UNIVERSIDADE FUMEC/FACE
FACULDADE DE CIÊNCIAS EMPRESARIAIS
CURSO DE MESTRADO PROFISSIONAL EM SISTEMAS DE INFORMAÇÃO E GESTÃO DO CONHECIMENTO

INTERNET DAS COISAS NO BRASIL: UMA ANÁLISE SOBRE PROPOSTAS DE CONECTIVIDADE E SUA ADERÊNCIA AOS ATRIBUTOS DE SEGURANÇA DA INFORMAÇÃO.

MANUEL DA ROCHA FIÚZA BRANCO JÚNIOR

Belo Horizonte
2019

MANUEL DA ROCHA FIÚZA BRANCO JÚNIOR

INTERNET DAS COISAS NO BRASIL: UMA ANÁLISE SOBRE PROPOSTAS DE CONECTIVIDADE E SUA ADERÊNCIA AOS ATRIBUTOS DE SEGURANÇA DA INFORMAÇÃO.

Dissertação apresentada ao Curso de Sistemas de Informação e Gestão do Conhecimento da Faculdade de Ciências Empresariais, da Universidade Fumec, como parte dos requisitos para a obtenção do título de Mestre em Sistemas de Informação e Gestão do Conhecimento.

Área de concentração: Gestão de Sistemas de Informação e Conhecimento

Linha de pesquisa: Tecnologia e Sistemas de Informação

Trilha de pesquisa: T3 Informação e Tecnologia

Orientador: Professor Doutor Luiz Cláudio Gomes Maia.

Belo Horizonte
2019

Dados Internacionais de Catalogação na Publicação (CIP)

B816i Branco Júnior, Manuel da Rocha Fiúza, 1959-

Internet das coisas no Brasil: uma análise sobre propostas de conectividade e sua aderência aos atributos de segurança da informação / Manuel da Rocha Fiúza Branco Júnior. - Belo Horizonte, 2019.

148 f.: il. ; 29,7 cm

Orientador: Luíz Cláudio Gomes Maia

Dissertação (Mestrado em Sistemas de Informação e Gestão do Conhecimento), Universidade FUMEC, Faculdade de Ciências Empresariais, Belo Horizonte, 2019.

1. Internet das coisas. 2. Conectividade (computadores). 3. Dispositivos de internet embarcados. I. Título. II. Maia, Luíz Cláudio Gomes. III. Universidade FUMEC, Faculdade de Ciências Empresariais, Belo Horizonte, 2019.

CDU: 004.738.5

Ficha catalográfica elaborada pela Biblioteca Universitária-FUMEC

FUMEC

Dissertação intitulada "**Internet das coisas no Brasil: uma análise sobre propostas de conectividade e sua aderência aos atributos da segurança da informação**" de autoria de Manuel da Rocha Fiúza Branco Junior, aprovada pela banca examinadora constituída pelos seguintes professores:

Prof. Dr. Luiz Cláudio Gomes Maia – Universidade FUMEC
(Orientador)

Prof. Dr. Rodrigo Moreno Marques – Universidade FUMEC
(Examinador Interno)

Prof. Dr. Cláudio Roberto Magalhães Pessoa – Universidade do Porto
(Examinador Externo)

Prof. Dr. Fernando Silva Parreiras
Coordenador do Programa de Pós-Graduação em Sistemas de Informação e Gestão do Conhecimento da Universidade FUMEC

Belo Horizonte, 18 de dezembro de 2019.

CAMPUS
Rua Cobre, 200 - Cruzeiro
30310-190 - Belo Horizonte, MG
Tel: (31) 3228-3000
www.fumec.br

AGRADECIMENTOS

Agradeço a todos que direta ou indiretamente me auxiliaram nesse trabalho.

Agradeço à minha esposa, Maria Celeste, e meus filhos, Daniela e Luciano, pela compreensão com as ausências.

Agradeço a todos os professores do curso de Sistemas de Informação e Gestão do Conhecimento pelo profissionalismo e dedicação, ao coordenador do curso, Professor Doutor Fernando Silva Parreiras, e em especial ao meu orientador, Professor Doutor Luiz Cláudio Gomes Maia, pela paciência, tranquilidade e luz nos momentos mais complicados.

Agradeço ainda aos colegas da Faculdade de Engenharia e Arquitetura, Professores Severino Dias Carneiro, Cássio Batista e Eduardo Winter e Professor Doutor Marco Elísio Marques, pelo apoio nas horas mais difíceis. Por fim, agradeço ao Professor Doutor Cláudio Roberto Magalhães Pessoa, primeiro orientador desse trabalho que, quis o destino, não pode terminar a orientação.

New quartermaster (Q) to 007:

- Age is no garantee of efficiency!

007 to Q:

- And youth is no garantee of innovation!

Skyfall - 2012

RESUMO

Tecnologias como o IoT (*Internet of Things* – Internet das Coisas) têm ganhado muita atenção pela possibilidade de trazer facilidade, agilidade e precisão dos computadores para a vida cotidiana. Entretanto, propostas de vários sistemas que disputam recursos finitos nas redes de telecomunicações e informática requerem atenção. Vários governos, empresas privadas e instituições de ensino e pesquisa têm atuado na prospecção de soluções de IoT para os problemas que enfrentam. Nesse contexto, a presente dissertação discorreu sobre as propostas de aplicações de IoT apresentadas no estudo do BNDES 'Internet das Coisas: Um Plano de Ação para o Brasil' para os ambientes Cidades, Saúde, Meio Rural e Indústria. O foco dado ao estudo foi sobre a conectividade planejada nas propostas e seu alinhamento com os atributos de Segurança da Informação: Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade. Também foi considerada a segurança dos dispositivos propostos para as redes IoT. Para isso, foram realizadas pesquisas bibliográficas e em bases de dados eletrônicos procurando por conceituação sobre IoT e descrição sistêmica das tecnologias de conectividade e segurança de dispositivos propostas. O processamento desse material foi realizado utilizando conceitos de Revisão da Literatura e os documentos selecionados submetidos ao processo de Análise de Conteúdo. Nas conclusões, foram identificadas características, pontos fortes e ameaças nas tecnologias de conectividade e segurança dos dispositivos propostas no plano do BNDES e sua influência na concepção dessas redes IoT.

Palavras-chave: Internet das Coisas. Conectividade IoT. Segurança de dispositivos IoT. Segurança da Informação.

ABSTRACT

Technologies such as the Internet of Things (IoT) have gained a lot of attention for bringing computers ease, agility and accuracy into everyday life. However, proposals for various systems that compete for finite resources in telecommunications and computer networks require attention. Several governments, private companies, and education and research institutions have been working on IoT solutions for the problems they face. In this context, the present dissertation discussed the proposals of IoT applications presented in the study of BNDES 'Internet of Things: An Action Plan for Brazil' for the Cities, Health, Rural, and Industry environments. The focus of the study was on the planned connectivity in the proposals and its alignment with the attributes of Information Security: Confidentiality, Integrity, Availability, Authenticity and Legality. The security of the proposed devices for IoT networks was also considered. For this purpose, bibliographic and electronic database searches were performed looking for IoT conceptualization and systemic description of the proposed connectivity and device security technologies. The processing of this material was performed using concepts of Literature Review and selected documents submitted to the Content Analysis process. In the conclusions, characteristics, strengths and threats were identified in the connectivity and device security technologies proposed in the BNDES plan and their influence on the design of these IoT networks.

Keywords: Internet of Things. IoT connectivity. IoT device security. Information security.

LISTA DE DIAGRAMAS

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

ABINC	Associação Brasileira de Internet das Coisas
ABNT	Associação Brasileira de Normas Técnicas
ADSL	*Asymmetrical Digital Subscriber Line*
AMPS	*Advanced Mobile Phone Service*
ANATEL	Agência Nacional de Telecomunicações
AIOTI	*Alliance for Internet of Things Innovation*
AMI	*Advanced Metering Infrastructure*
BI	*Business Intelligence*
BS	*British Standards*
BLE	*Bluetooth Low Energy*
BNDES	Banco Nacional de Desenvolvimento Econômico e Social
CAN bus	*Controller Area Network* (CAN) bus, barramento controlador de área de rede
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CDMA	*Code-Division Multiple Access*
CoE-IoT	*National Centre of Excellence for IoT*
CPqD	Centro de Pesquisa e Desenvolvimento em Telecomunicações
DDoS	*Distributed Denial of Service*
DoS	*Denial of Service*
DSL	*Digital Subscriber Lines*
DSM	*Digital Single Market*
DSSS	*Direct Sequence Spread Spectrum*
EC-GPRS	*Extended Coverage – General Packet Radio Services*
EDGE	*Enhanced Data rates for GSM Evolution*
EUA	Estados Unidos da América
FCC	*Federal Communications Commission*

FCAPS	*Fault, Configuration, Accounting, Performance and Security*
FDM	*Frequency Division Multiplexing*
FDMA	*Frequency-Division Multiple Access*
Fumec	Fundação Mineira de Educação e Cultura
FHSS	*Frequency Hoping Spread Spectrum*
GPON	*Gigabit Passive Optical Network*
GPRS	*General Packet Radio Services*
GPS	*Global Positioning System*
GSM	*Global System for Mobile Communications*, originalmente *Groupe Spécial Mobile*
GSMA	*Global System for Mobile Communications Association*
HR-DSSS	*High Rate Direct Sequence Spread Spectrum*
IEC	*International Electrotechnical Commission*
IEEE	*Institute of Electrical and Electronics Engineers*
IHM	Interface Homem Máquina
IIDF	*Internet Initiatives Development Fund*
IoT	*Internet of Things*, Internet das Coisas
ISO	*International Organization for Standardization*
ITAC	*IoT Acceleration Consortium*
ITU	*International Telecommunications Union*
LAN	*Local Area Network*
LoRa	*Long Range*
LPWA	*Low Power Wide Area*
LTE	*Long-Term Evolution*
LTE-M	*Long-Term Evolution – Machine-Type Communications*
MCTIC	Ministério da Ciência, Tecnologia, Inovações e Comunicação

MEMS	*MicroElectroMechanical Systems*
MITI	Ministério da Indústria e Tecnologia da Informação (China)
MMS	*Multimedia Messaging Service*
MTC	*Machine-Type Communications*
M2M	*Machine to Machine*
NB-IoT	*Narrow Band – Internet of Things*
NFC	*Near Field Communication*
NGN	*Next Generation Networks*
NHS	*National Health Service*
NMT	*Nordic Mobile Telephone*
OCR	*Optical Character Recognition*
OFDM	*Orthogonal Frequency-Division Multiplexing*
ONU	Organização das Nações Unidas
PAN	*Personal Area Networks*
PIB	Produto Interno Bruto
PLC	*Power Line Communications*
PPGSIGC	Programa de Pós-Graduação em Sistemas de Informação e Gestão do Conhecimento
PSTN	*Public Switched Telephone Network* (PSTN)
P&G	Procter & Gamble
P2P	*Point-to-Point*
RADAR	*Radio Detection And Ranging*
RFID	*Radio-Frequency IDentification*
RPMA	*Random Phase Multiple Access*
SCM	*Supply Chain Management*
SDMA	*Space-Division Multiple Access*

Sinef	Sistema de Informações dos Negócios da Fumec
SMART	*Systems and Modeling for Accelerated Research in Transportation*
SMS	*Short Message Service*
SUS	Sistema Único de Saúde
TCP/IP	*Transmission Control Protocol – Internet Protocol*
TDM	*Time-Division Multiplexing*
TDMA	*Time-Division Multiple Access*
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
UTI	Unidade de Tratamento Intensivo
UWB	*Ultra-Wide Band*
WBAN	*Wireless Body Area Network*
WEP	*Wired Equivalence Privacy*
Wi-Fi	*Wireless networking technology*
WLAN	*Wireless Local Area Network*
WMAN	*Wireless Metropolitan Area Network*
WPA	*Wired Protected Access*
WPAN	*Wireless Personal Area Network*
WWAN	*Wireless Wide Area Network*
1G	*First generation networks,* redes de primeira geração
2G	*Second generation networks,* redes de segunda geração
3G	*Third Generation networks,* redes de terceira geração
3GPP	*3rd Generation Partnership Project*
4G	*Fourth Generation networks,* redes de quarta geração
5G	*Fifth Generation networks,* redes de quinta geração

SUMÁRIO

1 INTRODUÇÃO

O mundo moderno tão corrido tem pedido por soluções que simplifiquem a vida cotidiana. Sistemas que permitam a ação direta de computadores e outros dispositivos de aquisição automática de dados nesses ambientes têm sido muito estudados. Nesse contexto, a Internet das Coisas (*Internet of Things* – IoT) tem ganhado espaço tanto no ambiente técnico e acadêmico quanto na mídia em geral. Uma pesquisa em um site de busca acadêmico realizada em 2017 sobre o termo IoT resultou em 628.000 resultados entre artigos, livros e outras publicações. A mesma pesquisa em 2019 encontrou 852.000, um aumento aproximado de 36% (GOOGLE ACADÊMICO, 2019).

Empresas no Brasil e no mundo têm investido em prospecção e soluções IoT para otimizar seus processos (MIGLIACCI, 2017). A alemã IoT *Analytics* apresenta informações sobre o mercado de IoT em geral divididas em tópicos como IoT Industrial/Indústria 4.0, *Smart City*, Software e Plataformas IoT, Conectividade IoT e Tecnologias Emergentes. As informações estão disponíveis em relatórios, bases de dados e opiniões técnicas e estão à venda por preços desde US$ 250.00 até US$ 10,000.00. Algumas informações são gratuitas e outras estão disponíveis somente para assinantes. Os pacotes de assinatura podem ser individuais (US$ 500.00 por mês) ou corporativos, sendo ainda possível assinar informações por tópico (IOT ANALYTICS, 2019). A Associação Brasileira de Internet das Coisas – ABINC, fundada em 2015, é uma organização sem fins lucrativos que visa o desenvolvimento da IoT em âmbito nacional. Essa associação tem por objetivo fomentar pesquisa, desenvolvimento e atividades comerciais relacionadas a IoT tanto na esfera pública quanto privada (ABINC, 2019).

No Brasil, foi veiculado o interesse em se realizarem testes de campo para implantação de sistemas IoT em Xerém, distrito do município de Duque de Caxias – RJ (OLIVEIRA, 2017). Atento a essas questões, o CPqD lançou em 2017 a plataforma aberta Dojot voltada para o desenvolvimento de aplicações IoT (MERKER, 2017). A plataforma Dojot conta com o apoio de empresas de TI e instituições de ensino, apresenta vários tutoriais em seu site e em 2018 foi adotada como solução de desenvolvimento de aplicações pela Fundação Parque Tecnológico de Itaipu (DOJOT, 2019). Todo esse movimento ressalta o destaque que o tema tem atraído.

Nesse contexto, o Banco Nacional de Desenvolvimento Econômico e Social (BNDES) e o Ministério da Ciência, Tecnologia, Inovações e Comunicação (MCTIC) elaboraram um amplo estudo sobre o tema intitulado ‘Internet das Coisas: Um Plano de Ação para o Brasil’, cujo

objetivo é “propor um plano de ação estratégico para o país em Internet das Coisas” dividido em quatro grandes fases:

a) Diagnóstico Geral e aspiração para o Brasil: Obtenção de visão geral do impacto de IoT no Brasil, entendimento das competências de TIC do País e definição de aspirações iniciais para IoT no Brasil;

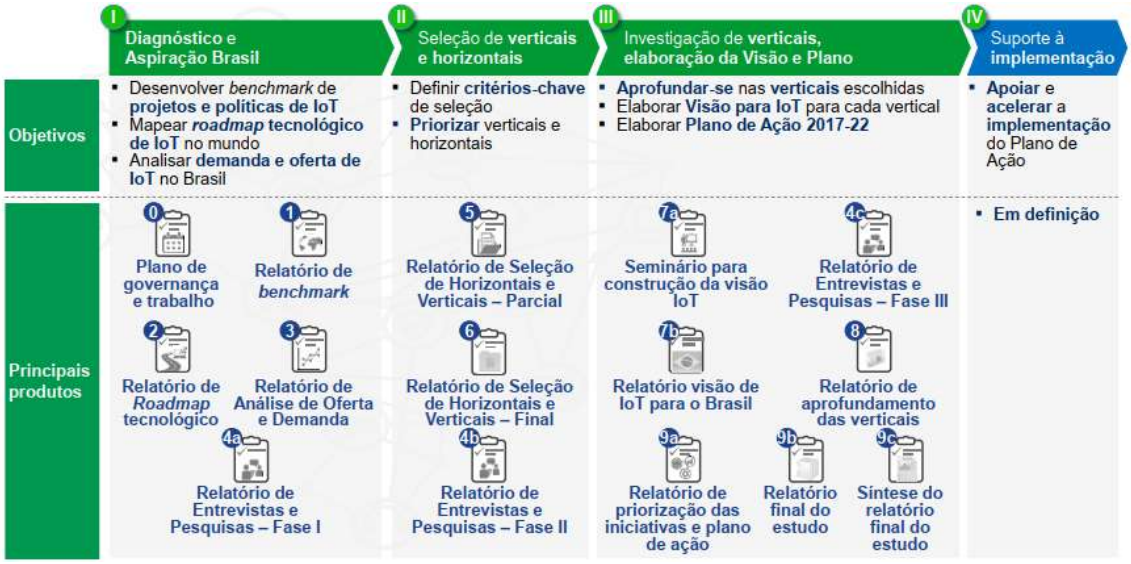
b) Seleção de verticais e horizontais: Definição de critérios-chave para seleção e priorização de verticais e horizontais;

c) Aprofundamento e elaboração de plano de ação (2017 - 2022): Aprofundamento nas verticais escolhidas, elaboração de visão para IoT para cada vertical e elaboração de Plano de Ação 2017-22;

d) Suporte à implementação: Apoio à execução do Plano de Ação 2017-22” (BNDES, 2017a).

A organização do plano foi apresentada no Quadro 1.

Quadro 1 – Principais produtos do estudo do BNDES



Fonte: BNDES, 2017a, v. 1, p. 3.

Esse plano do BNDES destacou algumas outras inciativas de IoT no Brasil nas áreas de Cidades e Saúde:

a) Implantação de sistema de telegestão de iluminação pública na cidade de Belo Horizonte, Minas Gerais, que permitirá controlar a intensidade da iluminação pública segundo a demanda e a transmissão de informações sobre falhas na iluminação, sem necessidade de vistoria ou reclamação. O sistema ainda prevê a integração com outros serviços públicos como semáforos e câmeras e um futuro suporte ao serviço Wi-Fi público na cidade. A conclusão está prevista para 2020 e deverá trazer uma economia de 45% de energia;
b) O projeto de implantação de serviços inteligentes baseados em IoT na cidade de Águas de São Pedro, no estado de São Paulo, financiado por uma operadora de telecomunicações em parceria com multinacionais de equipamentos, *startups* de tecnologia e fundações, instalou sensores para monitoramento da vida útil das lâmpadas na iluminação pública, sensores de presença para comandar essa iluminação, câmeras com sensores para identificação de veículos trafegando na contramão das vias públicas e sistema de controle de vagas de estacionamento; esse projeto permitiu uma redução de 35% no consumo de energia na área piloto implantada e um aumento de 150% na velocidade de conexão à Internet;
c) Projeto 'Hospital 4.0', do Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo, que planeja construir uma plataforma para suporte a aplicações IoT em ambientes como ambulâncias, UTI's, centros cirúrgicos, ambulatórios, serviços de diagnóstico, internações e centrais de materiais esterilizados;
d) O Hospital Israelita Albert Einstein possui sistema informatizado em que os equipamentos eletromédicos inserem automaticamente as informações do paciente no prontuário eletrônico. Esse hospital possui um sistema de localização de bens móveis (macas de transporte, cadeiras de rodas) baseado em etiquetas eletrônicas, que administra desde o trajeto de recém-nascidos no hospital até o controle das portas de entrada e saída (BNDES, 2017f; BNDES, 2017g).

