes de investimento, canais de financiamento e iniciativas de fomento, existentes ou a serem estruturadas, com o propósito de incentivar o desenvolvimento do setor aplicado a IoT no Brasil.

1 - O acesso a crédito ainda é muito oneroso para as empresas brasileiras, com taxas de juros elevadas. Além disso, a quantidade e o valor de investimentos de capital de risco ainda são baixos – no Brasil este tipo de investimento representa apenas 0,01% do PIB, enquanto outros países têm volumes muito superiores em termos relativos como os EUA que investe 0,18%, a Índia 0,12%, e a China 0,07% do PIB. Quais as fontes e modelos de financiamento disponíveis hoje no país, que atendem ao ecossistema de IoT?

2 - Como você avalia a eficácia dessas fontes e modelos de financiamento no estímulo à inovação do País, bem como na introdução de novos serviços e produtos no mercado nacional? O que poderia ser melhorado?

3 - Considerando fontes de investimento, financiamento e fomento, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

4 - As estruturas de Venture Capital e Seed Capital existentes no Brasil são adequadas quando se considera a dinâmica de ecossistemas de inovação presentes em outros países?

5. DEMANDA

Objetivo: identificar os desafios e oportunidades nacionais nos quais a Internet das Coisas pode ter impacto significativo, tanto na esfera pública, quanto na privada. Adicionalmente, entender o potencial econômico que a Internet das Coisas pode trazer para nossa sociedade, por meio do mapeamento dos principais casos de uso.

a) Demanda pública

1 - Quais são as possíveis aplicações de IoT no Brasil na esfera pública, analisando todos os possíveis setores e ambientes de aplicação?

2 - Qual o impacto potencial estimado de IoT na economia, considerando os principais usos para o setor público no Brasil?

3 - Quais barreiras na esfera pública existentes atualmente nas diferentes áreas de aplicação de IoT que poderiam ser superadas com seu uso?

4 - Considerando o mapeamento e geração da demanda por soluções de IoT, existem outras questões relevantes no setor público que devem ser observadas para um completo diagnóstico da IoT no Brasil?

b) Demanda privada

5 - Considerando as verticais de aplicação de IoT mapeadas e listadas abaixo, dê exemplos de casos de uso em cada uma delas.

- Saúde
- Agricultura
- Infraestrutura
- Petróleo e gás
- Automotivo
- Bens de consumo e varejo

- Energia
- Logística
- Aeroespacial
- Eletrônicos avançados
- Mineração
- Telecomunicações e mídia
- Serviços bancários
- Cidades inteligentes
- Indústria 4.0
- Escritórios e residências inteligentes
- Pequenas e médias empresas

6 - Existe alguma vertical adicional relevante de aplicação de IoT além das previamente mapeadas?
7 - No âmbito global, quais as principais lacunas de atuação (“white-spaces”) onde o IoT poderia proporcionar importantes mudanças?
8 - Qual o impacto potencial estimado de IoT na economia, considerando os principais usos para o setor privado no Brasil?
9 - Quais barreiras na esfera privada existentes atualmente nas diferentes áreas de aplicação de IoT que poderiam ser superadas com seu uso?
10 - Considerando o mapeamento e geração da demanda por soluções de IoT, existem outras questões relevantes no setor privado que devem ser observadas para um completo diagnóstico da IoT no Brasil?

6. ASPIRAÇÕES

Objetivo: Obter uma visão sobre quais deveriam ser as aspirações iniciais para o desenvolvimento de IoT no Brasil.
1 - Considerando a situação atual de IoT no Brasil, quais deveriam ser as aspirações para o país a médio e longo prazo?
2 - Quais países possuem aspirações para IoT que podem ser usadas como referência pelo Brasil?

7. GERENCIAMENTO DE INFRAESTRUTURA

Objetivo: mapear as questões críticas para o gerenciamento da infraestrutura de IoT, em todas as suas camadas, com o objetivo de garantir a confiabilidade dessa estrutura através do comissionamento, monitoramento, aprovisionamento e configuração dos dispositivos sensores e atuadores, elementos de rede e infraestrutura computacional, suportando toda a operação.
1 - Na sua visão, quais aspectos devem ser desenvolvidos no que diz respeito à gestão de inventário, no ecossistema IoT? Justifique sua contribuição com casos de uso.