Percebeu-se que essas ações ainda têm foco pontual em projetos piloto para provar as vantagens da tecnologia e sem caráter sistêmico. Não foram destacadas iniciativas no Meio Rural e na Indústria em andamento no plano do BNDES.

Considerando essas primeiras propostas de sistemas baseados em IoT, é possível conjecturar que a inclusão da 'inteligência' no ambiente cotidiano deverá causar grande impacto. Ainda pode-se antecipar a sua influência em vários sistemas tecnológicos que darão apoio a tecnologia IoT e que concorrem pelo uso de recursos limitados como o espectro radioelétrico para

transmissão de sinais, sistemas de telecomunicações compartilhados ou especialistas, redes de transmissão de dados, processamento, armazenamento e arquitetura de informações. Outra questão não menos importante é o volume de dados envolvido, que exigiria arquiteturas de informação compatíveis.

O objetivo geral deste trabalho foi verificar a aderência da conectividade para sistemas IoT proposta no documento 'Internet das Coisas: Um Plano de Ação para o Brasil' aos atributos de Segurança da Informação. A questão que norteou esta pesquisa foi:

> **Como as propostas de conectividade apresentadas no documento 'Internet das Coisas: Um Plano de Ação para o Brasil' se alinham aos cinco atributos de Segurança da Informação: Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade?**

O trabalho se justificou por estudar propostas de implantação de sistemas IoT em ambientes importantes no Brasil: Cidades, Saúde, Meio Rural e Indústria, que têm um impacto econômico e social significativo. Ao avaliar a sua aderência aos atributos de Segurança da Informação, o trabalho acrescentou uma nova visão às propostas de conectividade para esses sistemas.

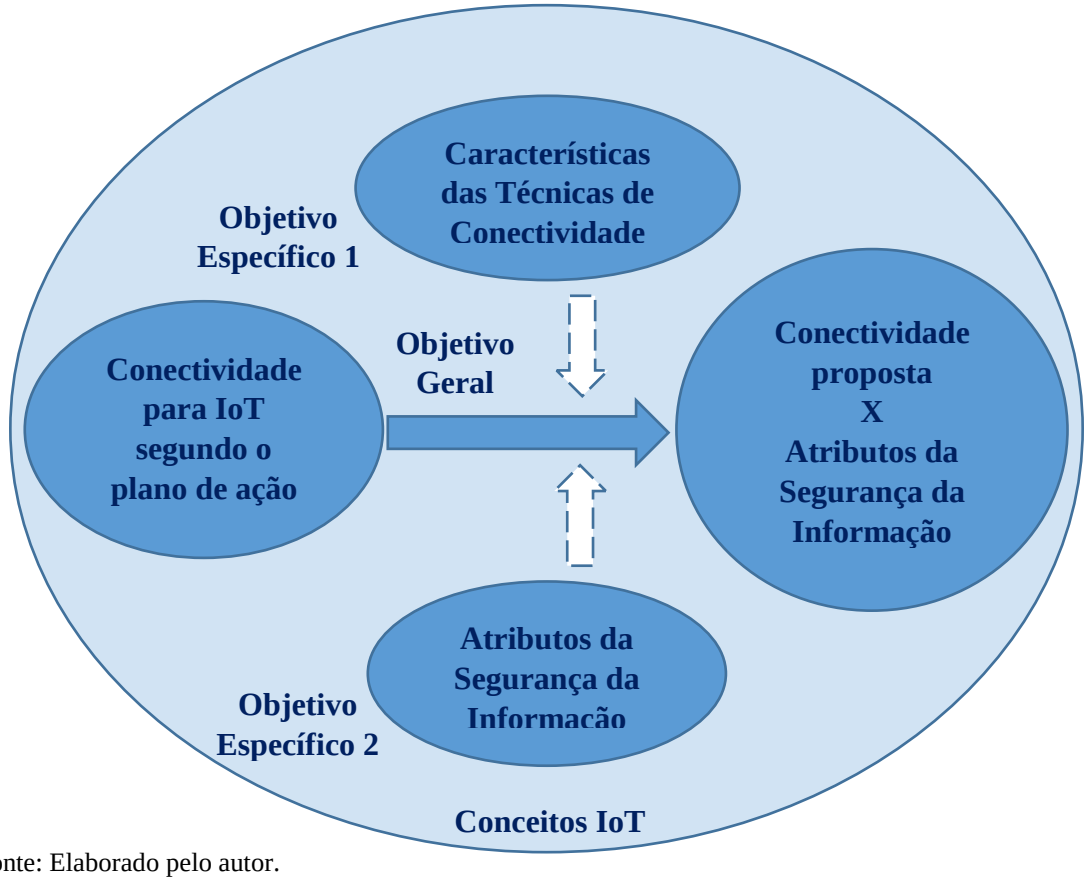
O objetivo geral foi dividido em dois objetivos específicos.

a) Objetivo Específico 1: Identificar as características da conectividade para sistemas IoT que foi proposta no documento 'Internet das Coisas: Um Plano de Ação para o Brasil';
b) Objetivo Específico 2: Relacionar os atributos de Segurança da Informação e as características da conectividade estudadas.

O objetivo específico 1 analisou as características das tecnologias para conectividade propostas para atender a Cidades, Saúde, Meio Rural e Indústrias, chamadas de verticais no documento 'Internet das Coisas: Um Plano de Ação para o Brasil'. Esse objetivo permitiu o mapeamento das principais tecnologias de telecomunicações previstas para cada atendimento levantado no plano de ação. Já o objetivo específico 2 teve foco na análise dos cinco atributos de Segurança da Informação e como esses atributos se relacionariam com as tecnologias de conectividade estudadas. Todo esse estudo ficou contido dentro da conceptualização de Sistemas IoT. Nesse ponto, foi possível atender ao objetivo geral da dissertação que se relaciona os quatro constructos a serem desenvolvidos na fundamentação teórica: conceitos de IoT, conectividade proposta pelo plano de ação, características técnicas da conectividade e atributos da segurança

da informação (Diagrama 1). Desse modo, pôde-se alinhar os atributos de Segurança da Informação com as tecnologias de conectividade propostas no plano de ação. O resultado permitiu também mapear o alinhamento de cada atributo com as tecnologias de conectividade propostas.

Diagrama 1 – Inter-relacionamento dos objetivos específicos



Fonte: Elaborado pelo autor.

Ao analisar o tema dessa dissertação frente aos objetivos do Programa de Pós-Graduação em Sistemas de Informação e Gestão do Conhecimento – PPGSIGC, constatou-se a sua aderência na medida que inter-relaciona uma tecnologia de aquisição e tratamento de dados (Internet das Coisas) e atributos de Segurança da Informação, ambos relacionados a Sistemas de Informação, com a conectividade necessária ao seu funcionamento. Essa natureza interdisciplinar é característica marcante do programa. Dentre os objetivos específicos do programa, podem-se destacar: (i) o alinhamento com a pesquisa relacionada a novas tecnologias e o seu impacto na teoria de Sistemas de Informação, (ii) a capacitação para análise de problemas complexos e (iii)

a capacitação para a utilização de tecnologias de gestão e de informação que promovam modernização (FUMEC, 2017, p. 4).

Especificamente, o trabalho se inseriu no programa segundo a classificação abaixo:

a) Linha de pesquisa: Tecnologia e Sistemas de Informação;
b) Trilha de pesquisa: T3 – Informação e Tecnologia.

Na descrição dessa linha de pesquisa, destaca-se:

> A trilha de pesquisa Informação e Tecnologia emprega aportes teóricos dos campos da Ciência da Informação, Computação, Engenharia Elétrica, Engenharia de Software e Engenharia Semiótica para construção de investigações interdisciplinares de caráter aplicado. As pesquisas da linha têm como campo empírico a área de tecnologia da informação e suas aplicações, a exemplo dos sistemas inteligentes que lidam com banco de dados e inteligência analítica, web semântica e ontologias, processos de software, sistemas digitais embarcados, redes de computadores, Internet das Coisas (IoT - Internet of Things), interface homem computador, aprendizado automático, modelos estatísticos computacionais, design de interfaces de metacomunicação, processamento digital de imagens (FUMEC, 2019).

Após essa introdução, apresenta-se a metodologia utilizada na pesquisa. Na sequência, seguem a fundamentação teórica, discussões sobre a fundamentação, trabalhos relacionados ao tema e considerações finais da dissertação.

2 METODOLOGIA

Para elaboração da dissertação realizaram-se pesquisas em bibliotecas e bases de dados digitais *on-line* visando uma revisão ampla, não exaustiva, da literatura sobre os constructos em questão.

Segundo Gonçalves e Meirelles (2004, p. 30), essa pesquisa poderia, pelas questões de engenharia e informática, ser colocada dentro das ciências formais, na lógica e matemática. Por outro lado, ao abordar um plano de ação governamental que abrange Cidades, Saúde, Meio Rural e Indústrias e, portanto, de grande impacto no cotidiano, a pesquisa poderia ser classificada entre as ciências reais ou factuais, nas humanas, notadamente administração.

Considerando a classificação de Gonçalves e Meirelles (2004) quanto aos métodos de investigação, a pesquisa foi conduzida no sentido mais indutivo partindo do particular para geral e, no caso, através do estudo dos conceitos de IoT até sua aplicação nas propostas de conectividade para as quatro verticais: Cidades, Saúde, Meio Rural e Indústrias, além de considerar os atributos de Segurança da Informação (p. 31). Com relação aos métodos de investigação, pode-se dizer que a proposta foi de um estudo bibliográfico documental sobre as tecnologias de telecomunicações e os atributos de Segurança da Informação dentro do ambiente de Internet das Coisas (p. 34). A pesquisa teve um enfoque exploratório baseado em estudos documentais, procurando identificar melhor a inter-relação entre a conectividade proposta no documento ‘Internet das Coisas: Um Plano de Ação para o Brasil’ e os atributos de Segurança da Informação (p. 37 e 64). A pesquisa teve uma abordagem qualitativa já que busca destacar a conexão entre as áreas pesquisadas sem se fixar nos aspectos de medida dessas conexões (p. 62).

Abordando a questão da pesquisa como um processo, Mingers (2001) identifica quatro fases que compõem esse processo: (a) apreciação da situação da pesquisa (identificação e conceituação inicial do fenômeno), (b) análise dos dados produzidos (envolve métodos de análise e formulação de explicações sobre o que pode ter produzido os fenômenos observados), (c) avaliação das explicações propostas (envolve interpretação dos resultados e inferências) e (d) ação para reportar e disseminar os resultados da pesquisa. Nesse contexto, pode-se argumentar que, após a definição da temática da pesquisa e a reunião de arquivos e documentos (a), foi realizado o trabalho de estudo, mapeamento das soluções de conectividade e confronto com os atributos de Segurança da Informação (b e c) para em seguida discutir e apresentar as considerações finais (d).

A pesquisa para elaboração da fundamentação teórica desta dissertação se baseou na Revisão da Literatura, utilizando conceitos da Análise de Conteúdo para Pesquisas Qualitativas. Nesse contexto, apresentam-se algumas ideias de autores da área:

a) Flick (2013): discorrendo sobre o embasamento teórico e metodologia de revisão divide a literatura em teórica, metodológica e empírica. O primeiro tipo aborda conceitos e definições sobre o campo em investigação. A literatura metodológica discorre sobre métodos e alternativas de pesquisa. A literatura empírica se relaciona a pesquisas anteriores e similares ao campo de estudo. Flick esclarece que todas as três devem ser consideradas na elaboração de uma metodologia de revisão da literatura;
b) Creswell (2007): como qualquer técnica de análise de dados, a Análise de Conteúdo é uma metodologia de interpretação possuindo procedimentos específicos para preparação dos dados e procurando "extrair sentidos dos dados e imagem" (p. 194);
c) Chizzotti (2006): "o objetivo da análise de conteúdo é compreender criticamente o sentido das comunicações, seu conteúdo manifesto ou latente, as significações explícitas ou ocultas" (p. 98); a escolha do procedimento mais adequado de análise de dados depende do material a ser analisado, dos objetivos da pesquisa e da posição ideológica e social do analisador;
d) Shah e Corley (2006): os métodos qualitativos e quantitativos são complementares e os estudos organizacionais podem ser favorecidos com o uso concomitante dos dois métodos.

Bardin (2002, p.38) define a Análise de Conteúdo: "conjunto de técnicas de análise das comunicações, que utiliza procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens. ... A intenção da análise de conteúdo é a inferência de conhecimentos relativos às condições de produção ...". Pôde-se perceber que a Análise de Conteúdo objetiva ultrapassar as incertezas e enriquecer a leitura dos dados coletados. Nesse contexto, o material textual escrito é o mais tradicionalmente utilizado incluindo notas de campo, diários de pesquisa, fichas de documentação e transcrições, mas também se estendendo a material documentado em fotos, filmes, áudios e outras formas relevantes no processo de pesquisa (BAUER & GASKELL, 2002; FLICK, 201).

Mozzato e Grzybovski (2011) destacaram que o processo da Análise de Conteúdo, como todo processo de análise de dados, envolve várias etapas e recebe organização diferente de diversos autores. Bardin (2002) divide o processo em três fases:

a) Pré-análise: trata da organização do material e pode ser subdividida em quatro etapas: (i) leitura flutuante, primeiro contato com o material, (ii) seleção dos documentos a serem analisados, (iii) formulação de hipóteses e dos objetivos, e (iv) estabelecimento de índices e elaboração de indicadores para os textos em análise;
b) Exploração do material: definição de categorias (codificação) e identificação das unidades de registro (atribuem significado à codificação permitindo sua classificação, categorização e contagem) e das unidades de contexto nos documentos (permitem a compreensão do código utilizado);
c) Tratamento dos resultados, inferências e interpretação: condensação e destaque das informações que permitem as interpretações; nessa fase realiza-se a análise intuitiva, reflexiva e crítica dos dados pelo pesquisador.

Considerando a fase de pré-análise definida por Bardin (2002), o método inicial de pesquisa planejado foi buscar arquivos nas bases de dados eletrônicas Ebsco, *Web of Science*, Google Acadêmico e ScienceDirect. A busca foi feita pela inserção de palavras chave em português e inglês nas *search engines* dessas bases. Os termos pesquisados foram detalhados nos apêndices 1, 2 e 3.

Sobre a codificação, Bardin (2002, p.103) a define como o recorte, a agregação e a enumeração dos dados brutos do texto segundo regras precisas e que permite representar seu conteúdo ou sua expressão: “A codificação corresponde a uma transformação - efectuada segundo regras precisas - dos dados brutos do texto, transformação esta que, por recorte, agregação e enumeração, permite atingir uma representação do conteúdo, ou da sua expressão, susceptível de esclarecer o analista acerca das características do texto ...”. Nesse contexto, o levantamento das características técnicas da conectividade proposta para sistemas IoT e dos atributos de Segurança da Informação estariam inseridos nessa fase.

Já sobre a categorização, Bardin (2002) a interpreta como a classificação e diferenciação dos elementos constitutivos de um conjunto seguida pelo reagrupamento dos elementos desse conjunto por analogia segundo critérios pré-definidos. O mapeamento das principais tecnologias de telecomunicações previstas para a conectividade de sistemas IoT e sua aderência aos atributos de Segurança da Informação foram elaborados nessa fase.

A elaboração desta dissertação evoluiu a partir da ideia inicial de estudar os aspectos de hardware e software de arquiteturas de informação que utilizam Internet das Coisas e que seriam

mais adequados para gestão de informações de saúde humana. Após a primeira pesquisa, realizada nas bases Google Acadêmico, Ebsco, Periódico CAPES e ScienceDirect, registrada no apêndice 1, o trabalho sofreu uma interrupção por constatar-se que o foco inicial era muito amplo. Após discussões, o trabalho tomou o foco em conceitos de IoT, arquitetura de informação e contexto nacional na área de saúde realizando-se as pesquisas apresentadas no apêndice 2.

Ao se estudar o contexto nacional, o documento 'Internet das Coisas: Um plano de ação para o Brasil' chamou atenção pela organização e amplitude. A questão de estudar a conectividade veio à tona, a princípio somente para a área da saúde e, posteriormente, assumindo a versão atual de estudo da conectividade relacionada às quatro verticais: Cidades, Saúde, Meio Rural e Indústrias.

Nesse ponto, procedeu-se a leitura do documento do BNDES com foco nas propostas de conectividade para as verticais. Essa leitura conduziu a um conjunto de termos sobre conectividade que deveriam ser pesquisados. Também foram pesquisados termos sobre os atributos de Segurança da Informação. As bases consultadas nessa etapa foram Ebsco, *Web of Science* e Google Acadêmico e foram detalhadas no apêndice 3. Também foram feitas pesquisas em bibliotecas virtuais dentro do Sinef – Sistema de Informações dos Negócios da Fumec, em livros na biblioteca central da Universidade e outros de posse do autor. Os artigos baixados na pesquisa passaram por uma pré-análise que se iniciou pela leitura do título, resumo e conclusões buscando verificar sua pertinência ao foco considerado à época. Procurou-se por descrições sistêmicas dos sistemas de comunicação propostos nas aplicações IoT do documento do BNDES. Os artigos pesquisados e trechos de livros selecionados passaram por uma leitura flutuante considerando a pertinência ao tópico considerado, objetividade, qualidade e relevância que, no caso dos artigos, seria expressa pelo número de citações. Os artigos e livros passaram pela exploração do material através leitura mais atenta dentro do software Zotero, quando possível, para construção da fundamentação teórica. Nessa fase, as citações mais relevantes levaram a busca específica da fonte primária para leitura do artigo ou livro original. Outros termos de interesse que surgiram nas diversas leituras também foram pesquisados diretamente em ferramentas de busca na Internet.

Com base no material pesquisado, elaborou-se na Fundamentação Teórica uma contextualização e descrição teórica sobre IoT e uma análise do documento 'Internet das Coisas: Um Plano de Ação para o Brasil'. Nessa etapa, percebeu-se a relevância da Segurança

dos Dispositivos IoT para fazer o relacionamento entre a Conectividade e a Segurança da Informação, o que conduziu à inclusão do assunto nas discussões. Seguiu-se a apresentação das tecnologias de Conectividade e Segurança de Dispositivos proposta no plano, uma descrição de cada uma das soluções de IoT propostas nas verticais, considerando as necessidades para atendê-las e a capacidades do mercado nacional para provimento dessas soluções, e uma explanação sobre os atributos de Segurança da Informação.

O capítulo de Discussões a seguir apresentou uma descrição sistêmicas das tecnologias de Conectividade, com foco nas questões relacionadas ao ambiente de IoT, objetivo específico 1 da dissertação, e uma breve explanação das tecnologias de Segurança de Dispositivos. Essas considerações subsidiaram a elaboração do relacionamento entre Conectividade, Segurança da Informação e Segurança de Dispositivos, objetivo específico 2 da dissertação. Especificamente, foram relacionados:

a) Cada tecnologia de Conectividade proposta e os atributos de Segurança da Informação;
b) Cada tecnologia de Segurança de Dispositivo proposta e os atributos de Segurança da Informação;
c) As tecnologias de Conectividade e de Segurança de Dispositivo.