2 - Que questões relacionadas a instalação de dispositivos precisam ser consideradas no ecossistema IoT? Justifique sua contribuição com casos de uso.
3 - Quais os aspectos que necessitam de desenvolvimento no que diz respeito à gestão de configuração, no ecossistema IoT? Justifique sua contribuição com casos de uso.
4 - Quais os aspectos que necessitam de desenvolvimento no que diz respeito à faturamento, no ecossistema IoT? Justifique sua contribuição com casos de uso.
5 - Na sua visão, o que ainda precisa ser equacionado no que diz respeito à tratamento de falhas, no ecossistema IoT? Justifique sua contribuição com casos de uso.
6 - Que questões carecem de tratamento no que diz respeito à qualidade de serviço, no ecossistema IoT? Justifique sua contribuição com casos de uso.
7 - No que diz respeito à qualidade da experiência, no ecossistema IoT, que aspectos precisam ser desenvolvidos? Justifique sua contribuição com casos de uso.
8 - Na sua opinião, quais as principais questões que ainda devem ser equacionadas no que diz respeito à analytics, no ecossistema IoT? Justifique sua contribuição com casos de uso.
9 - Considerando as funcionalidades relacionadas nas questões anteriores, há necessidade de desenvolvimentos adicionais nos sistemas de gerenciamento para a implantação em larga escala da IoT? Neste aspecto, existe alguma especificidade para o caso do Brasil?
10 - Considerando aspectos de gerenciamento da infraestrutura, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

8. SUPORTE A APLICAÇÃO E SERVIÇOS

Objetivo: mapear as questões relevantes nesta camada que provê abstrações de alto nível para uma ampla gama de dispositivos de internet das coisas, acelerando o desenvolvimento de aplicações de alto valor agregado através de serviços que contemplam: Gerenciamento de dispositivos; Padronização de API para monitoramento e atuação em dispositivos; Configuração de dispositivos virtuais (dispositivos cujo estado atual é o resultado da agregação ou transformação de estado de múltiplos dispositivos físicos); Geração de eventos e alertas de valor agregado; Gerenciamento de histórico de eventos e comandos, entre outros. Além de propiciar a interoperabilidade entre aplicações.
1 - A interoperabilidade é a capacidade de um sistema ou aplicação de se comunicar de forma transparente (ou o mais próximo disso) com outro sistema ou aplicação (semelhante ou não). Pode-se dizer que a interoperabilidade pressupõe a comunicação entre sistemas e, consequentemente, troca de dados. No contexto do desenvolvimento e implantação da tecnologia IoT, qual é a importância de haver ou não interoperabilidade entre as aplicações? Justifique e dê exemplos, se possível.
2 - As aplicações IoT podem ser desenvolvidas sem necessariamente utilizar a camada de suporte a aplicações e serviços. Na sua visão essa camada será comum na maioria dos casos de uso ou será considerada como um overhead desnecessário? Se sim, quais as principais facilidades que tal camada deveria ter? Quais oferecem oportunidades para desenvolvimento local? Justifique e dê exemplos.

3 - Já existem diversas ofertas comerciais de soluções para a camada de suporte a serviços e aplicações de IoT de código fechado e algumas iniciativas de código aberto. Na sua visão, qual destes dois modelos terá maior adoção?
4 - Na sua visão, todas as funcionalidades desejáveis para a camada de suporte a aplicações e serviços deveriam ser providas por uma única solução? Caso contrário, como você vê a interoperabilidade entre soluções?
5 - Em geral essa camada se vale de infraestrutura computacional em nuvem. Na sua visão, essa nuvem seria pública, privada ou mista? O quanto IoT será significativa no crescimento deste mercado? Existem oportunidades de oferta nacional de IaaS / PaaS / SaaS para atender as demandas de IoT?
6 - Uma das áreas da computação que mais tem evoluído nos últimos 5 anos é Machine Learning. Na sua visão que facilidades a camada de suporte a serviços e aplicações deve prover, neste contexto, para viabilizar o desenvolvimento das aplicações? Dê exemplos com base em casos de uso.
7 - Qual o impacto do Machine Learning para IoT e quais oportunidades existem para o desenvolvimento local?
8 - Além do Machine Learning, que outras áreas da computação oferecem oportunidades para desenvolvimento local, no ecossistema de IoT? Que dificuldades devem ser superadas para tal?
9 - No contexto de analytics, que facilidades a camada de suporte a serviços e aplicações deve prover, para viabilizar o desenvolvimento das aplicações? Dê exemplos com base em casos de uso.
10 - No contexto de manipulação de dados espaço-temporal, onde os dispositivos informam o local e o tempo da informação, que facilidades a camada de suporte a serviços e aplicações deve prover, para viabilizar o desenvolvimento das aplicações? Dê exemplos com base em casos de uso.
11 - Considerando aspectos de suporte a aplicações e serviços, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

9. REDES E TRANSPORTE DE DADOS

Objetivo: Identificar as tecnologias de comunicação para IoT, as soluções com maior potencial para atender os diferentes casos de uso, o melhor uso do espectro de frequência para a conectividade dos dispositivos e questões de adoção de padrões e interoperabilidade.

1 - Uma forma de facilitar a interoperabilidade é o desenvolvimento de soluções em padrões de acesso já consolidados no mercado, como, por exemplo: ethernet, WiFi, Bluetooth, entre outros. Qual a necessidade de desenvolvimento de novos padrões de acesso para atender as necessidades específicas da IoT? Considere em sua resposta eventuais limitações que as tecnologias de acesso já consolidadas apresentam no contexto de IoT, em função dos diversos casos de uso (IoT para missão crítica e IoT massivo).
2 - Em que pese as tecnologias de acesso que podem ser adotadas na implantação de um ecossistema de IoT, em sua opinião, quais se mostram mais interessantes ou à prova de futuro e por quê?
3 - Considerando a questão de interoperabilidade, com respeito a tecnologias do core da rede qual a necessidade de desenvolvimento de novos padrões para atender as necessidades específicas da IoT? Considere em sua resposta eventuais limitações que as tecnologias de core já consolidadas apresentam no contexto de IoT, em função dos diversos casos de uso (IoT para missão crítica e IoT massivo).
4 - Em que pese as tecnologias de core da rede que podem ser adotadas na implantação de um ecossistema de IoT, em sua opinião, quais se mostram mais interessantes ou à prova de futuro e por quê?

5 - Considerando a questão de interoperabilidade, com respeito a protocolos qual a necessidade de desenvolvimento de novos padrões para atender as necessidades específicas da IoT? Considere em sua resposta eventuais limitações que os protocolos já consolidados apresentam no contexto de IoT, em função dos diversos casos de uso (IoT para missão crítica e IoT massivo).
6 - Em que pese a multiplicidade de protocolos que podem ser adotados na implantação de um ecossistema de IoT, em sua opinião, quais se mostram mais interessantes ou à "prova do futuro" e por quê?
7 - Na sua visão a IoT irá impactar o core da rede, ou a evolução destas tecnologias atualmente focadas no aumento de throughput para suportar serviços como vídeo em alta definição irá também acomodar naturalmente as demandas da IoT? A IoT deverá impactar ou ser impactada por novas tecnologias de core de rede como o SDN (Software Defined Network), convergência IP e óptica, dentre outras?
8 - Hoje as tecnologias para o acesso de dispositivos IoT (Wi-Fi HaLow, ZigBee, ZWave, Bluetooth LE, GSM, HSPA, LTE, LoRa, SigFox, LTE-M, NB-IoT, EC-GSM) se encontram padronizadas ou em vias de. Em sua opinião, quais os principais desafios a servem vencidos no que diz respeito à especificação dessas tecnologias para o desenvolvimento do ecossistema de IoT? Há necessidade de desenvolvimento de aspectos tecnológicos específicos para o Brasil? Há espaço para a indústria nacional desenvolver ofertas no que diz respeito à equipamentos de rede para IoT?
9 - Para soluções de conectividade IoT em área ampla (ex. LoRa, UNB, NB-IoT, EC-GSM), as que se baseiam em espectro não licenciado possuem mais ou menos potencial para a ampla adoção em comparação às soluções de espectro licenciado? Considerando-se fatores técnicos, a atual composição das faixas de frequência no Brasil é favorável para o desenvolvimento da IoT? Quais são as alterações sugeridas para fomentar o uso da IoT?
10 - Qual o impacto que o desenvolvimento e implantação do 5G trará para IoT? Em que medida o desenvolvimento da IoT depende do 5G?
11 - Qual a necessidade do conjunto de protocolos TCP/IP, em especial o IP na versão 6 (mesmo com adaptações como o 6LoWPAN), serem suportados nativamente em todos os dispositivos finais? Justifique a sua resposta baseando-se em casos de uso.
12 - Considerando aspectos relacionados a redes e comunicação de dados, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

10. GATEWAYS E DISPOSITIVOS

Objetivo: mapear as questões relevantes às capacidades e funcionalidades dos dispositivos e gateways, o que inclui entender os elementos que o compõe, como modem, processador, firmware, memória, sensores e atuadores, considerando restrições como custo, consumo energético, e largura de banda.