Esses relacionamentos permitiram alcançar o objetivo geral do estudo que foi verificar o alinhamento entre as propostas de Conectividade no plano do BNDES e os cinco atributos da Segurança da Informação.

Pesquisaram-se ainda trabalhos relacionados, tanto no âmbito de ações de governo quanto em artigos que destacam a conectividade para IoT no país e fora dele.

Por fim, as considerações finais destacaram os achados da pesquisa, sua relevância e contribuições além de indicar novos caminhos de pesquisa relacionados a IoT.

3 FUNDAMENTAÇÃO TEÓRICA

Dissertou-se a seguir sobre a conceituação relacionada a Internet das Coisas – IoT. Posteriormente, o documento ‘Internet das Coisas: Um Plano de Ação para o Brasil’ foi apresentado e analisado considerando as tecnologias de conectividade propostas. Essas tecnologias foram então detalhadas de modo a destacar suas características principais. Em seguida, os atributos da Segurança da Informação foram examinados e cada tecnologia de conectividade foi confrontada com esses atributos.

3.1 Contextualizando a Internet das Coisas – IoT

Kevin Ashton cunhou o termo Internet das Coisas em 1999 referindo-se ao uso de etiquetas RFID na cadeia de suprimentos de produtos da P&G. Um aspecto importante associado ao conceito de IoT ainda pouco destacado é a característica de independência da interferência humana, com todas as suas limitações de tempo, atenção e precisão, na aquisição dos dados:

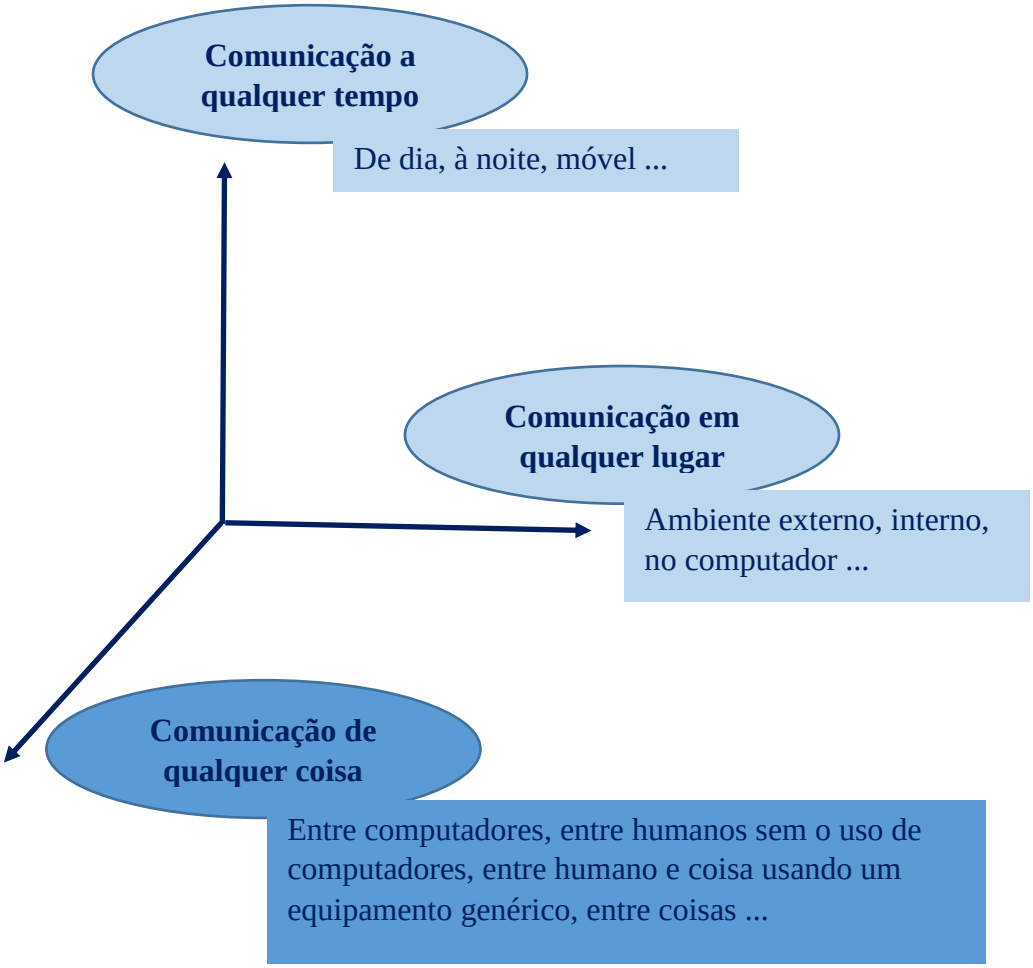
> Se tivéssemos computadores que soubessem tudo o que havia para saber sobre as coisas - usando dados que eles reunissem sem qualquer ajuda nossa - poderíamos acompanhar e contar tudo, e reduzir muito o desperdício, perda e custo. Nós saberíamos quando as coisas precisariam ser substituídas, reparadas ou retiradas de serviço, e se elas estavam atualizadas ou superadas (ASHTON, 2009, p. 1).

Para o grupo RFID, a Internet das Coisas é "a rede mundial de objetos interligados de endereço exclusivo, com base em protocolos de comunicação padrão" (ATZORI *et al*., 2010, p. 2; BASSI & HORN, 2008, p. 4). Os mesmos Atzori *et al.* colocaram a IoT como uma evolução da computação ubíqua por meio da presença pervasiva de ‘objetos e coisas inteligentes’ no cotidiano que estão prontos a interagir e cooperar para propósitos específicos (ATZORI *et al.*, 2010).

A ITU – *International Telecommunications Union*, órgão da Organização das Nações Unidas – ONU, no seu Setor de Normatização das Telecomunicações – ITU-T, apresentou a seguinte definição para IoT: “Do ponto de vista da padronização técnica, a IoT pode ser vista como uma infraestrutura global para a sociedade da informação, possibilitando serviços avançados através da interconexão (física e virtual) de coisas baseadas em tecnologias de informação e comunicação (TIC) interoperáveis existentes e em evolução”. Destaca-se que, mais do que uma tecnologia disruptiva, IoT é a integração de tecnologias de comunicação já existentes visando acessar todos os dispositivos pertencentes a rede (BNDES, 2017a).

Segundo o ITU-T (2012), o conceito de IoT acrescentou uma terceira dimensão às tecnologias de informação e comunicação (TIC): além da comunicação “a qualquer tempo” e “em qualquer lugar” que regeram a evolução da TIC, surgiu a dimensão “de qualquer coisa” significando comunicação vinda de qualquer fonte de informação, o que foi apresentado no Diagrama 2.

Diagrama 2 – Nova dimensão introduzida pela IoT



Fonte: Adaptado de ITU-T, 2012, p. 3.

O conceito de ‘coisa’ tem evoluído a cada novo sistema, conduzindo a uma evolução do conceito de Internet de uma rede de computadores para uma rede de objetos interconectados e atuantes no mundo físico (ITU-T, 2012, p. 1). O Cluster de Projetos de Pesquisa Europeus sobre Internet das Coisas define: "coisas são participantes ativos em negócios, informações e processos sociais, onde eles são capazes de interagir e se comunicar entre si e com o meio

ambiente, trocando dados e informações obtidas do meio ambiente, enquanto reagem de forma autônoma aos eventos físicos do mundo real e influenciando-os na execução de processos que desencadeiam ações e criam serviços com ou sem intervenção humana direta" (GUBBI *et al.*, 2013, p. 3; SUNDMAEKER *et al.*, 2010, p. 43). Destacou-se novamente a questão da obtenção de dados sem intervenção humana.

Algumas tecnologias já consolidadas (*Bluetooth*, RFID, Wi-Fi e GSM) permitiram que 9 bilhões de dispositivos estejam conectados à *web* em 2013, representando uma receita de US$ 1.3 trilhões para operadoras de redes móveis nesse ano. Projeções para 2020 consideram 24 bilhões de dispositivos. (GUBBI *et al.*, 2013, p. 2).

As previsões de impacto econômico para a tecnologia IoT são de 3,9 a 11,1 trilhões de dólares em 2025, que correspondem de 4% a 11% do produto interno bruto global e de 50 a 200 bilhões de dólares no mesmo ano no Brasil (BNDES, 2017j; BNDES, 2018; MANYIKA *et al.*, 2015a).

Na área social, a ITU – *International Telecommunications Union*, salienta que a IoT pode auxiliar o mundo a alcançar os Objetivos de Desenvolvimento Sustentável, definidos na *IoT Week Geneva* de 6 a 9 de junho de 2017, em dez atividades das quais pôde-se destacar: "Promover o desenvolvimento e a adoção de Tecnologias IoT em benefício da humanidade, do meio ambiente e do desenvolvimento sustentável" e "Promover o desenvolvimento e a adoção de Tecnologias IoT em benefício da humanidade, do meio ambiente e do desenvolvimento sustentável" (BNDES, 2017j)

Devido as cifras envolvidas, o assunto tem atraído grande interesse mundial e existem algumas propostas de aplicações e suas arquiteturas. Nesse contexto, surgiram conceituações diferentes com sua terminologia própria, cada uma pretendendo deixar sua marca particular na área:

> O conceito de IoT também pode ser visto com uma derivação dos conceitos de computação ubíqua (WIESER, 1991), computação pervasiva (SATYANARAYANAN, 2001), "*things that think*" (GERSHENFELD, 1999), "*ambiente intelligence*" (FERGUNSON, 2002) e "*silente commerce*" (AARTS, HARWIGE, SCHUURMANS, 2002). Todos esses conceitos têm em comum a visão de que haverá um mundo com objetos físicos do cotidiano equipados com uma lógica digital, sensores e uma capacidade de conexão à Internet (FLEISH, SARMA, THIESSE, 2009) (PACHECO *et al*., 2016, p. 3).

Dentre algumas conceituações, destacou-se o trabalho de Fleisch (2010) que procura diferenciar IoT de um conceito mais recente, *web-of-things*. Alguns autores acreditaram que o conceito inicial de IoT poderia ser considerado somente como uma outra aplicação de Internet, similar à web *services*. Em uma *web-of-things*, os objetos se comunicariam com outros elementos da

rede utilizando componentes de baixo nível para endereçamento e conexão. Nesse contexto, a IoT poderia ser "corretamente conceituada como uma extensão da Internet, na qual há endereçamento de objetos do cotidiano e possibilidade de fazê-los agir como se fossem pequenos computadores" (PACHECO *et al*., 2016).

Gubbi *et al.* (2013) apresentaram uma classificação das 'coisas' em quatro áreas de aplicação conforme quadro 2.

Quadro 2 – Classificação de usuários finais e áreas de aplicação para IoT

CASA	**TRANSPORTE**	**COMUNIDADE**	**NACIONAL**
Saúde	Logística	Fábricas	Serviços públicos
Entretenimento	Tráfego	Varejo	Infraestrutura
Segurança	Estacionamento	Meio ambiente	*Smart Grid*
Eletrodomésticos	Serviços de emergência	Inteligência de negócios	Monitoramento remoto
	Estradas	Vigilância	Defesa
		Medição inteligente	

Fonte: Adaptado de Gubbi *et al*., 2013, p. 3.

Existe uma relação direta em Internet das Coisas e *Big Data*. Lohr (2012, p. 2) avaliou que *Big Data* é mais do que "mais dados". Seriam dados inteiramente novos. Considerando a grande quantidade de sensores já existente, não só o volume maior, mas a qualidade e confiabilidade desses dados entrariam no contexto de *Big Data*. Nesse sentido, a implantação de sistemas baseados em IoT alimentaria essa tendência.

Manyika *et al*. (2011, p. 11) estabeleceram que *Big Data* refere-se a conjuntos de dados cujo tamanho está além da capacidade para capturar, armazenar, gerenciar e analisar, presente em ferramentas típicas de software de banco de dados. Esta definição é intencionalmente subjetiva e móvel no sentido do tamanho que um conjunto de dados precisa ter para ser considerado grande, ou seja, não se define *Big Data* em termos de serem maiores do que um certo número de terabytes (10^{12} bytes).

Outra questão relevante para o *Big Data* é que, diferentemente dos dados anteriormente depositados por atividade humana, os dados colhidos por sensores seriam mais estruturados, o

que demonstra outra vantagem de sistemas IoT. Segundo Lohr (2012), esses dados estruturados tratados por ferramentas computacionais de inteligência artificial adequadas (processamento de linguagem natural, reconhecimento de padrões, *machine learning*) representariam grande valor para empresas que conseguirem transformá-los em conhecimento aplicado aos seus negócios. Destacou ainda que o poder preditivo do *Big Data* está sendo explorado - e mostra promessa - em diversos campos. Citou o achado de pesquisadores que encontraram um pico nos pedidos de pesquisa em ferramentas de busca na Internet para termos como "sintomas de gripe" e "tratamentos de gripe" algumas semanas antes de acontecer um aumento nos pacientes com gripe que chegaram à emergência de hospitais. Isso indicou a confiança que os internautas depositam nas ferramentas de busca e que isso poderia ser utilizado como dado para preparar a reação dos sistemas públicos de saúde.

No contexto de volume de dados, segundo McAfee & Brynjolfsson (2012), 2,5 exabytes (10^{18} bytes) de dados foram criados por dia em 2012 e esse número dobrava a cada 40 meses. Empresas como o Walmart coletavam mais de 2,5 petabytes (10^{15} bytes) de dados de transações de seus consumidores a cada hora. Dados mais atualizados indicaram que no início de 2017, 8 exabytes de dados foram criados somente por dispositivos móveis (SCHULTZ, 2019).

Manyika *et al*. (2011) e Schultz (2019) destacaram mais algumas informações na crescente torrente de *Big Data*:

a) 30 bilhões de *posts* foram compartilhadas no Facebook por mês em 2011; esse número subiu para 3 milhões de posts por minuto em 2016;
b) Dados globais teriam um crescimento projetado de 40% por ano contra 5% de crescimento global em gastos de TI; espera-se um total de 175 zettabytes (10^{21} bytes) de dados globais em 2025;
c) A Biblioteca do Congressos dos EUA tinha 235 terabytes de dados coletados até abril de 2011; informação sobre o processo de digitalização de documentos ocorrido nessa biblioteca estimam que em 2019 a quantidade de dados armazenados seria de 7 petabytes (10^{15} bytes).

Em termos de valores, Galov (2019, p.1) apresentou algumas estimativas sobre o *Big Data*:

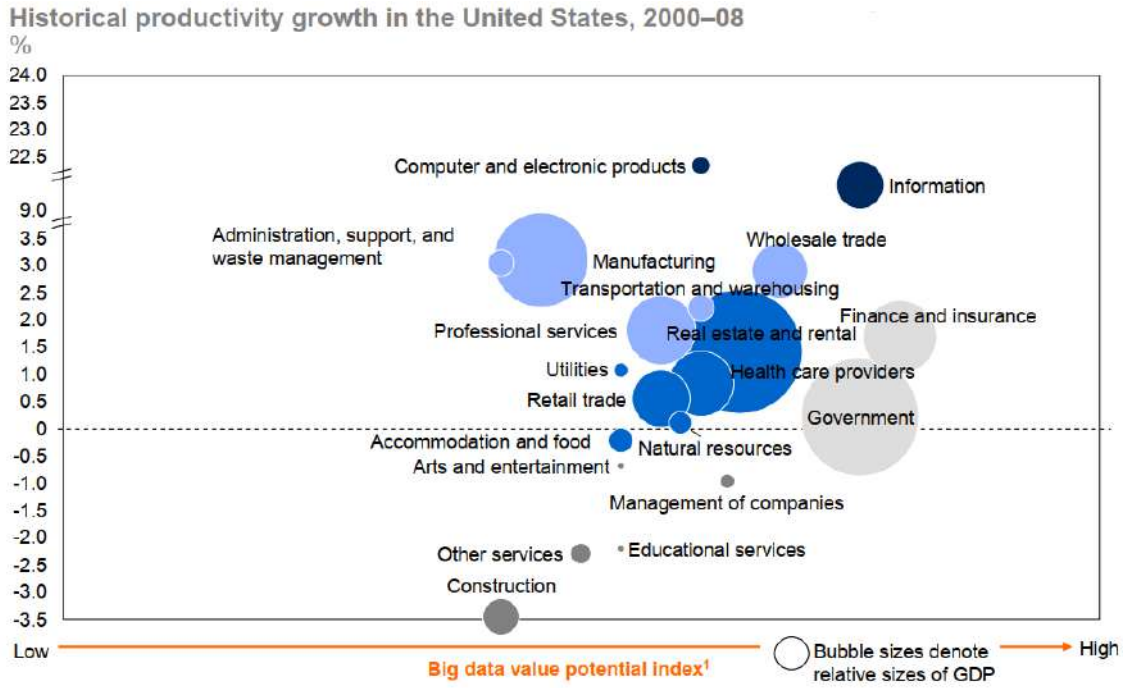
a) As estatísticas mostram que a receita gerada a partir de *Big Data* estaria aumentando. Em 2015, foi responsável por US$ 122 bilhões em lucros. A expectativa é de gerar US$ 189,1 bilhões em 2019 e US$ 274,3 bilhões em 2022;

b) Os EUA são de longe o maior mercado. A receita de 2019 deve chegar a US$ 100 bilhões. Para colocar isso em perspectiva, os outros quatro países entre os cinco maiores gerariam US $ 35 bilhões;
c) O Reino Unido é o terceiro maior mercado de *Big Data*, depois dos EUA e do Japão. Gerará US$ 9,2 bilhões em 2019. No entanto, as previsões para 2020 indicariam que *Big Data* e a IoT valerão quase US $ 420 bilhões para a economia do Reino Unido.

São esses últimos dados relacionados a receitas, retorno financeiro, mercado de trabalho e lucro que reforçam a importância do *Big Data* e dos sistemas IoT para a economia mundial.

O diagrama 3 destacou o valor dado ao *Big Data* em diversas áreas nos EUA. Nesse diagrama, o tamanho das bolhas está relacionado ao Produto Interno Bruto previsto para cada área.

Diagrama 3 – Histórico de crescimento de produtividade com *Big Data* nos EUA



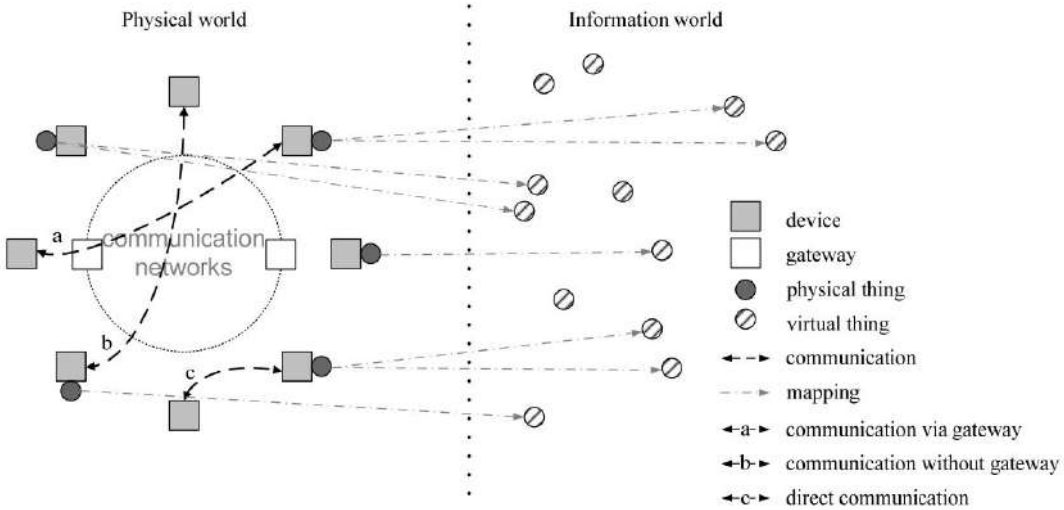
Fonte: Adaptado de Manyika *et al.*, 2011, p. 9.