1 - Em sua opinião, quais os principais desafios a serem vencidos no que diz respeito as tecnologias para o desenvolvimento de dispositivos e gateways no ecossistema de IoT? Qual o espaço para empresas nacionais atuarem neste segmento?
2 - No que diz respeito a microcontroladores de pequena capacidade e baixo consumo (ex.: ARM Cortex-M, Quark Intel), que arquiteturas se mostram mais interessantes ou à prova de futuro e por quê? Há espaço para desenvolvimento de novas arquiteturas de processadores em âmbito nacional?

3 - No que diz respeito a baterias de longa duração e elementos de captação energia, que tendências tecnológicas são vislumbradas para o curto e médio prazos, e quais seus potenciais impactos no ecossistema de IoT? Há espaço para desenvolvimento de novas tecnologias de sistemas de geração, armazenamento e captação de energia em âmbito nacional?

4 - Levando em consideração a multiplicidade de aplicações que podem ser implantadas, quais famílias de sensores (MEMS, PFOE, Ópticos, etc) apresentam maiores oportunidades de desenvolvimento local? Justifique com exemplos.

5 - Os sistemas operacionais embarcados de código livre e demais bibliotecas já se encontram em maturidade suficiente para atenderem os casos de uso de IoT ou ainda há gaps? Considere na sua resposta questões como suporte a novos protocolos de rede e mecanismos de segurança, assim como sua aderência à estratégia de uso/adoção

6 - O papel dos Gateways é relevante na maioria dos casos de uso de IoT ou a tendência mais proeminente é os dispositivos terem acesso direto a Internet? Considere em sua resposta aspectos tais como a capacidade de processamento, processamento distribuído, interação entre dispositivos e autonomia para a tomada de decisão.

7 - Na sua visão, qual tendência é prevalente: dispositivos/gateways dotados de menor capacidade de processamento ou dispositivos/gateways com maior potencial para tomada de decisão de forma autônoma? Justifique com exemplos.

8 - Em relação aos protocolos de comunicação entre dispositivos, quais dos protocolos disponíveis são à prova de futuro? Neste contexto, qual é o nível de maturidade necessária à um padrão aberto para que ele alcance a adoção mundial no cenário IoT?

9 - Considerando o volume de dados e os protocolos existentes, quais são os avanços tecnológicos necessários para memórias de Gateways e dispositivos, para que estas atendam as questões de segurança e autonomia demandadas pelas aplicações em IoT?

10 - Qual o potencial dos Smartphones atuarem como Gateways para os dispositivos IoT? Esse cenário será comum? Se sim, em quais casos de uso?

11 - Considerando aspectos relacionados a dispositivos e gateways, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

11. SEGURANÇA E PRIVACIDADE

Objetivo: abordar como lidar com as questões relacionadas à segurança geral do ecossistema de IoT, bem como das informações e privacidade dos dados em um ambiente que, a cada dia, estará mais conectado utilizando mais informações potencialmente relacionadas com indivíduos, em nome da melhoria das prestações de serviços, pertinentes as suas liberdades individuais – v.g. localização, saúde, bens adquiridos.

1 - A partir do momento que um dispositivo se conecta à Internet com dados do seu usuário e transmite informações/se comunica com outros dispositivos, várias ameaças surgem:

a) Violação de privacidade: a violação de privacidade é a primeira, mais óbvia. Como o ambiente M2M/IoT pode coletar informações sobre um usuário, alguma outra parte pode se aproveitar disso para prejudicá-lo. É uma ameaça horizontal, ou seja, afeta todas as áreas.

b) Segurança física: segurança física do usuário também entra em risco, uma vez que não é mais preciso ter proximidade física para causar lesões à indivíduos. Para citar uma ameaça possível na área residencial, por exemplo, seria possível provocar um vazamento de gás e explodir uma casa remotamente. Outro exemplo de ameaça possível é provocar acidentes remotamente em carros conectados ou em indústrias automatizadas. Trata-se de uma ameaça horizontal.

c) Ataques distribuídos: a perspectiva é ter bilhões de dispositivos IoT e se pegarmos uma grande parcela deles é possível realizar ataques distribuídos, como por exemplo, um ataque de negação de serviço a uma rede de transmissão e de distribuição de energia. Novamente é uma ameaça horizontal.

d) Perdas financeiras: perdas financeiras podem acontecer através de fraudes em dispositivos IoT. Para citar uma ameaça possível nas áreas residencial e elétrico, seria possível alterar o consumo de uma casa, por exemplo, registrar 100 kW no medidor de energia quando o consumo real foi 1 MW. Trata-se de uma ameaça horizontal.