3.2 Aspectos Técnicos de IoT

O objetivo por trás do conceito de IoT é representar os objetos (‘coisas’) do mundo físico no ambiente virtual através do mapeamento desses objetos, conforme apresentado no diagrama 4.

Nesse diagrama, os dispositivos seriam equipamentos que obrigatoriamente têm capacidade de comunicação e que capturam as informações dos objetos físicos. Além da comunicação, os dispositivos podem ter capacidades de detecção, atuação, captura, armazenamento e processamento de dados. Os dispositivos seriam capazes de se comunicar entre si diretamente ou via uma rede de comunicação. Também pode ser necessário um *gateway* para fazer a interface com a rede. Um objeto do mundo físico poderia ser mapeado em mais de um no mundo virtual. As interações que ocorrem entre objetos não ficam limitadas ao mundo físico podendo ocorrer interações entre objetos virtuais diretamente e entre objetos virtuais e físicos (ITU-T, 2012, p. 3).

Diagrama 4 – Mapeamento de objetos físicos para o ambiente virtual



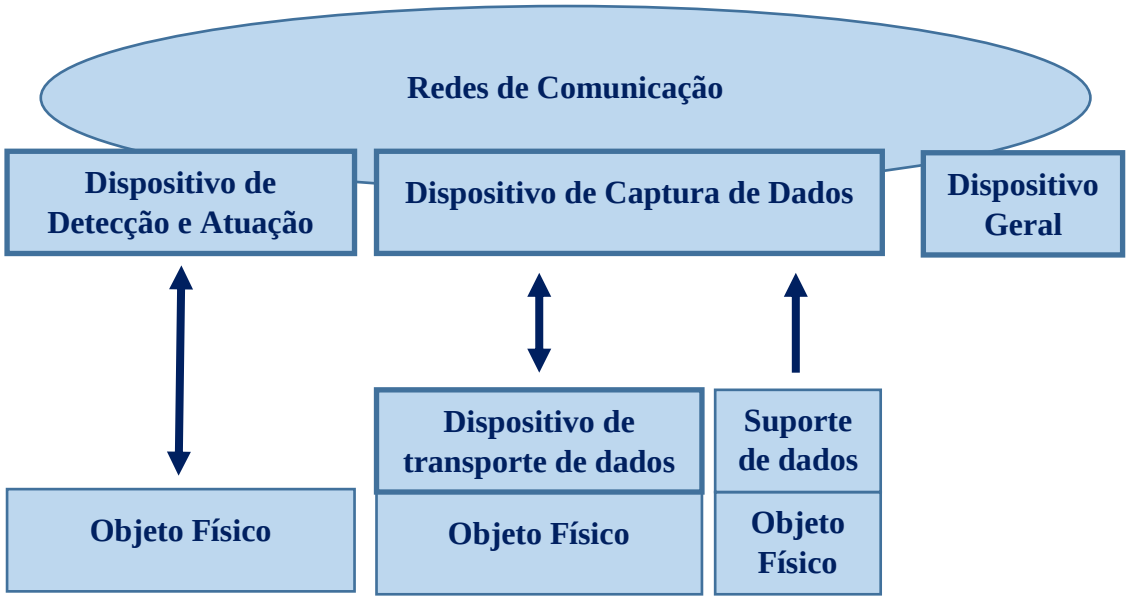
Fonte: ITU-T, 2012, p. 3.

Essa rede de comunicação poderia dar suporte a diversos tipos de aplicações nas áreas de logística, *smart grid* (rede elétrica inteligente), *smart home* (casa inteligente), *e-health* por exemplo, e que poderiam ainda ser baseadas em plataformas proprietárias ou abertas que garantam os serviços básicos de rede, como autenticação e gerenciamento do dispositivo. A rede de comunicação deve prover a transferência eficiente e confiável dos dados adquiridos pelos dispositivos assim como das instruções das aplicações para eles usando redes existentes TCP/IP ou NGN (*Next Generation Networks*) (ITU-T, 2012).

Segundo o ITU-T (2012), os dispositivos podem ser classificados de acordo com o diagrama 5, a saber:

a) Dispositivo de detecção e atuação: pode detectar ou medir informações relacionadas ao meio ambiente e convertê-las em sinais digitais ou converter sinais digitais das redes de informação em operações. Geralmente, os dispositivos de detecção e atuação das redes locais se comunicam entre si usando tecnologias de comunicação com ou sem fio e *gateways* para conectar-se às redes de comunicação;
b) Dispositivo de captura de dados: refere-se a um dispositivo de leitor / gravador com capacidade de interagir com objetos físicos. A interação pode acontecer indiretamente através de dispositivos de transporte de dados ou diretamente através de suportes de dados conectados às coisas físicas. No primeiro caso, o dispositivo de captura de dados lê informações em um dispositivo de transporte de dados e, opcionalmente, também pode gravar informações fornecidas pelas redes de comunicação no dispositivo de transporte de dados;
c) Dispositivo geral: dispositivo que possui recursos incorporados de processamento e comunicação e pode se comunicar com as redes de comunicação por meio de tecnologias com ou sem fio. Os dispositivos gerais incluem equipamentos e dispositivos para diferentes domínios de aplicação da IoT, como máquinas industriais, eletrodomésticos e *smart phones* (ITU-T, 2012).

Diagrama 5 – Tipos de dispositivos e seu relacionamento com objetos físicos



Fonte: Adaptado de ITU-T, 2012, p. 4.

O ITU-T (2012) enumerou as seguintes características fundamentais da IoT:

a) Interconectividade: qualquer coisa pode ser interconectada com a infraestrutura global de informação e comunicação;
b) Serviços relacionados a coisas: os serviços relacionados às coisas devem obedecer às restrições das coisas, como proteção de privacidade e consistência semântica entre coisas físicas e suas coisas virtuais associadas; as tecnologias no mundo físico e no mundo da informação deverão se adaptar a essas restrições;
c) Heterogeneidade: os dispositivos na IoT são heterogêneos, com base em diferentes plataformas e *hardware* de rede e podem interagir com outros dispositivos ou plataformas de serviço através de redes diferentes;
d) Alterações dinâmicas: várias características dos dispositivos mudam dinamicamente, como por exemplo, ‘dormindo’ e ‘acordando’ ou conectado e desconectado (para poupar energia do dispositivo), bem como informações de contexto como localização e velocidade. Como consequência, o número de dispositivos pode mudar dinamicamente;
e) Escala enorme: o ITU-T estima que o número de dispositivos que precisam ser gerenciados e se comunicam será pelo menos uma ordem de magnitude maior que os dispositivos conectados à Internet atual. Estimativa do Help Net Security indica que esse número foi de 22 bilhões de dispositivos em 2018 (HELP NET SECURITY, 2019). O ITU-T vislumbra uma maior quantidade de comunicações acionadas por dispositivos em relação a comunicações acionadas por humanos. O gerenciamento dos dados gerados e sua interpretação para fins de aplicação será ainda mais crítico devido à semântica dos dados e seu manuseio eficiente.

O ITU-T (2012) listou os requisitos de alto nível para a IoT que considera mais relevantes. Quanto a conectividade, a IoT precisa garantir que a conectividade entre uma coisa e a IoT seja estabelecida com base no identificador da coisa, o que é chamado de conectividade baseada em identificação. Para isso, é necessário que os identificadores heterogêneos das diferentes coisas sejam processados de maneira unificada. Outro requisito, a interoperabilidade, deve ser garantida entre diversos sistemas distribuídos para que seja possível o fornecimento e consumo de informações e serviços variados. Outra questão levantada é que a rede IoT deve ser autônoma o que inclui técnicas e mecanismos de autogerenciamento, autoconfiguração, autocura, auto otimização e autoproteção. As funções de controle de rede IoT precisam suportar essas características para se adaptar a diferentes domínios de aplicação, diferentes ambientes de comunicação e ao grande número e variedade de dispositivos. Os serviços oferecidos nas redes

IoT também precisam ser capazes de capturar, comunicar e processar automaticamente os dados das coisas com base nas regras configuradas pelos operadores ou personalizadas pelos assinantes. Esse requisito é chamado de provisionamento de serviços autônomo e pode depender das técnicas de fusão e mineração de dados automáticas utilizadas.

Continuando a lista de requisitos de alto nível, o ITU-T (2012, p. 6) destaca que a IoT deve suportar a capacidade de localização dos dispositivos. As comunicações e serviços relacionados aos dispositivos poderão depender das informações de localização de itens e usuários que devem ser detectadas e rastreadas automaticamente. Destacam ainda que essas comunicações e os serviços baseados em localização podem estar limitados por leis e regulamentos de privacidade e devem cumprir os requisitos de segurança. A questão da segurança em IoT, onde tudo estará conectado, representa uma ameaças significativa à confidencialidade, autenticidade e integridade dos dados e serviços. A criticidade dos requisitos de segurança se destaca na necessidade de integrar diferentes políticas e técnicas de segurança relacionadas à variedade de dispositivos e redes de usuários na IoT. A questão da privacidade também precisa ser suportada na IoT já que os dispositivos mapeados em coisas têm seus proprietários e usuários e podem conter informações particulares. A IoT precisa oferecer suporte à proteção de privacidade durante a transmissão, agregação, armazenamento, mineração e processamento de dados. Entretanto, a proteção à privacidade não deve definir uma barreira para a autenticação da fonte de dados.

Outro requisito importante listado pelo ITU-T (2012) está relacionado ao corpo humano para aplicações vestíveis (*wearables*) de saúde e *home-care*. A IoT precisa dar suporte de alta qualidade e segurança para serviços relacionados ao corpo humano. Deve-se considerar a legislação e regulamentos de diferentes países sobre esses serviços uma vez que se projeta a IoT como uma tecnologia mundial. A relação com os humanos deve considerar o fornecimento de recursos *Plug and play* pelas redes IoT para "permitir geração, composição ou aquisição *on-the-fly* de configurações semânticas para integração e cooperação contínuas de itens interconectados com aplicativos e capacidade de resposta a requisitos de aplicação" (p. 6). Por fim, a rede IoT deve permitir o gerenciamento de suas operações normais. Os aplicativos de IoT geralmente funcionam automaticamente sem a participação de pessoas, mas todo o processo de operação deve ser passível de gerenciamento pelas partes envolvidas.

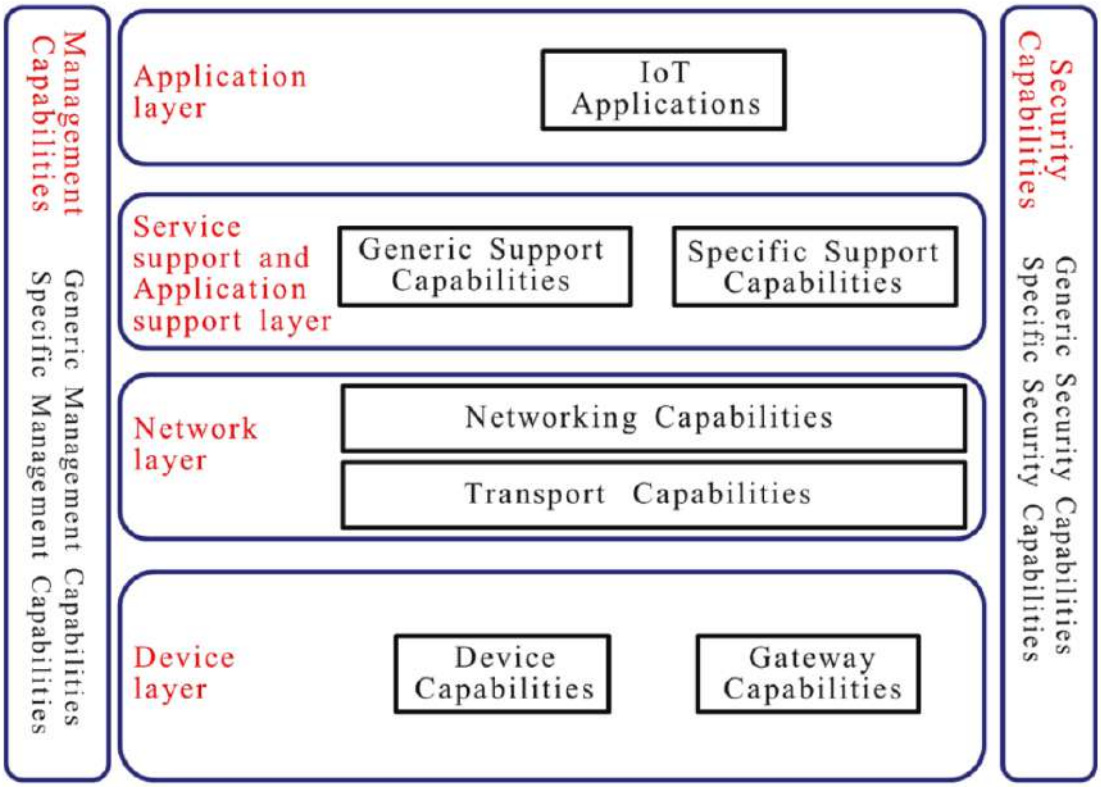
O ITU-T (2012) apresenta um modelo de referência para IoT composto de quatro camadas conforme apresentado no diagrama 6:

a) Camada de aplicação: dá suporte às aplicações que utilizando a tecnologia IoT;
b) Camada de suporte a serviços e aplicações: que deve dar suporte tanto a recursos genéricos, comuns a diferentes aplicações IoT, quanto a recursos específicos de alguns grupos de aplicações;
c) Camada de rede: suporta funções de controle para a conectividade de rede e de controle de acesso e transporte de recursos, gerenciamento ou autenticação de mobilidade, autorização e contabilidade. Também deve dar suporte aos recursos de transporte com foco no fornecimento de conectividade para o transporte de serviços e dados específicas de aplicativos de IoT, bem como no transporte de informações de controle e gerenciamento relacionadas à IoT;
d) Camada de dispositivo: dividida em dois tipos de recursos: do dispositivo e do *gateway*. Considerando o dispositivo, pode-se listar recursos de interação direta ou indireta com a rede de comunicação, tanto para coletar e carregar informações quanto para recebê-las. Outros recursos do dispositivo incluem a capacidade de construir redes *ad-hoc* e suporte a mecanismos de "dormir" e "acordar" para economia de energia. Já o *gateway* deve dar suporte à conexão de dispositivos de diferentes tecnologias com ou sem fio (CAN bus - barramento controlador de área de rede, ZigBee, *Bluetooth*, Wi-Fi), diferentes redes (PSTN, 2G, 3G, LTE, Ethernet, DSL) e conversão de protocolos de comunicação tanto entre dispositivos quanto entre o dispositivo e a rede.

Servindo às quatro camadas ainda se tem os recursos de gerenciamento da rede IoT que cobrem as classes de falha, configuração, contabilidade, desempenho e segurança (FCAPS) e os recursos de segurança que abrangem dois tipos:

a) Recursos de segurança genéricos que tratam da autorização, autenticação, uso e confidencialidade de dados, proteção da integridade e da privacidade, controle de acesso, auditoria de segurança e antivírus em geral nas camadas de aplicação, de rede e do dispositivo;
b) Recursos de segurança específicos associados a requisitos específicos de aplicativos como pagamento móvel e requisitos de segurança, por exemplo (ITU-T, 2012, p. 7).

Diagrama 6 – Modelo de Referência para IoT



Fonte: ITU-T, 2012, p. 7.

3.3 Internet das Coisas: Um Plano de Ação para o Brasil

Como já mencionado, o Banco Nacional de Desenvolvimento Econômico e Social (BNDES) e o Ministério da Ciência, Tecnologia, Inovações e Comunicação (MCTIC) iniciaram, em janeiro de 2017, um amplo estudo sobre a aplicação de Internet das Coisas no Brasil intitulado 'Internet das Coisas: um plano de ação para o Brasil' cujo objetivo foi propor um plano de ação estratégico sobre o tema para o país. Esse estudo gerou 28 documentos entre capítulos, relatórios e apresentações totalizando mais de 2.300 páginas. O estudo visou consolidar as aspirações do Brasil para IoT:

> Acelerar a implantação da Internet das Coisas como instrumento de desenvolvimento sustentável da sociedade brasileira, capaz de aumentar a competitividade da economia, fortalecer as cadeias produtivas nacionais, e promover a melhoria da qualidade de vida (BNDES, 2017e, v. 6, p. 12).

Os capítulos iniciais procuraram situar o Brasil e diversos países quanto ao desenvolvimento da Internet das Coisas fazendo uma análise de tendências, oferta e demanda. A seguir, o plano apresentou entrevistas com representantes de empresas públicas e privadas da área de TIC,

operadores de redes de telefonia e especialistas em economia, dentre outros (BNDES, 2017d). Em seguida, apresentou-se a organização do estudo em verticais e horizontais e a priorização de algumas dessas verticais para o Brasil. Posteriormente, o plano aprofundou o estudo em cada uma das verticais priorizadas (BNDES, 2017f). Por fim, o plano concluiu com proposta de iniciativas, aspectos regulatórios a serem considerados, além de relatórios finais.

Para organização do material, o plano dividiu os espaços físicos de operação da Internet das Coisas em 'Ambientes de Aplicação'. Essa análise facilita a identificação da interoperabilidade e interação entre os diversos atores do sistema que normalmente ocorrem dentro do mesmo ambiente, além de indicar os impactos em casos que transcendem setores específicos (BNDES, 2017b). A figura 1 exemplificou esses Ambientes de Aplicação escolhidos considerando as características do ambiente brasileiro.

Figura 1 – Ambientes de Aplicação para IoT

Fonte: BNDES, 2017b, v. 2A, p. 8, adaptado de Manyika *et al.*, 2015a, p. 9.

Quanto a essa organização, caberiam algumas considerações. Alguns autores organizam o universo IoT em 'casos de uso' (IoT ONE, 2018; Manyika *et al.*, 2015b). O BNDES (2017c) define casos de uso como a unidade básica para cálculo do impacto que pode ser alcançado com a implementação de uma solução IoT em determinado ambiente considerando que todo o processo (recebimento de dados, conexão com a rede externa e capacidade de processamento) será executado por interações M2M ou seja *Machine to Machine*, sem interferência humana. Complementarmente, o IoT ONE (2018) considera que os casos de uso definem o intervalo de

soluções possíveis que existem hoje ou que existirão no futuro sendo, portanto, dependentes da disponibilidade do mercado. Essa organização se contrapõe a organização por ‘setores econômicos’, que representam a forma mais tradicional de classificar as empresas segundo suas semelhanças operacionais, já que os casos de uso, por definição, podem abranger vários setores.