Nesse aspecto, o trabalho do OWASP (Open Web Application Security Project) ilustra perfeitamente a complexidade e a imaturidade do mercado no que se refere à segurança em ambientes M2M/IoT, haja vista as seguintes falhas de segurança:

1. Interface web insegura
2. Autenticação e autorização insuficientes
3. Serviços de rede inseguros
4. Ausência de transporte seguro
5. Preocupações com a privacidade
6. Interface com a nuvem insegura
7. Interface móvel insegura
8. Configurações de segurança insuficientes
9. Software e firmware inseguros
10. Segurança física deficiente

Essas falhas típicas do mundo pré-IoT serão fonte de ameaças ainda maiores no ambiente M2M/IoT, uma vez que esse novo ambiente é caracterizado por:

1. Grande quantidade de fornecedores de dispositivos, muitos dos quais sem qualquer experiência em segurança.
2. Há dispositivos IoT feitos para serem descartáveis.
3. Existem dificuldades em se realizar atualizações.
4. Controles tradicionais necessitam de adaptação ou não funcionam no escopo de IoT.
5. Há maior superfície de ataque.

Desse modo, fica claro que a segurança e a privacidade devem ser blocos essenciais de qualquer modelo de referência para IoT, sendo necessário uma implementação adequada em todas as camadas, do hardware ao software, das aplicações de negócio e de controle. Portanto, é importante que a segurança e a privacidade sejam tratadas em todas as etapas de desenvolvimento de um produto ou serviço comercializado no mercado, incluindo avaliações sobre a segurança do dispositivo, o software, a gestão de identidades e controle de acesso, a comunicação entre dispositivos e sistemas e o monitoramento e tratamento de incidentes de segurança.

Em linhas gerais, partindo do modelo preconizado pelo ITU, o qual estabelece camadas de Aplicação, Suporte a serviços de aplicações, Rede, Dispositivos e Gestão, há uma camada de capacidade de Segurança que deve ser responsável por:

a) Na camada de aplicação: autorização, autenticação, proteção à integridade e confidencialidade de dados, proteção à privacidade, auditoria de segurança e antivírus;

b) Na camada de rede: autorização, autenticação, confidencialidade de dados de uso e de sinalização, e proteção de integridade de sinalização;

c) Na camada de dispositivos: autenticação, autorização, validação de integridade do dispositivo, confidencialidade de acesso, controle e dados e proteção de integridade.

Com base nesse contexto, quais os desafios para a implementação dessas camadas de capacidade de segurança em dispositivos M2M/IoT? Em sua opinião, existe no contexto de M2M/IoT a necessidade de novos mecanismos de segurança, devido a particularidades desses novos ambientes? Se sim, existe oportunidade para desenvolvimento local? Poderia citá-los juntamente com os cenários de uso?

2 - Quanto a criptografia, embora ela seja técnica fundamental para se manter a segurança e a privacidade em dispositivos M2M/IoT, a grande maioria dos dispositivos possui limitações técnicas e de capacidade de processamento que dificultam a utilização de soluções de criptografia robustas. Desse modo, quais algoritmos e soluções de criptografia devem ser incentivados em dispositivos M2M/IoT para garantir eficiência e segurança no ecossistema?

3 - Conceitualmente, o ecossistema de IoT exige a cooperação e compartilhamento de informações entre seus agentes, em especial para se ter uma rápida divulgação de vulnerabilidades de software que possam comprometer a segurança de toda a rede. Como desenvolver um ambiente de cooperação entre os agentes do ecossistema de M2M/IoT? Em especial, como prevenir os riscos de ataques de negação de serviço massivos implementados através de redes de dispositivos M2M/IoT?

4 - No que tange a privacidade e proteção de dados pessoais, além das vulnerabilidades já mencionadas é importante ter em mente que o ecossistema de M2M/IoT poderá potencializar os negócios com big data, em especial com empresas interessadas em monetizar bases de dados, seja para fins publicitários ou outras destinações. Essas bases de dados podem possuir dados pessoais individualizados ou dados agregados/anonimizados sobre indivíduos. Nesse cenário, ciente da coleta e comunicação de dados potencializada pelo desenvolvimento do ecossistema de M2M/IoT, qual a abordagem legal, existente ou a ser implementada, necessária para proteger a privacidade e os dados pessoais dos indivíduos? Como deve ser tratada a coleta de dados de sensores IoT? Existem experiências estrangeiras que lidam com o binômio desenvolvimento e proteção à privacidade dos indivíduos no ecossistema M2M/IoT? Os projetos de lei em trâmite no Congresso Nacional referentes a proteção de dados pessoais (PL 4060/2012 da Câmara dos Deputados, PL 330/2013 do Senado e PL 5276/2016 de Autoria do Executivo) possuem regras adequadas para lidar com esse cenário e ao mesmo tempo possibilitar o desenvolvimento do ecossistema de M2M/IoT? É possível desenvolver dispositivos M2M/IoT com “políticas de privacidade” embarcadas, de modo a possibilitar a comunicação entre dispositivos com políticas compatíveis?