A organização em setores econômicos é mais aderente aos Ambientes de Aplicação onde a interoperabilidade e interação entre diversos atores ocorre, geralmente, dentro de um mesmo ambiente. Considerando esse antagonismo entre duas formas de agrupamento, o plano optou por usar a organização em Ambientes de Aplicação por considerar que (i) os usuários de IoT enxergam as soluções dentro desses ambientes, (ii) a visão por ambiente destaca a importância da interoperabilidade entre diferentes sistemas e (iii) essa segmentação é utilizada por importantes referências nos setores público e privado como, por exemplo, a AIOTI – *Alliance for Internet of Things Innovation* (BNDES, 2017b; BNDES, 2017c).

Os Ambientes de Aplicação passaram por um processo detalhado de estudo e priorização. Os insumos para essa priorização foram:

a) As aspirações do Brasil para IoT, já apresentadas;
b) A escolha dos Ambientes de Aplicação considerando a realidade brasileira, a saber: Fábricas, Saúde, Cidades, Lojas, Indústrias de base, Logística, Veículos, Rural, Casas, e Escritórios e ambientes administrativos (BNDES, 2017e).

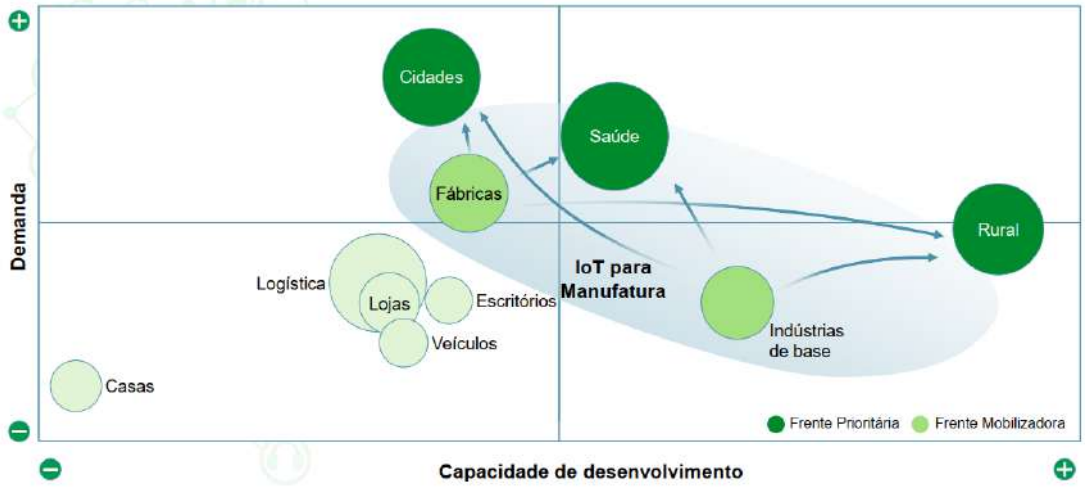
Esses Ambientes de Aplicação foram considerados como ‘verticais’ para priorização. As verticais foram analisadas por fóruns envolvendo representantes de setores públicos e privados, especialistas em IoT, TIC, economia e política além de representantes do BNDES e do MCTIC e avaliadas segundo critérios e métricas para priorização e definição de pesos representativos de sua importância. Esse processo foi representado na figura 2 (BNDES, 2017e).

Figura 2 – Processo de análise e priorização de verticais

Fonte: BNDES, 2017e, v. 6, p. 9.

O resultado desse processo é a Matriz de Priorização apresentada no diagrama 7. Nessa matriz apresentam-se as quatro verticais que foram desenvolvidas no plano: Cidades, Saúde, Meio Rural e Indústrias, essa última sendo o resultado da união dos Ambientes de Aplicação Fábricas e Indústria de base (BNDES, 2017e).

Diagrama 7 – Matriz de Priorização de Verticais



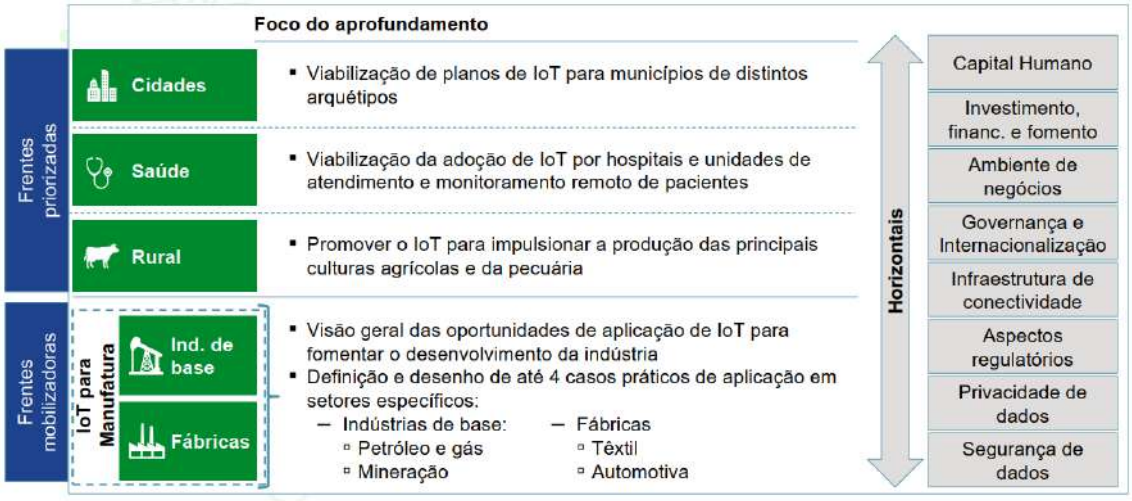
Fonte: BNDES, 2017e, v. 6, p. 130.

Foram definidas aspirações para cada uma das verticais priorizadas, a saber:

a) Cidades: “elevar a qualidade de vida da população por meio da adoção de tecnologias e práticas que viabilizem a gestão integrada dos serviços e a melhoria da mobilidade, segurança pública e uso de recursos”;
b) Saúde: “contribuir para a ampliação do acesso à saúde de qualidade no Brasil, por meio da criação de uma visão integrada dos pacientes, descentralização da atenção à saúde, e da melhoria de eficiência das unidades de saúde”;
c) Meio Rural: “aumentar a produtividade e a relevância do Brasil no comércio mundial de produtos agropecuários, com elevada qualidade e sustentabilidade socioambiental, e posicioná-lo como o maior exportador de soluções de IoT para agropecuária tropical”;
d) Indústria: “incentivar a produção de itens mais complexos e aumentar a produtividade nacional a partir de modelos de negócios inovadores e de maior cooperação nas diversas cadeias produtivas” (BNDES, 2018).

O estudo de cada uma dessas verticais foi aprofundado considerando inicialmente os seguintes aspectos ‘horizontais’: Capital Humano, Investimento, financiamento e fomento, Ambiente de negócios, Governança e Internacionalização, Infraestrutura de conectividade, Aspectos regulatórios, Privacidade de dados e Segurança de dados conforme apresentado no quadro 3 (BNDES, 2017e).

Quadro 3 – Aprofundamento das Verticais – Aspectos Horizontais



Fonte: BNDES, 2017e, v. 6, p. 131.

Posteriormente, foi feita uma seleção de quatro horizontais que foram consideradas essenciais a todas as verticais, conforme quadro 4.

Quadro 4 – Horizontais selecionadas

Fonte: BNDES, 2017e, v. 6, p. 48

O relatório final destaca o esforço do BNDES e do MCTIC no sentido de consolidar uma visão estratégica sobre IoT para o Brasil:

> Mais importante do que os documentos deste estudo é o legado de um ecossistema de IoT nacional, mais maduro e robusto. Isso está sendo alcançado por meio de uma construção inovadora, que está engajando atores de diversos órgãos públicos, sociedade civil, iniciativa privada e academia. A mensagem dessa integração é clara: "o Governo deseja atuar como facilitador, colocando a sociedade como protagonista dessa revolução" (BNDES, 2018, v. 9A, p. 3).

3.4 Tecnologias de Conectividade Propostas

Apresentou-se a seguir as características de conectividade propostas por vertical no plano Internet das Coisas: um plano de ação para o Brasil. No esforço de esclarecer as definições usadas, o plano apresentou uma descrição dos tipos de tecnologias de conectividade, dispositivos e aplicações consideradas, dos quais destacaram-se:

a) Redes cabeadas: tecnologia de longo e curto alcance cuja principal característica é a transmissão em meio confinado como cabos de cobre e fibras ópticas e tem como

exemplos as redes Ethernet, PLC – *Power Line Communications* e GPON – *Gigabit Passive Optical Network*;

b) Redes celulares: técnica de comunicação sem fio de longo alcance padronizadas pelo GSMA – *Global System for Mobile Communications Association* e 3GPP – *3rd Generation Partnership Project*. Nesse contexto, se destacam as soluções:
   - EC-GPRS – *Extended Coverage – General Packet Radio Services;*
   - LTE-M – *Long-Term Evolution – Machine Type Communications;*
   - NB-IoT – *Narrow Band – Internet of Things;*

c) Redes de curto alcance e alta banda: tecnologia de comunicação *wireless* com cobertura local (de algumas dezenas a poucas centenas de metros) e capacidade de banda situada entre Mbps e Gbps. Exemplo: Wi-Fi;

d) Redes *Low Power Wide Area* – LPWA: técnica de acesso de baixo consumo de energia, longo alcance e banda limitada que tem como exemplos LoRa – *Long Range*, Weightless, Sigfox e RPMA – *Random Phase Multiple Access*;

e) Redes de curto alcance e baixa banda: outra técnica de comunicação sem fio de cobertura local, mas com capacidade de banda entre kbps e Mbps. Exemplo: *Bluetooth*;

f) Redes *Ultra-Wide Band* – UWB: tecnologia de comunicação de baixo consumo de energia que pode ser utilizada para transmissão de altas taxas de dados e localização precisa do transmissor, especialmente *indoor*. Utiliza larga porção do espectro para transmissão, da ordem de centenas de MHz;

g) *Smart tag*: técnica de localização e identificação de objetos que tem como exemplos:
   - RFID – *Radio-Frequency Identification*;
   - Pontos de acesso *Bluetooth* (BLE *beacon* – *Bluetooth Low Energy beacon*);
   - NFC – *Near Field Communication*;

h) Redes *Mesh*: associada a uma topologia de rede, não é propriamente uma tecnologia de comunicação; é uma funcionalidade nas redes *wireless* em que os nós podem encaminhar pacotes vindos de outros nós da mesma rede. Exemplo: *Bluetooth* 5.0 e outras tecnologias que seguem o padrão IEEE 802.15.4;

i) Módulo de Geolocalização: dispositivo dotado de capacidade de definir dinamicamente sua localização por acesso GPS – *Global Positioning System*, e triangulação de sinais de outras redes;

j) *Advanced analytics*: técnicas de processamento de dados que utilizam computação cognitiva (*machine learning*) que trabalham um grande volume de dados como

treinamento para inferir padrões complexos e progressivamente aprimorar seu resultado (BNDES, 2017f).

Apresentou-se ainda um glossário com as definições relacionadas às tecnologias de Segurança da Dispositivo apresentadas nas verticais, a saber:

a) Criptografia embarcada: técnica de criptografia de dados geralmente executada em dispositivos com restrição de processamento, memória e comunicação;
b) *Anti jamming*: tecnologia que procura reduzir o risco de interferência na comunicação do dispositivo por outro sinal na mesma faixa de frequência;
c) *Anti tampering*: tecnologia que impede que o dispositivo seja violado fisicamente gerando alarmes podendo conduzir à sua incapacitação proposital;
d) Assinatura digital: técnicas e métodos de autenticação de informações com o objetivo de garantir a identidade dos usuários da rede;
e) *Blockchain*: tecnologia de segurança descentralizada que cria e compartilha um índice global de transações entre os componentes de uma rede;
f) Controle de acesso ao dispositivo: técnica que visa impedir o acesso remoto não autorizado a objetos conectados à rede;
g) Falha segura: técnica que, na ocorrência de falhas, procura garantir o nível de serviço dentro do mínimo aceitável através de funções pré-configuradas no objeto;
h) *Firmware* seguro: tecnologia que visa garantir a integridade do *software* embarcado nos objetos inteligentes impedindo que códigos adulterados sejam executados ou copiados, ou a utilização remota para correção de falhas;
i) Ingresso seguro à rede de acesso: técnicas que impedem o ingresso de objetos não autorizados à rede de comunicação;
j) Prevenção à negação de serviço: tecnologia de combate a ataques por DoS – *Denial of Service* que incapacitem prestação de serviços pela rede ou que transformem objetos da rede em atacantes a esses serviços (DDoS – *Distributed DoS*) (BNDES, 2017f).

3.4.1 Cidades

O BNDES (2017f) apontou as vantagens sociais e econômicas da aplicação de IoT no ambiente das cidades do Brasil. Destacou-se benefícios econômicos nas áreas de transporte (monitoramento do tráfico em tempo real), segurança (redução da mortalidade causada pela

violência urbana) e eficiência energética (economia com iluminação pública) calculando-se um ganho estimado de US$ 27 bilhões até 2025. Os benefícios sociais teriam grande alcance considerando que 85% da população brasileira vive em cidades perfazendo mais de 170 milhões de brasileiros no ambiente urbano. O plano também citou algumas barreiras a serem transpostas relacionadas com capacitação de servidores públicos, recursos para investimentos, dificuldades com a legislação de contratação pública, privacidade de dados dos cidadãos e cooperação intermunicipal. Outra questão que foi destacada é a grande diferença socioeconômica e técnica entre as prefeituras brasileiras (p. 8).

Foram estudados dentro do plano do BNDES dez eixos que representam os desafios para os municípios brasileiros, a saber: mobilidade, segurança pública, eficiência energética e saneamento, empreendedorismo e inovação, urbanismo e moradia, saúde pública, qualidade de vida, educação e formação humana, governança e instituições e, por fim, atividade econômica. Identificou-se que quatro deles sofreriam grande impacto com a aplicação da IoT: mobilidade, segurança pública, eficiência energética e saneamento, e saúde pública. Como o tema saúde pública está contido dentro da vertical saúde a ser apresentada, considerou-se os três primeiros no âmbito das cidades (BNDES, 2017f).

Esses três eixos foram detalhados segundo as seguintes dimensões:

a) Mobilidade:
    - Tempo de deslocamento e experiência no trânsito;
    - Gestão do transporte público;
    - Formas alternativas de deslocamento (bicicleta).
b) Segurança Pública:
    - Conjuntura e contexto da violência;
    - Incidentes;
    - Responsividade;
    - Outros desafios (sentimento de segurança, terrorismo).
c) Eficiência Energética e Saneamento:
    - Qualidade do ar e da água;
    - Gestão e distribuição de água, energia e outros (resíduos sólidos) (BNDES, 2017f).

Considerando essas dimensões, idealizou-se aplicações IoT que atenderiam a cada um dos três eixos. O quadro 5 apresentou as aplicações selecionadas inicialmente e a captura de valor esperada para os eixos Eficiência Energética e Saneamento e Outros (BNDES, 2017f).

Quadro 5 – Aplicações IoT – Cidades, eixos Eficiência, Saneamento e Outros

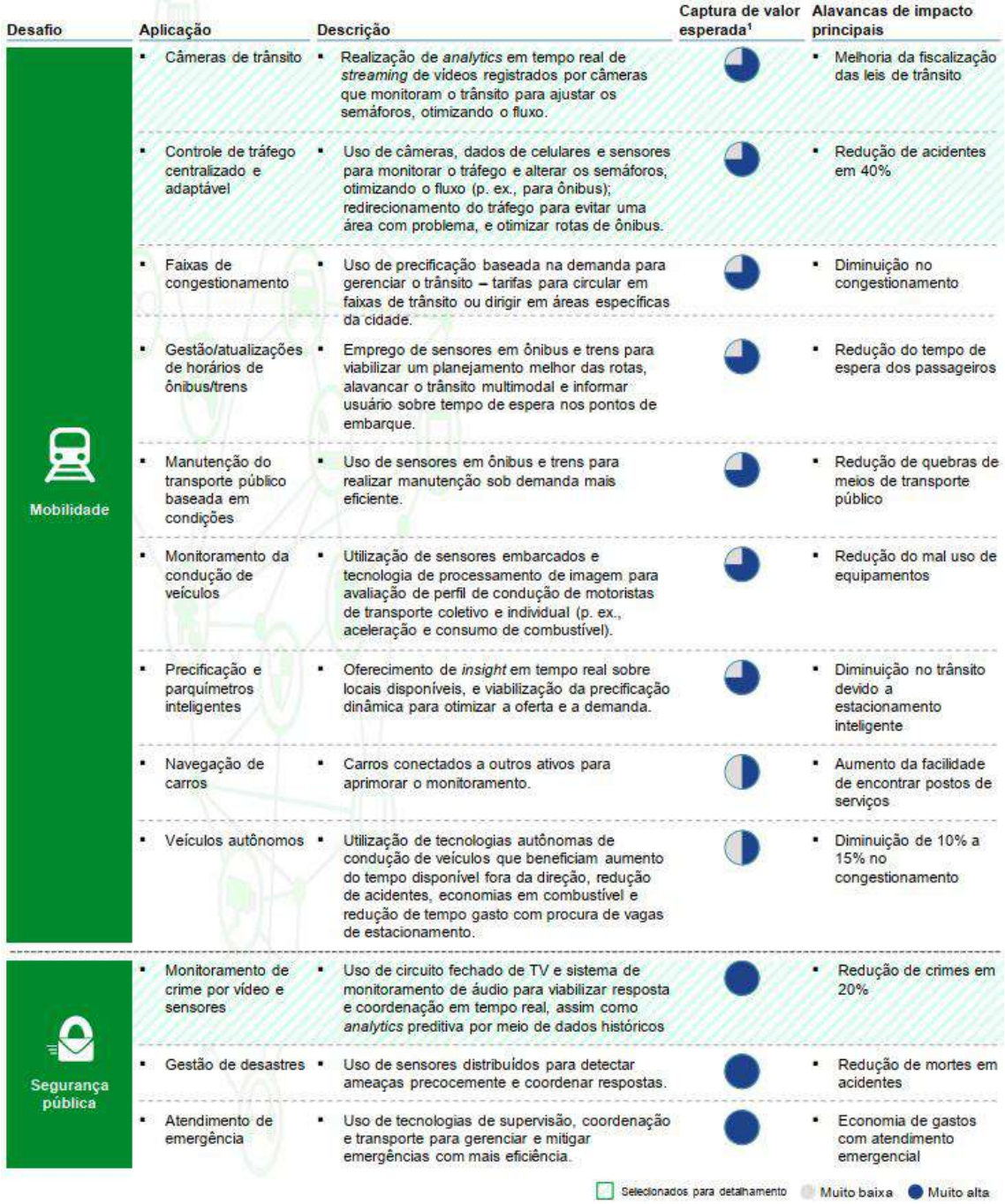
Desafio	Aplicação	Descrição	Captura de valor esperada[1]	Alavancas de impacto principais
Eficiência energética e saneamento	• Identificação de vazamentos de água	• Uso de sensores em canos, bombas e demais partes da infraestrutura hidráulica para monitorar condições e gerenciar perdas por meio de identificação e reparo de vazamentos ou mudança de pressão, conforme a necessidade.	●	• Redução dos vazamentos de água em 40%-50%
	• Medidores inteligentes de energia elétrica	• Redução de custos operacionais de leitura de medidores e prevenção de roubos.	●	• Redução de 50% de perdas não técnicas
	• Iluminação pública inteligente	• Utilização de sensores de monitoramento e de queima de lâmpadas para otimizar o uso e a substituição de ativos de iluminação pública.	◕	• Redução de custos operacionais de energia
	• Medidores de água inteligentes e gestão da demanda	• Redução dos custos operacionais e viabilização da coleta de dados sob demanda em tempo real – fornecer aos residentes e gerentes de propriedades dados de consumo de água em tempo real para que eles possam identificar onde o consumo está ocorrendo e também onde há vazamentos.	◕	• Redução da demanda de água em 5%
	• Automação de distribuição e subestações de energia	• Uso de automatização na subestação para reduzir perdas na linha de distribuição, reparo automático de defeitos na linha, e melhor gerenciamento dos equipamentos da subestação com aparelhos eletrônicos inteligentes.	◑	• Redução 4% de perdas nas linhas de transmissão
	• Lixeiras inteligentes	• Otimização das rotas de coleta de resíduos de lixeiras através do uso de sensores de monitoramento de capacidade.	◑	• Redução de custos operacionais na coleta de lixo
	• Monitoramento da qualidade da água	• Uso de sensores distribuídos para monitorar a qualidade da água nos canos, rios, lagos etc.	◑	• Redução de doenças relacionadas à qualidade da agua
	• Monitoramento da qualidade do ar	• Emprego de sensores distribuídos para monitorar partículas suspensas no ar.	◑	• Redução de doenças relacionadas à qualidade do ar
	• Tarifação inteligente de resíduos sólidos	• Uso de *tags* de identificação por radiofrequência para cobrança automática de taxa variável de acordo com o consumo.	◑	• Melhoria da produtividade em 23%
Outros	• Monitoramento estrutural (iluminação de ruas e pontes)	• Realização de manutenção preventiva sob demanda com sensores localizados na infraestrutura.	●	• Economia com gastos na manutenção de iluminação e pontes
	• Anúncios geolocalizados no transporte publico	• Seleção de anúncios em tempo real de acordo com região de passagem do transporte público.	◕	• Melhoria na taxa de retorno dos investimentos em publicidade
	• Melhoria da eficiência de ativos por meio de IoT	• Uso de sensores para coleta de dados sobre as condições das rodovias e os padrões de direção, por exemplo, usando dados para aprimorar a eficiência operacional.	◑	• Economia de custo operacional de manutenção de ativos
	• Realidade aumentada para crescimento de produtividade humana	• Uso de realidade aumentada para aplicação da lei e de serviços de correio, por exemplo.	◑	• Economia no uso de mão de obra e aumento da agilidade

□ Selecionados para detalhamento ○ Muito baixa ● Muito alta

Fonte: BNDES, 2017f, v. 7A, p. 24.