Na sua contribuição, considere os seguintes perfis de indivíduos:

-Que admitem o uso de dados dos dispositivos associados à sua identidade;

-Que só admitem o uso de dados do dispositivo se desassociados de sua identidade;

-Que não admitem o uso de dados do dispositivo associados e desassociados de sua identidade.

5 - Para se criar um ambiente de inovação disruptivo, algumas premissas devem ser atendidas, como o não confinamento de recursos e a liberdade de aplicação de dados, por exemplo. Estas tratam, respectivamente, do uso de um mesmo dispositivo e de informações para fins diferentes dos originalmente previstos. Dentre elas pousam questões de segurança sobre as duas primeiras premissas.

Vamos explicar seus significados:

Os recursos não podem estar confinados. Não confinar recursos significa utilizar um mesmo dispositivo para aplicações diversas. Por exemplo, a mesma câmera que monitore a segurança nas ruas também pode medir iluminação, otimizar tempo de semáforo por contagem de carros em uma via, pode estar acessível ao cidadão para monitorar seu carro estacionado, existência de vaga de estacionamento, presença de taxi livre ou mesmo para verificar se um ônibus se aproxima do ponto para o qual alguém se desloca.

Deve haver liberdade na aplicação dos dados, sem que isso implique em violações a privacidade e aos dados pessoais dos indivíduos. Um equipamento monitor de pressão arterial é utilizado com frequência para verificação de doenças coronarianas. Os dados são utilizados apenas por seu médico e depois descartados. Ocorre que pode haver diversos outros indivíduos interessados no conjunto de informações cardíacas agregadas e anonimizadas da população e, por isso, dispostas a oferecer contrapartida pela informação, o mesmo sendo válido para centros de pesquisas e universidades para elaboração de estudos científicos. Entretanto, a mesma informação poderia vir a ser utilizada por seu plano de saúde, sua seguradora implicando em graves violações a privacidade e proteção de dados pessoais dos indivíduos.

Neste contexto, questiona-se:

- Quais os limites de segurança e privacidade na premissa de não confinamento de recursos para que seja fomentado o ambiente de inovação?
- Como fomentar um ambiente de compartilhamento de informações de modo a aprimorar os padrões de segurança em IoT?
- Quais padrões e modelos de anonimização de dados devem ser implementados de modo a possibilitar o não confinamento de dados em IoT?
- Até que ponto a premissa de liberdade na aplicação dos dados pode ser utilizada de maneira virtuosa para o conjunto da sociedade?

6 - Existem outros fatores de Segurança e privacidade que possam criar barreiras ao desenvolvimento do ecossistema de IoT?

12. PAPEL DO ESTADO

Objetivo: identificar oportunidades e desafios no papel do estado, no que diz respeito ao modelo de governança de IoT no Brasil e ao direcionamento de modelos de negócio, com o objetivo de alavancar o desenvolvimento do ecossistema de M2M/IoT.

1 - Diante de um cenário novo e ainda incerto, qual deveria ser o papel do Estado no desenvolvimento do ecossistema de M2M e IoT?

2 - Em que áreas ou fases o Estado deverá exercer uma coordenação das ações para desenvolvimento do ecossistema de IoT?

3 - Seria interessante a atuação do Estado na formação de novos mercados de nicho para IOT? Por quê? Exemplifique.

4 - Cabe ao Estado desenvolver ou adaptar instrumentos fiscais visando o desenvolvimento e comercialização de produtos que se encaixam nas distintas camadas da IoT, conforme arquitetura apresentada? Por quê? De que forma os instrumentos atuais podem obstruir o desenvolvimento?

5 - Existem questões sobre como o Estado assegura a preservação dos direitos de propriedade intelectual (patentes e registros de software) que desfavorece o desenvolvimento da IoT, no Brasil?

6 - Existem barreiras de entrada que dificultam a localização da produção de soluções tecnológicas para IoT, no Brasil? Se sim, exemplifique.

7 - A Internet das Coisas vai afetar diferentes setores, de diferentes formas, em diferentes momentos. Os governos irão se beneficiar enormemente. A Cisco identifica quatro potenciais alavancas de economia no setor público: produtividade dos funcionários, redução de custos, melhoria da experiência do cidadão e aumento das receitas. A análise estima que mais de 25% de um valor estimado de US$ 19 trilhões do valor do mercado global disponível até 2022 pode ser realizado pelo setor público. Para usufruir desses benefícios – e ao mesmo tempo fomentar o mercado, dando escala aos fornecedores de soluções –, o Governo pode se tornar um demandante de soluções que utilizem a Internet das Coisas.

8 - Os municípios são os espaços onde os benefícios com implantação do ecossistema de M2M/IoT são descritos como os mais imediatos. Os estados, por sua vez, podem usufruir desse ambiente na melhoria da prestação dos seus serviços. Já a União tem desafios, sobretudo logísticos, em que a aplicação de tecnologia e inteligência de dados é fundamental para tornar mais eficientes setores como energia, transporte e saúde, por exemplo.

9 - Quais são as principais áreas de aplicações de IoT que podem melhorar os serviços públicos ou a gestão pública nas diferentes esferas?

10 - Ainda nesse contexto, que problemas específicos você sugeriria que o Governo resolvesse por meio dessas novas tecnologias e quais seriam as áreas prioritárias de atuação e os meios de contratação existentes mais adequados?

11 - No âmbito da atual legislação, há dificuldades para a aquisição pelos Entes da Federação das soluções que utilizam as tecnologias de Comunicação M2M e Internet das Coisas? Justifique preferencialmente com detalhes e exemplos.

12 - Na busca pelo desenvolvimento do ecossistema de IoT, qual deveria ser o papel das parcerias público-privadas (PPPs)?

13 - De que forma a burocracia brasileira pode ser uma barreira ao desenvolvimento de IoT?

14 - Quais são atualmente os países de referência em políticas públicas de IoT?

15 - De que forma as soluções demandadas pelo governo devem ser especificadas, buscando, na medida do possível, aproximar a demanda brasileira da que seria uma demanda em um mercado internacional, facilitando uma posterior exportação dos bens e serviços?

16 - Considerando a atuação do Estado no ecossistema de IoT, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

13. ASSUNTOS REGULATÓRIOS

Objetivo: Identificar as possíveis questões regulatórias (incluindo questões fiscais e tributárias) que necessitam de criação ou alteração de legislação ou regulamentos para que os negócios que envolvam comunicação M2M/IoT possam se desenvolver.

Os sistemas regulatórios vêm apresentando expressiva expansão nos últimos anos, em diferentes áreas de atuação estatal de diversos países que buscam crescimento econômico sustentável. Um Sistema de Gestão Regulatória robusto tem como foco a regulação de alta qualidade, que não distorce desnecessariamente a concorrência; é simples, proporcional, consistente, transparente e atende aos objetivos de política pública a que se destina com o menor custo possível para a sociedade e considerando as novas tecnologias, tais como a Internet das Coisas. Diante deste cenário, considere em sua contribuição os aspectos relacionados a seguir:

- Estágio atual do sistema regulatório do Brasil, no que tange à Internet das Coisas;
- As lacunas na legislação brasileira que podem constituir desafios à difusão de IoT no país;
- Disposições legais ou regulamentares que consistam em barreiras à entrada e que prejudiquem modelos de negócio IoT; e
- O nível de regulação adequado para a rápida adoção e massificação da tecnologia IoT no Brasil.

Segundo o Decreto n. 8.234/2014, são considerados "sistemas de comunicação máquina a máquina os dispositivos que, sem intervenção humana, utilizem redes de telecomunicações para transmitir dados a aplicações remotas com o objetivo de monitorar, medir e controlar o próprio dispositivo, o ambiente ao seu redor ou sistemas de dados a ele conectados por meio dessas redes". As atividades inerentes a um sistema IoT, de ponta a ponta, abrangem tanto serviços de telecomunicações quanto serviços de valor adicionado ("SVA"), nos termos da Lei Geral de Telecomunicações (Lei n. 9.472/97 – LGT), assim definidos:

- Serviços de telecomunicações como o "conjunto de atividades que possibilita a oferta de telecomunicação", entendendo-se, por telecomunicação, a "transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza" (LGT, art. 60);
- Serviços de Valor Adicionado (SVA) como a "atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações" (LGT, art. 61)

Por exemplo, os serviços de Tecnologia de Rastreamento e Monitoramento veicular, são compostos por: (i) um serviço de telecomunicações que dá suporte à conexão entre os equipamentos embarcados nos veículos; e (ii) um serviço de valor adicionado correspondente ao rastreamento propriamente dito e análise dos dados gerados pelos equipamentos embarcados nos veículos.