O quadro 6 apresentou também as aplicações selecionadas inicialmente e a captura de valor esperada mas para os eixos Mobilidade e Segurança Pública (BNDES, 2017f).

Quadro 6 – Aplicações IoT – Cidades, eixos Mobilidade e Segurança Pública



Desafio	Aplicação	Descrição	Captura de valor esperada[1]	Alavancas de impacto principais
Mobilidade	Câmeras de trânsito	Realização de *analytics* em tempo real de *streaming* de vídeos registrados por câmeras que monitoram o trânsito para ajustar os semáforos, otimizando o fluxo.		Melhoria da fiscalização das leis de trânsito
	Controle de tráfego centralizado e adaptável	Uso de câmeras, dados de celulares e sensores para monitorar o tráfego e alterar os semáforos, otimizando o fluxo (p. ex., para ônibus); redirecionamento do tráfego para evitar uma área com problema, e otimizar rotas de ônibus.		Redução de acidentes em 40%
	Faixas de congestionamento	Uso de precificação baseada na demanda para gerenciar o trânsito – tarifas para circular em faixas de trânsito ou dirigir em áreas específicas da cidade.		Diminuição no congestionamento
	Gestão/atualizações de horários de ônibus/trens	Emprego de sensores em ônibus e trens para viabilizar um planejamento melhor das rotas, alavancar o trânsito multimodal e informar usuário sobre tempo de espera nos pontos de embarque.		Redução do tempo de espera dos passageiros
	Manutenção do transporte público baseada em condições	Uso de sensores em ônibus e trens para realizar manutenção sob demanda mais eficiente.		Redução de quebras de meios de transporte público
	Monitoramento da condução de veículos	Utilização de sensores embarcados e tecnologia de processamento de imagem para avaliação de perfil de condução de motoristas de transporte coletivo e individual (p. ex., aceleração e consumo de combustível).		Redução do mal uso de equipamentos
	Precificação e parquímetros inteligentes	Oferecimento de *insight* em tempo real sobre locais disponíveis, e viabilização da precificação dinâmica para otimizar a oferta e a demanda.		Diminuição no trânsito devido a estacionamento inteligente
	Navegação de carros	Carros conectados a outros ativos para aprimorar o monitoramento.		Aumento da facilidade de encontrar postos de serviços
	Veículos autônomos	Utilização de tecnologias autônomas de condução de veículos que beneficiam aumento do tempo disponível fora da direção, redução de acidentes, economias em combustível e redução de tempo gasto com procura de vagas de estacionamento.		Diminuição de 10% a 15% no congestionamento
Segurança pública	Monitoramento de crime por vídeo e sensores	Uso de circuito fechado de TV e sistema de monitoramento de áudio para viabilizar resposta e coordenação em tempo real, assim como *analytics* preditiva por meio de dados históricos		Redução de crimes em 20%
	Gestão de desastres	Uso de sensores distribuídos para detectar ameaças precocemente e coordenar respostas.		Redução de mortes em acidentes
	Atendimento de emergência	Uso de tecnologias de supervisão, coordenação e transporte para gerenciar e mitigar emergências com mais eficiência.		Economia de gastos com atendimento emergencial

Selecionados para detalhamento · Muito baixa · Muito alta

Fonte: BNDES, 2017f, v. 7A, p. 23.

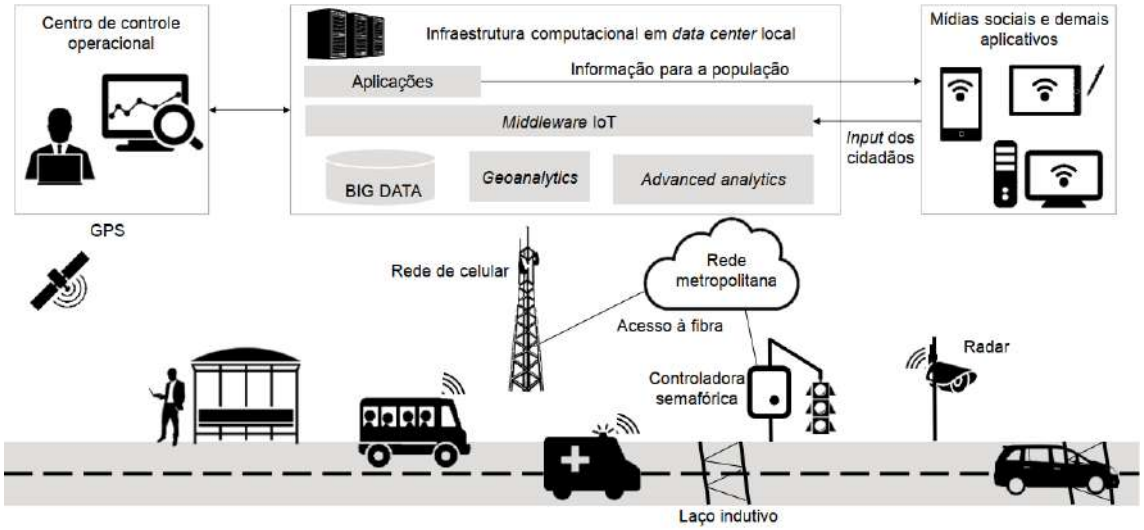
Após análises, foram detalhadas as aplicações controle de tráfego centralizado e adaptável, no eixo mobilidade, monitoramento de crimes por vídeo e sensores, no eixo segurança pública, monitoramento por vídeo, nos eixos mobilidade e segurança, e medidores inteligentes de

energia elétrica e iluminação pública inteligente, no eixo eficiência energética e saneamento que foram analisados a seguir sob o aspecto de conectividade. Essas aplicações foram selecionadas segundo a captura de valor esperada, facilidade de implementação e capacidade de habilitar tecnologicamente outras aplicações (BNDES, 2017f).

3.4.1.1 Controle de tráfego centralizado e adaptável

Essa aplicação pressupôs a instalação de sensores IoT em diversos elementos do trânsito urbano que possibilitem a captação de dados sobre as condições do trânsito e a localização de veículos de interesse público (transporte, saúde, segurança), sua transmissão e armazenamento em ambiente computacional de alta capacidade e sua análise por algoritmos que permitam tomar ações em tempo real para auxílio à mobilidade urbana. A aplicação também prevê o processamento de dados provenientes das mídias sociais dos cidadãos e deve disponibilizar informações *on-line* sobre as condições de trânsito. Estimou-se que essa aplicação teria potencial de redução no consumo de combustíveis e melhoria da qualidade de vida nas cidades onde for implementada pela diminuição do tempo de deslocamento e da poluição atmosférica. A figura 3 apresentou a visão sistêmica da solução (BNDES, 2017f).

Figura 3 – Controle de tráfego centralizado e adaptável



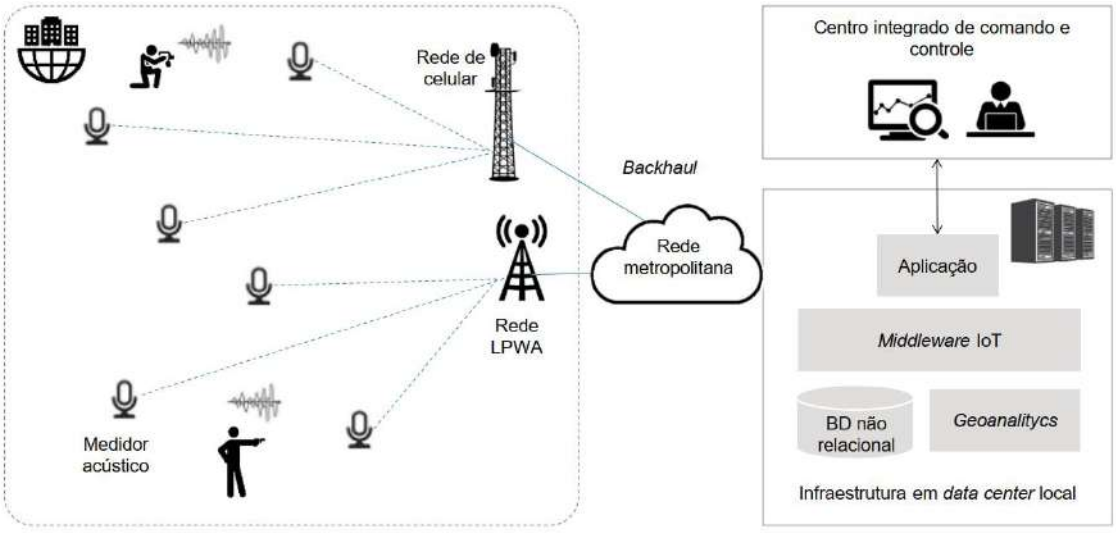
Fonte: BNDES, 2017f, v. 7A, p. 51.

A aquisição de dados se faria por *smart tags* nos veículos em conexão com pontos de acesso *Bluetooth* de baixa energia (BLE – *Bluetooth Low Energy Beacons*), localização por GPS via rede celular (GPRS – *General Packet Radio Services* ou NB-IoT – *Narrow Band – Internet of Things*) e via radares dotados de mecanismos de reconhecimento de caracteres (OCR – *Optical Character Recognition*) para leitura automática de placas de veículos. A proposta de conectividade com os sistemas de análise utilizaria redes cabeadas por fibra óptica e redes celulares, principalmente aquelas já adaptadas para o IoT como EC-GPRS – *Extended Coverage – General Packet Radio Services*, LTE-M – *Long-Term Evolution – Machine Type Communications* e NB-IoT – *Narrow Band – Internet of Things*. As redes ópticas permitiriam não só o tráfego de informações da aplicação como também das estações rádio base das redes celulares. Esses sistemas de comunicação serão apresentados mais adiante (BNDES, 2017f).

3.4.1.2 Monitoramento de crimes por sensores

Essa solução seria implementada pela instalação de sensores de áudio no ambiente urbano que fariam o seu constante monitoramento e permitiriam captar, identificar e localizar determinados sons específicos como disparos de armas de fogo, tiroteios, colisão de automóveis e explosões, por exemplo. As informações seriam transmitidas a coordenação das operações policiais da região permitindo agilidade no atendimento de ocorrências e o salvamento de vidas. A figura 4 demonstrou a visão sistêmica da aplicação (BNDES, 2017f).

Figura 4 – Monitoramento de crimes por sensores



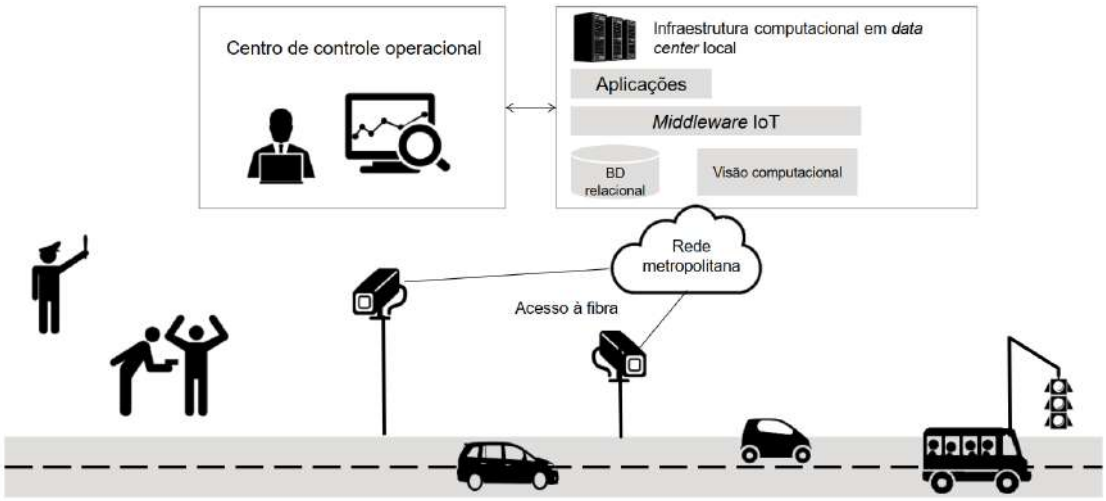
Fonte: BNDES, 2017f, v. 7A, p. 56.

Além de microfones, o dispositivo de aquisição de dados faria a conversão analógico-digital do som e seu processamento visando comparar o evento com assinaturas acústicas pré-programadas e inferir sua localização. Para conectividade, foram destacados dois tipos de redes de acesso: celular e LPWA – *Low Power Wide Area* incluindo as recentemente concebidas para atender a IoT como NB-IoT, EC-GPRS, Weightless, LoRa – *Long Range* e Sigfox. Essas redes sem fio de grande alcance foram consideradas mais adequadas devido à necessidade de cobertura do sistema (BNDES, 2017f).

3.4.1.3 Monitoramento por vídeo

Essa proposta, apresentada na figura 5, considerou a implantação de câmeras de alta definição no espaço urbano conectadas por infraestrutura de fibras ópticas a um centro de controle operacional onde se faria o armazenamento e processamento das imagens. Previu-se o uso de algoritmos de visão computacional que permitiriam a interpretação de imagens sem intervenção humana conferindo ao sistema agilidade na tomada de decisões com impacto direto na segurança pública e na mobilidade urbana (BNDES, 2017f).

Figura 5 – Monitoramento por vídeo



Fonte: BNDES, 2017f, v. 7A, p. 59.

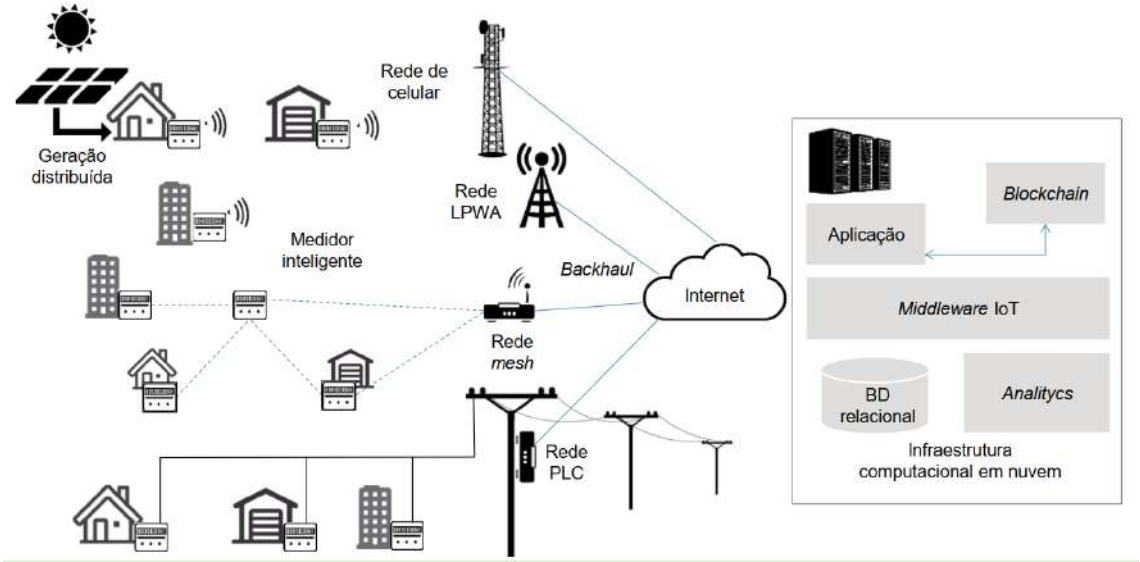
Por se tratar de sistema de vídeo de alta definição, as altas taxas de transmissão de dados decorrentes demandariam uma rede cabeada de alto desempenho, preferencialmente por fibra

óptica. A tecnologia mais indicada é a GPON – *Gigabit Passive Optical Network* (BNDES, 2017f).

3.4.1.4 Medidores inteligentes e gestão da demanda de energia

A aplicação se apoiou na concepção de infraestrutura de medição avançada (AMI – *Advanced Metering Infrastructure*) dentro do conceito de *smart grid*. Esses conceitos preveem a coleta de informações referentes à energia consumida e gerada pelos usuários, a sua análise e influência em opções de geração e consumo de energia baseado em preços. Seria possível ainda avaliar a qualidade do fornecimento de energia elétrica, comportamentos fraudulentos e implementar funções de desligamento e religamento remoto do fornecimento. Essas características exigiriam uma rede de comunicação bidirecional, medidores elétricos inteligentes, sistema de armazenamento e processamento de dados, conforme apresentado na figura 6 (BNDES, 2017f).

Figura 6 – Medidores inteligentes e gestão da demanda de energia



Fonte: BNDES, 2017f, v. 7A, p. 62.

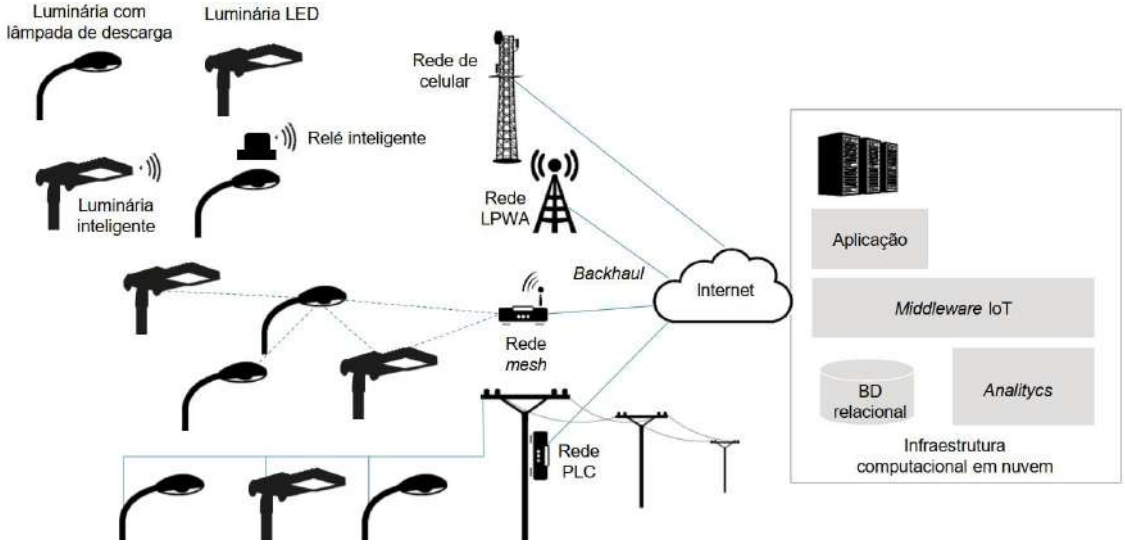
Os medidores inteligentes deveriam incorporar capacidades de armazenamento de dados, mecanismos de segurança, relés para desligamento e religamento além da capacidade de comunicação criptografada e medição de energia. Quanto a conectividade necessária, uma série de tecnologias poderiam ser usadas: redes celulares e LPWA (NB-IoT, LoRa e RPMA – *Random Phase Multiple Access*) dentre as tecnologias wireless e PLC – *Power Line*

Communications, dentre as tecnologias cabeadas. Quanto à topologia da rede, seria possível implementar redes tipo *mesh* onde os medidores teriam papel ativo no roteamento de dados vindos de outros medidores (BNDES, 2017f).

3.4.1.5 Iluminação pública inteligente

A proposta apresentou um sistema de iluminação pública em que as luminárias teriam capacidade de processamento para avaliar a sua condição de operação (degradação e queima das lâmpadas), a luminosidade do ambiente e consequente intensidade de iluminação necessária (‘dimerização’), além do usual controle para ligamento e desligamento. A figura 7 demonstrou a visão sistêmica da aplicação (BNDES, 2017f).

Figura 7 – Iluminação pública inteligente



Fonte: BNDES, 2017f, v. 7A, p. 66.

A conectividade necessária a esse sistema teve muita similaridade com a aplicação do medidor elétrico inteligente em razão de ambos se aplicarem ao sistema elétrico e possuírem uma grande quantidade de pontos a serem atendidos, estimados em 80 milhões de unidades consumidoras de energia elétrica e 19 milhões de pontos de iluminação pública, respectivamente, em 2017 (BNDES, 2017f).

3.4.1.6 Necessidades e capacidades

Para cada uma das aplicações IoT detalhadas, foram avaliadas as necessidades tecnológicas essenciais dos dispositivos IoT, a conectividade necessária, o suporte às aplicações e as questões relacionadas à segurança da informação. O quadro 7 apresentou essas necessidades considerando somente os aspectos de Conectividade e Segurança da Informação. Como Segurança da Informação nesse quadro, foram listadas técnicas que procurariam garantir a segurança do dispositivo IoT (BNDES, 2017f).

Quadro 7 – Necessidades Tecnológicas – Cidades

Aplicação	Nome	Controle de tráfego centralizado e adaptável	Monitoramento de crime por sensores	monitoramento por vídeo (segurança e mobilidade)	Medidores inteligentes e gestão da demanda de energia	Iluminação pública inteligente	Necessidade
Conectividade	Redes Low Power Wide Area		✓		✓	✓	◕
	Redes cabeadas	✓		✓	✓	✓	●
	Redes celular	✓	✓		✓	✓	●
	Redes de curto alcance e alta banda						○
	Redes de curto alcance e baixa banda	✓					◔
	Redes mesh				✓	✓	◑
	Redes Ultra Wideband						○
Segurança da informação	Criptografia embarcada	✓			✓		◑
	Anti jamming	✓					◔
	Anti tampering	✓			✓		◑
	Assinatura digital				✓		◔
	Blockchain				✓		◔
	Controle de acesso ao dispositivo	✓		✓	✓	✓	◕
	Falha segura	✓			✓	✓	◑
	Firmware seguro	✓		✓	✓	✓	◕
	Ingresso seguro à rede de acesso	✓	✓		✓	✓	●
	Prevenção a DDoS	✓		✓	✓	✓	◕

Legenda para Necessidades: ● **Alta** ◑ **Média** ○ **Baixa.**

Fonte: Adaptado de BNDES, 2017f, v. 7A, p. 26.

Foi realizada uma análise qualitativa da relevância de cada tecnologia para o desenvolvimento da aplicação (coluna Necessidades) assim como da capacidade local que espelha a quantidade e habilidade de atores no cenário nacional com as competências necessárias para o seu desenvolvimento (coluna Capacidades). Nessa última coluna, o sinal verde significa confiança, o amarelo, atenção e o vermelho, dificuldades quanto a capacidade dos atores. Os resultados dessa análise para Conectividade e Segurança da Informação são apresentados no quadro 8.

Esse quadro destacou que as tecnologias de conectividade mais relevantes são as redes LPWA, redes cabeadas e celulares. Destacou também que há carência de atores para LPWA e redes celulares. O quadro 8 mostrou ainda que as tecnologias de segurança mais relevantes são controle de acesso ao dispositivo, *firmware* seguro, ingresso seguro à rede de acesso e prevenção contra negação de serviço (DDoS – *Distributed Denial of Service*). Com relação à capacidade tecnológica local, há de carência de atores para as tecnologias de *anti tampering*, falha segura e *firmware* seguro (BNDES, 2017f).

Quadro 8 – Necessidades e Capacidades para Conectividade e Segurança – Cidades

	Tecnologias	Necessidades [%]				Capacidades		
		25	50	75	100			
Conectividade	Redes cabeadas	■	■	■				■
	Redes celulares	■	■	■			■	
	Redes Low Power Wide Area – LPWA	■	■	■			■	
	Redes de curto alcance e alta banda							■
	Redes de curto alcance e baixa banda	■						■
	Redes Ultra-Wide Band – UWB							■
	Redes Mesh	■	■				■	
Segurança do dispositivo	Criptografia embarcada	■	■				■	
	Anti jamming	■					■	
	Anti tampering	■	■			■		
	Assinatura digital	■					■	
	Blockchain	■					■	
	Controle de acesso ao dispositivo	■	■	■			■	
	Falha segura	■	■			■		
	Firmware seguro	■	■	■		■		
	Ingresso seguro à rede de acesso	■	■	■			■	
	Prevenção à negação de serviço	■	■	■			■	

Legenda para Capacidades – Status:

■ **- Confiança;**
■ **- Atenção;**
■ **- Dificuldade.**

Fonte: Adaptado de BNDES, 2017f, v. 7A, p. 28 e 30.

3.4.2 Saúde

As vantagens sociais e econômicas da aplicação de IoT no ambiente de saúde foram destacadas pelo BNDES (2017g) na melhoria da qualidade de vida da população e no aumento da eficiência das unidades de saúde em contrapartida aos aumentos com os gastos de saúde. Estimou-se que

entre US$ 5 e US$ 39 bilhões até 2025 poderiam ser economizados com a aplicação de conceitos de IoT na área de saúde no Brasil o que representa entre 3 e 21% do gasto em saúde em 2014. Entretanto, questões regulatórias, privacidade dos dados clínicos pessoais, problemas de conectividade em áreas remotas do país e até disponibilidade de recursos para avaliar corretamente o custo-efetividade de tecnologias foram listadas como barreiras ao desenvolvimento e adoção de IoT na saúde brasileira (BNDES, 2017g).

O plano do BNDES estudou três eixos que materializam os desafios na área da saúde no Brasil: Qualidade de Vida que atenderia ao objetivo de melhoria do estado de saúde da população, Satisfação do Paciente para o objetivo de incremento da satisfação de cidadãos e profissionais de saúde e Sustentabilidade Financeira do Sistema de saúde. Pôde-se destacar:

> Nossa população é acometida por uma tripla carga de doenças (crônicas, infectocontagiosas e de causas externas/violência), e pelo rápido processo de envelhecimento. A cobertura do sistema de saúde e os indicadores-chave de desempenho, como mortalidade infantil e materna, melhoraram significativamente nas últimas décadas, mas a coordenação do cuidado nos diferentes níveis de atenção é ainda incipiente. Um dos desafios é justamente a integração dos diferentes atores do sistema de saúde, estruturados em torno de uma visão unificada das pessoas, sejam elas pacientes ou não. Por último, o fenômeno global conhecido como "inflação médica", principalmente atribuído à constante incorporação de novas tecnologias de diagnóstico e tratamento, deve desafiar a sustentabilidade financeira do sistema de saúde brasileiro. Portanto, a melhoria da gestão dos recursos existentes é fundamental para que a área continue absorvendo inovações que impactem positivamente a vida das pessoas (BNDES, 2017g, v 7B, p. 6).

Os três eixos foram estudados considerando as seguintes informações:

a) Qualidade de Vida:
   - Aumento da cobertura de atenção primária e diminuição da mortalidade infantil e materna nas últimas décadas;
   - Doenças crónicas são a principal causa de morte no país, mas doenças infecciosas e causas externas/violência são relevantes;
   - Apesar da melhoria dos hábitos de vida dos brasileiros em geral (menos tabagismo, melhores hábitos alimentares) ainda existem riscos preocupantes (obesidade, diabetes, hipertensão arterial);
   - Até 2030, a população acima de 60 anos deverá triplicar.

b) Satisfação do Paciente:
   - O SUS – Sistema Único de Saúde brasileiro tem cobertura mais ampla do que países com maior renda *per capita*;

- Os gastos com saúde representam 8,3% do PIB nacional, mas os resultados para o cidadão são menores em comparação com países em que ocorrem gastos semelhantes;
- O gasto com o SUS representa 7% do orçamento público enquanto sistemas similares em outros países representam 15%.

c) Sustentabilidade Financeira do Sistema:
   - A "inflação médica" que tem acometido todo o mundo aumenta os gastos com saúde;
   - Os gastos do governo, dos pacientes privados e os custos das operadoras privadas de saúde vêm aumentando acima da inflação;
   - Em todo o mundo, estão sendo reestudados modelos de pagamento por serviços de saúde;
   - Gasta-se mais no Brasil com atendimentos de média e alta complexidade do que em países que são referência nesses atendimentos (BNDES, 2017g).

Essas informações levaram a uma lista de dez desafios para a área de saúde, agrupados em torno dos três eixos, em que foram grifados os quatro desafios considerados principais, a saber:

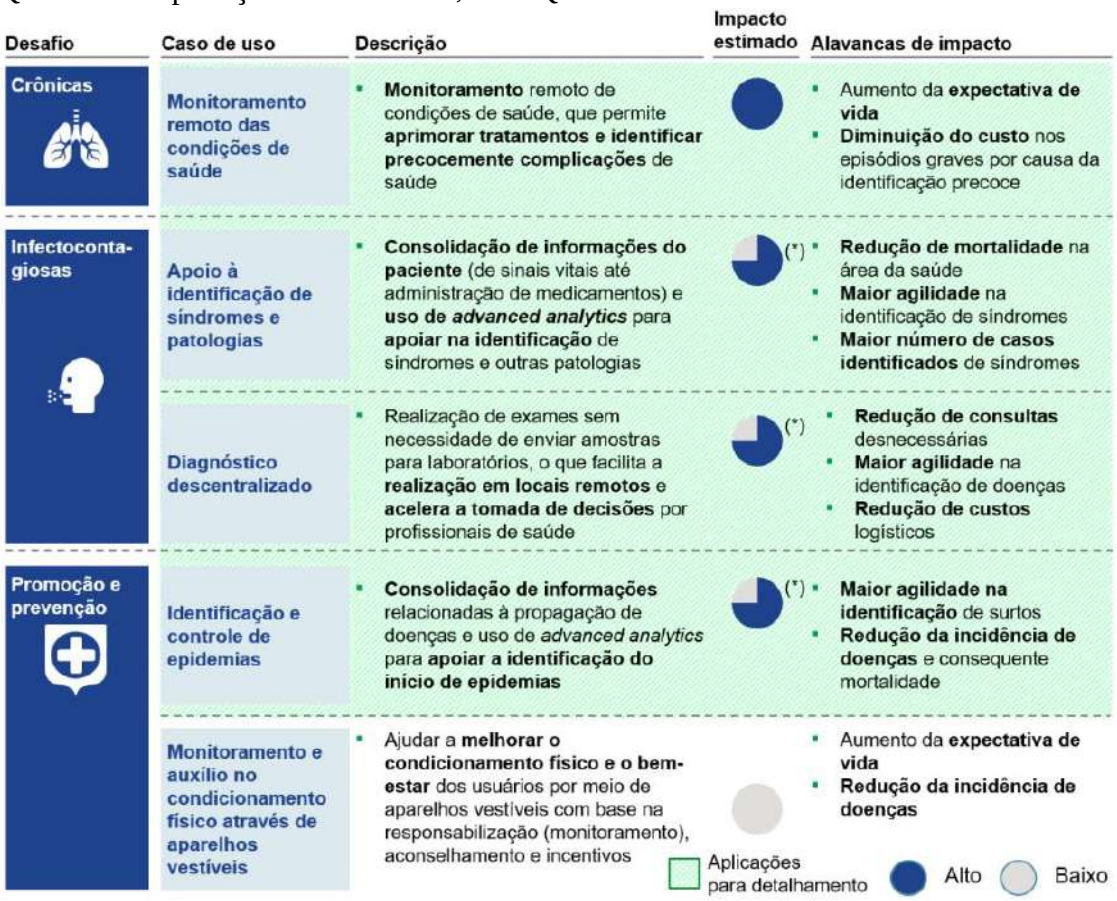
a) Qualidade de vida:
   - **Doenças crônicas**;
   - **Doenças infectocontagiosas**;
   - Causas externas/violência;
   - **Promoção e prevenção à saúde**;
   - Envelhecimento da população.

b) Satisfação do paciente:
   - Aumento das expectativas;
   - Gestão da informação/visão do paciente

c) Sustentabilidade financeira do sistema:
   - Cobrança;
   - **Eficiência de gestão**;
   - Inovação (BNDES, 2017g).

Foram considerados os casos de uso de tecnologia IoT para atender a esses quatro desafios. O quadro 9 apresentou as propostas iniciais de casos de uso e estimativa de captura de valor para o eixo Qualidade de Vida (BNDES, 2017g).

Quadro 9 – Aplicações IoT – Saúde, eixo Qualidade de Vida



Fonte: BNDES, 2017g, v. 7B, p. 13.

O quadro 10 apresentou essas propostas e estimativa de captura de valor para o eixo Sustentabilidade Financeira 1/2 (BNDES, 2017g).

Quadro 10 – Aplicações IoT – Saúde, eixo Sustentabilidade Financeira 1/2

Fonte: BNDES, 2017g, v. 7B, p. 15.

E, complementando, o quadro 11 apresentou as propostas e estimativa de captura de valor para o eixo Sustentabilidade Financeira 2/2 (BNDES, 2017g).

Quadro 11 – Aplicações IoT – Saúde, eixo Sustentabilidade Financeira 2/2

Fonte: BNDES, 2017g, v. 7B, p. 16.

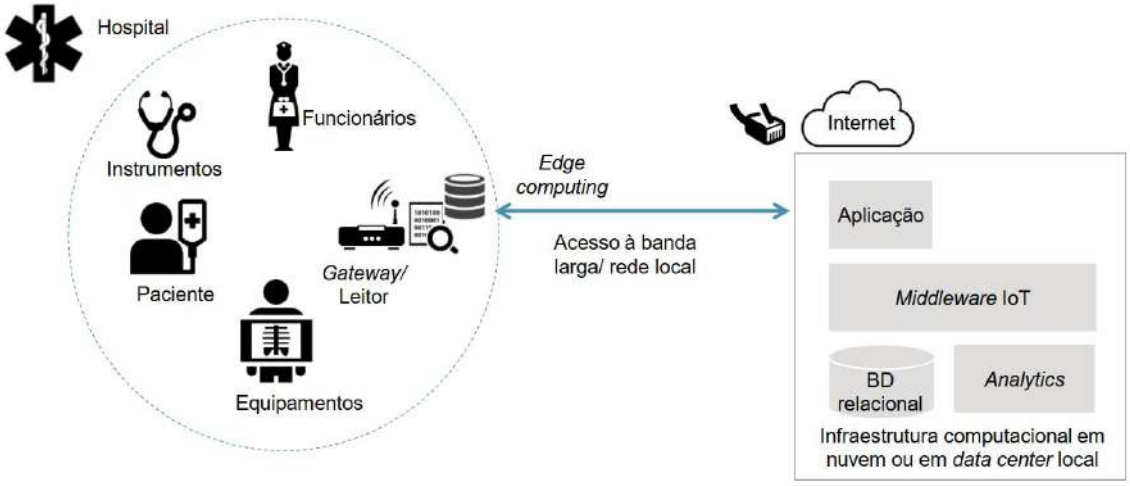
Dentre esses casos de uso, foram selecionados cinco por sua relevância, alto impacto e facilidade de desenvolvimento e que foram detalhadas nas aplicações: Localização de ativos e pessoas nas unidades de saúde, no eixo Eficiência de gestão e Monitoramento remoto das condições dos pacientes com diabetes, Diagnóstico descentralizado, Apoio ao diagnóstico de síndromes e patologias, e Identificação e controle de epidemias, dentro do eixo Qualidade de Vida. Essas aplicações foram analisadas a seguir com foco na conectividade necessária à sua viabilização (BNDES, 2017g).

3.4.2.1 Localização de ativos e pessoas nas unidades de saúde

A solução proposta, apresentada na figura 8, considerou o monitoramento de médicos, enfermeiros, pessoal de apoio e pacientes, além de equipamentos hospitalares e insumos de alto valor, itens de instrumentação e outros itens mais comuns, mas de impacto na operação de hospitais. A captura dos dados se faria por *smart tags* que se conectariam com *gateways*

espalhados pelas unidades de saúde e estes as transfeririam a *data centers* via rede local em banda larga para processamento. Essa aplicação permitiria o melhor uso dos ativos hospitalares, economia de tempo dos diversos profissionais de saúde envolvidos e agilidade no atendimento de pacientes, além de melhoria da segurança física do ambiente e prevenção de roubos e fraudes (BNDES, 2017g).

Figura 8 – Localização de ativos e pessoas nas unidades de saúde.