As dúvidas surgem quando a comunicação não fica restrita à IoT, permitindo adicionalmente o uso de serviços de telecomunicações pelos proprietários das "coisas". Partindo do exemplo anterior, seria o caso de um sistema de rastreamento que também disponibilizasse a conexão à internet para comunicação do usuário do veículo com outros usuários dos serviços de telecomunicações. Nesse caso, a empresa de Tecnologia de Rastreamento e Monitoramento atuaria como uma revendedora de serviço de telecomunicações, o que demandaria a obtenção das autorizações necessárias junto aos órgãos competentes.

Nesse contexto, questiona-se:

1. Esse enquadramento regulatório é adequado? Ele traz problemas ou limitações para os sistemas IoT?

2. Seria mais adequado haver outro enquadramento regulatório – v.g. considerar todas as atividades compreendidas como serviços de telecomunicações ou SVA? Caso positivo, identificar qual seria e se haveria (ou não) necessidade de alteração regulamentar ou legislativa.

3. A definição de IoT presente no Decreto n. 8.234/2014 é suficiente e adequada ou ela impede o desenvolvimento de alguma atividade?

4. Há a necessidade de se estabelecer um enquadramento regulatório de acordo com o nível de interação humana nos dispositivos M2M/IoT?

5. A figura do Mobile Virtual Network Operator ("MVNO"), prevista atualmente na regulamentação setorial, deve ser tratada para verificar a necessidade de cobrir eventuais lacunas na atuação dos agentes em sistemas IoT, levando em consideração os impactos na regulação?

6. Faz sentido ter um arcabouço regulatório especifico para IoT/M2M?

7. O conjunto de dispositivos que requeiram conectividade deveria ter um arcabouço regulatório próprio, visto que as complexas obrigações das operadoras e os diretos e deveres dos usuários dos serviços de telecomunicações muitas vezes são inconsistentes no cenário de conectividade de máquinas?

8. O eventual roaming internacional permanente (p.ex., chips de dispositivos operando no Brasil mas conectados permanentemente à operadoras de outros países) deveria passar a ser permitido?

9. A permissão de utilização comercial das faixas de radiofrequência dos "espaços brancos" (White spaces) seria uma alternativa para a comunicação entre dispositivos M2M/IoT?

10. Em relação a utilização das faixas de radiofrequência de radiação restrita pelo ecossistema de M2M/IoT, há necessidade de avaliar alterações regulatórias, considerando seus impactos setoriais?

11. Quais referências internacionais comparáveis podem ser utilizadas do ponto de vista de regulação/legislação? Em especial, discorrer como a legislação estrangeira de referência trata dos seguintes temas:

- Definição de padrões de segurança e/ou requisitos específicos para a homologação de equipamentos IoT pelos órgãos competentes;
- Definição de padrões de qualidade/confiabilidade para serviços de telecomunicação que servem de suporte à IoT e eventual existência de assimetrias em relação aos serviços de telecomunicações destinados aos usuários em geral;
- Destinação de radiofrequências aos serviços de telecomunicações que servem de suporte a sistemas IoT e regras de utilização, inclusive em relação à interferência com outros serviços;
- Outras assimetrias regulatórias e tributárias entre os serviços de telecomunicações destinados a IoT e aos usuários em geral;

12. Quais os prós e contras de se permitir o roaming permanente internacional? Quais foram os efeitos da permissão nos mercados locais de outros países?

13. A questão de interoperabilidade está intimamente ligada à forma de sua validação ou certificação. O modelo de certificação para IoT deve garantir que toda a solução seja interoperável garantindo ao usuário final a fruição do serviço/aplicação que escolheu. Dentre as formas de certificação, compulsória ou voluntária, em sua opinião, qual se mostra mais adequada ao desenvolvimento do ecossistema de IoT no Brasil? Justifique.

14. Considerando aspectos regulatórios e de legislação, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

15. Qual impacto a carga tributária do Brasil pode ter sobre o ecossistema de Internet das Coisas?

16. Existem outros fatores fiscais ou tributários que impeçam o desenvolvimento do Ecossistema?

Referência Bibliográfica

Portal Participa, Consulta Pública Plano Nacional de IoT. Disponível em: <http://participa.br/cpiot/itens-da-consulta >. Acesso em 02 de fevereiro de 2017.