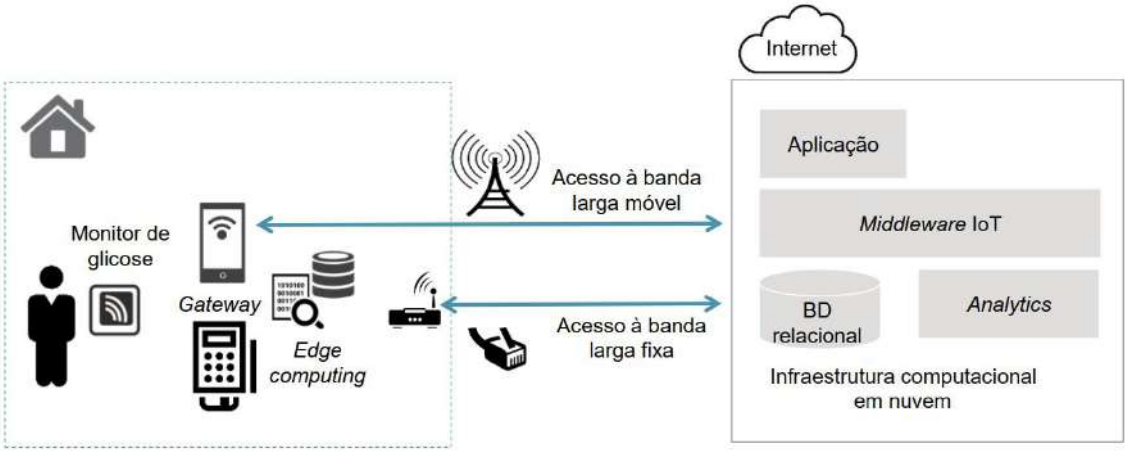
Fonte: BNDES, 2017g, v. 7B, p. 46.

A aquisição de dados utilizaria tags que permitissem a conexão com pontos de acesso *Bluetooth* (BLE – *Bluetooth Low Energy Beacons*) ou RFID ativa que também fariam a localização do item. A Conectividade seria provida por *gateways* e leitores de *smart tags*, classificados como rede de curto alcance e baixa banda, conectados à rede LAN – *Local Area Network*. Para maior precisão na localização, seria necessário o uso da tecnologia *Ultra-Wide Band* – UWB para conectividade (BNDES, 2017g).

3.4.2.2 Monitoramento remoto das condições dos pacientes com diabetes

Para essa aplicação, considerou-se a implantação de um monitor de glicose no paciente que faria o monitoramento dos níveis glicêmicos em tempo real, conforme apresentado na figura 9. A conexão com nuvem ser faria por *gateways* ou *smartphone* com essa facilidade. Os dados adquiridos seriam processados na nuvem para extrair significado e encaminhados na forma de relatórios para pacientes, médicos e planos de saúde (BNDES, 2017g).

Figura 9 – Monitoramento remoto das condições dos pacientes com diabetes



Fonte: BNDES, 2017g, v. 7B, p. 50.

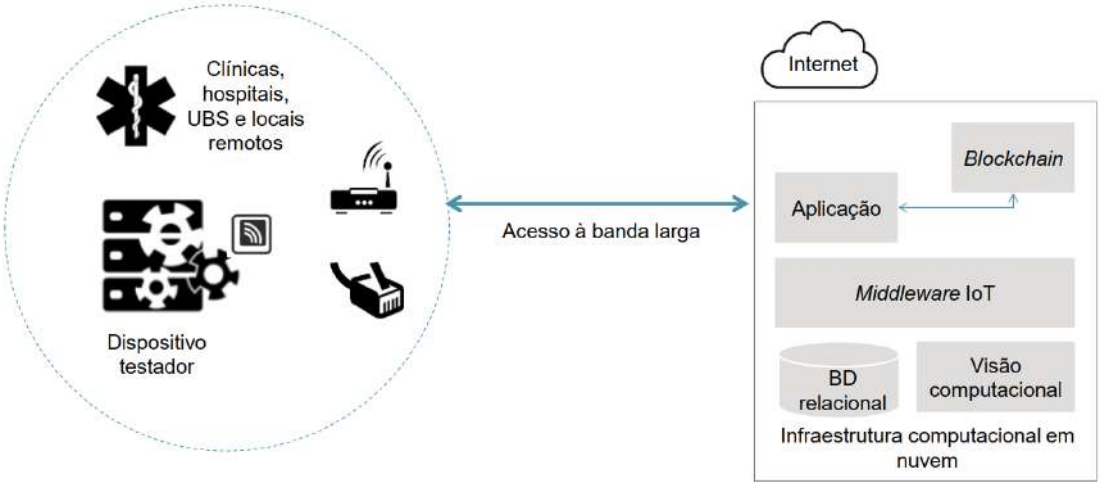
Nessa solução, a conectividade utilizaria redes de curto alcance de baixa e alta banda com a aquisição de dados por sensores *Bluetooth Low Energy* – BLE e *Near Field Communication* – NFC (BNDES, 2017g).

3.4.2.3 Diagnóstico descentralizado

Essa aplicação se baseou em dispositivos testadores que identificam rapidamente patógenos de doenças específicas a partir de amostras de sangue, saliva e outros fluídos e tecidos corporais. Esses dispositivos mediriam ainda frequência cardíaca, temperatura, níveis de oxigênio e pressão arterial dos pacientes em tempo real. Os dados seriam armazenados no dispositivo e transferidos para a nuvem para diagnóstico e relatórios. A realização desses testes e diagnósticos de forma descentralizada permitiria maior agilidade na identificação e início do tratamento de doenças, redução de custos advindos do transporte de materiais biológicos dos pacientes e permitindo o acesso a esses serviços de saúde a populações distantes dos grandes centros urbanos (BNDES, 2017g).

A conectividade para essa solução, apresentada na figura 10, utilizaria redes *wireless* de curto alcance ou redes cabeadas (Ethernet) já que o ambiente previsto para a instalação do dispositivo testador é *indoor* (BNDES, 2017g).

Figura 10 – Diagnóstico descentralizado



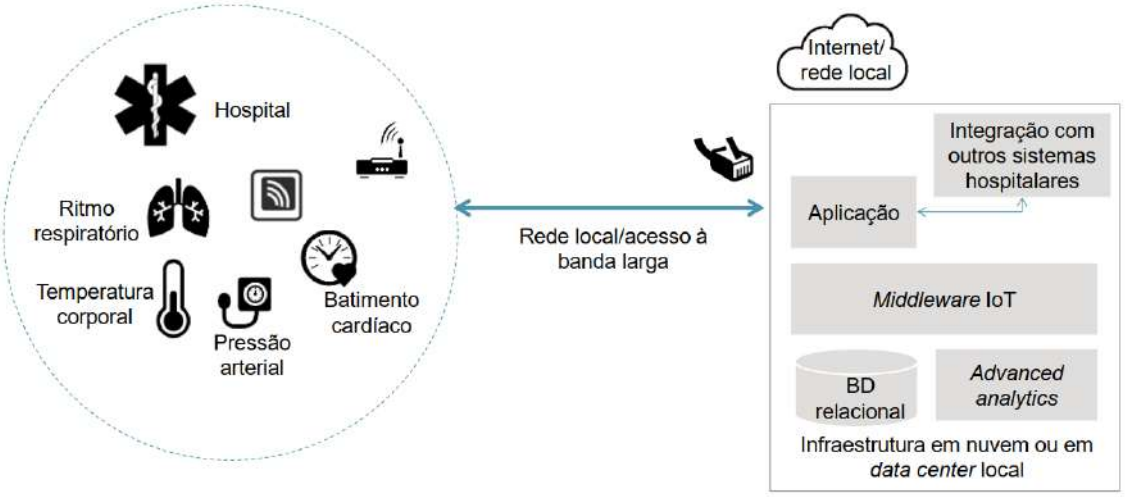
Fonte: BNDES, 2017g, v. 7B, p. 54.

3.4.2.4 Diagnóstico de síndromes e patologias

A solução proposta para Diagnostico de Síndromes e Patologias se fundamentou no monitoramento em tempo real da pressão arterial, temperatura, frequência cardíaca e respiratória de pacientes internados em hospitais. Como a reação do organismo a infecções do tipo sepse frequentemente oferecem risco à vida de pacientes, a rápida identificação dessa condição é importante e seria obtida por monitoramento contínuo dos sinais vitais do paciente. Esse monitoramento se faria por sensores empregando tecnologia MEMS – *Microelectromechanical Systems* ou óptica para a aquisição de dados. O armazenamento e tratamento dos dados adquiridos se faria localmente e na infraestrutura pública em nuvem (BNDES, 2017g).

Essa solução também usaria *gateways* BLE (redes de curto alcance e baixa banda) que se conectariam à rede local por interface cabeada ou sem fio como apresentado na figura 11 (BNDES, 2017g).

Figura 11 – Apoio ao diagnóstico de síndromes e patologias

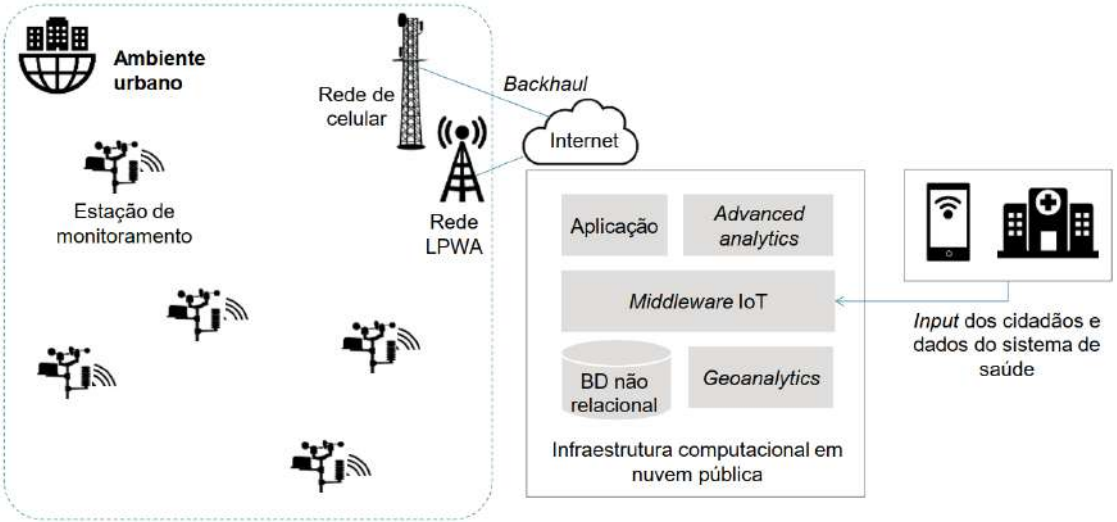


Fonte: BNDES, 2017g, v. 7B, p. 58.

3.4.2.5 Identificação e controle de epidemias

Essa solução prevê o monitoramento contínuo de variáveis ambientais por estações de monitoramento inseridas no ambiente urbano conforme exposto na figura 12. Os dados coletados seriam avaliados por *software* que emitiriam relatórios para as autoridades envolvidas. O sistema seria de grande valia para a identificação de enfermidades relacionadas com a qualidade do ar além de dengue e gripe possibilitando a rápida identificação e predição de focos epidemiológicos (BNDES, 2017g).

Figura 12 – Identificação e controle de epidemias



Fonte: BNDES, 2017g, v. 7B, p. 62.

A conectividade dessa solução se faria por redes LPWA e pela rede celular urbana, já que as estações de monitoramento seriam instaladas nesse ambiente. O (BNDES, 2017g) destacou as tecnologias GPRS, LTE-M e NB-IoT para as redes celulares e LoRa, Sigfox e RPMA para redes LPWA.

3.4.2.6 Necessidades e capacidades

Apresentou-se as tecnologias relevantes com suas necessidades para atender às aplicações IoT detalhadas para a vertical Saúde. O quadro 12 mostrou essas necessidades considerando somente os aspectos de Conectividade e Segurança da Informação. Ressaltou-se que essa concepção do uso de tecnologias de conectividade e segurança não é exaustiva nem contempla todas as possibilidades de uso podendo existir outras combinações viáveis. Aqui também a Segurança da Informação se referiu a técnicas que procuram garantir a segurança do dispositivo IoT (BNDES, 2017g).

Quadro 12 – Necessidades Tecnológicas – Saúde

Aplicação	Nome	Localização de ativos e pessoas nas unidades de saúde	Monitoramento de condições dos pacientes com diabetes	Diagnóstico descentralizado	Diagnóstico de sepse	Identificação e controle de epidemias	Necessidade
Conectividade	Redes *Low Power Wide Area*					✓	◔
	Redes cabeadas			✓			◔
	Redes de celular					✓	◔
	Redes de curto alcance e alta banda		✓	✓			◑
	Redes de curto alcance e baixa banda	✓	✓		✓		●
	Redes *mesh*						○
	Redes *Ultra Wideband*	✓					◔
Segurança da informação	Criptografia embarcada		✓	✓			◑
	Anti jamming						○
	Anti tampering						○
	Assinatura digital			✓			◔
	Blockchain			✓			◔
	Controle de acesso ao dispositivo						○
	Falha segura						○
	Firmware seguro						○
	Ingresso seguro à rede de acesso						○
	Prevenção a DDoS						○

Legenda para Necessidades: ● **Alta** ◑ **Média** ○ **Baixa.**

Fonte: Adaptado de BNDES, 2017g, v. 7B, p. 25.

O quadro 13 destacou as necessidades tecnológicas e suas capacidades para essa vertical considerando a Conectividade e a Segurança da Informação, respectivamente, e levantadas a partir de uma análise qualitativa. Esse quadro ressaltou como mais relevantes as redes de curto alcance, tanto para alta banda quanto para baixa banda, e avaliou que os atores locais nesse cenário têm capacidade tecnológica para desenvolvê-las. Já o cenário para os dispositivos salientou a relevância da criptografia embarcada, assinatura digital e *blockchain* como tecnologias de Segurança da Informação para as aplicações consideradas. Na avaliação, foi considerado que somente o desenvolvimento de assinaturas digitais tem atores de confiança (BNDES, 2017g).

Quadro 13 – Necessidades e Capacidades para Conectividade e Segurança – Saúde

	Tecnologias	**Necessidades [%]**				**Capacidades**		
		25	**50**	**75**	**100**			
Conectividade	Redes cabeadas	■					■	
	Redes celulares	■					■	
	Redes Low Power Wide Area – LPWA	■					■	
	Redes de curto alcance e alta banda	■	■					■
	Redes de curto alcance e baixa banda	■	■	■				■
	Redes Ultra-Wide Band – UWB	■						■
	Redes Mesh						■	
Segurança do dispositivo	Criptografia embarcada	■	■				■	
	Anti jamming						■	
	Anti tampering						■	
	Assinatura digital	■						■
	Blockchain	■					■	
	Controle de acesso ao dispositivo						■	
	Falha segura						■	
	Firmware seguro						■	
	Ingresso seguro à rede de acesso						■	
	Prevenção à negação de serviço						■	

Legenda para Capacidades – Status:

■ **- Confiança;**
■ **- Atenção;**
■ **- Dificuldade.**

Fonte: Adaptado de BNDES, 2017g, v. 7B, p. 27 e 29.

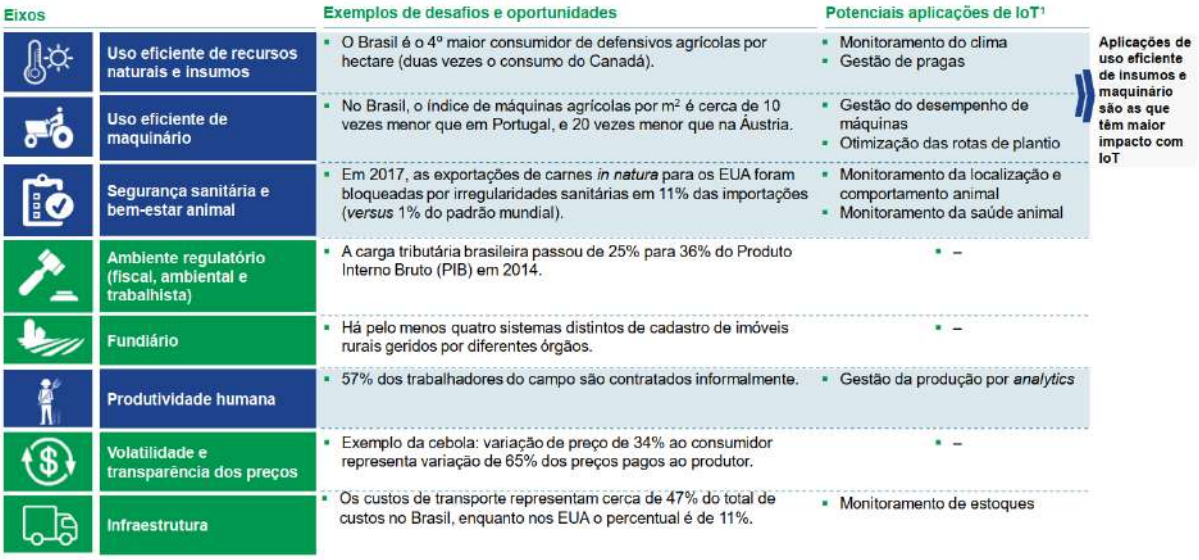
3.4.3 Meio Rural

Segundo o BNDES (2017h), as aplicações IoT no ambiente rural brasileiro produziriam ganhos de produtividade, redução de custos com insumos agrícolas e aumentariam a competitividade dos produtos brasileiros no mercado internacional. Alguns benefícios dessas aplicações foram destacados como, por exemplo, o acompanhamento das condições climáticas, do crescimento das plantações, do desempenho de máquinas agrícolas e da saúde dos animais. Algumas oportunidades também foram citadas na oferta de soluções IoT para climas tropicais a outros países semelhantes, mercado que já vem sendo explorado por *startups* brasileiras, e o melhor controle fitossanitário dos produtos agropecuários através de sistemas de rastreamento por IoT. O ganho econômico estimado para o Brasil pela implantação de aplicações IoT no campo seria entre US$ 5,5 a US$ 21,1 bilhões até 2025. Ressaltou-se que o Brasil é uma das principais fronteiras de crescimento agrícola, possuindo 69 milhões de hectares de terra utilizados na agricultura, 167,5 milhões de hectares na pecuária e 90 milhões de hectares seriam terras agriculturáveis inexploradas. Apesar de todo esse potencial, foram apontadas algumas barreiras estruturais para o desenvolvimento de IoT no campo:

a) Infraestrutura deficitária na logística e armazenagem que gera perdas e aumento de custos;
b) Baixa profissionalização da mão de obra dificultando a adoção de novas tecnologias;
c) Insegurança dos direitos fundiários que limita os investimentos no campo;
d) Descumprimento de normas sanitárias que limitam a expansão internacional;
e) Imprevisibilidade e falta de transparência sobre preços que pressiona as margens de lucro do setor;
f) Requisitos regulatórios complexos que dificultam a gestão;
g) Uso ineficiente de insumos acarretando baixa produtividade;
h) Falta de otimização do uso do maquinário agrícola que aumenta os custos operacionais (BNDES, 2017h).

Essas barreiras foram compiladas em oito eixos apresentados no quadro 14 (BNDES, 2017h).

Quadro 14 – Eixos estudados para aplicações IoT no ambiente rural



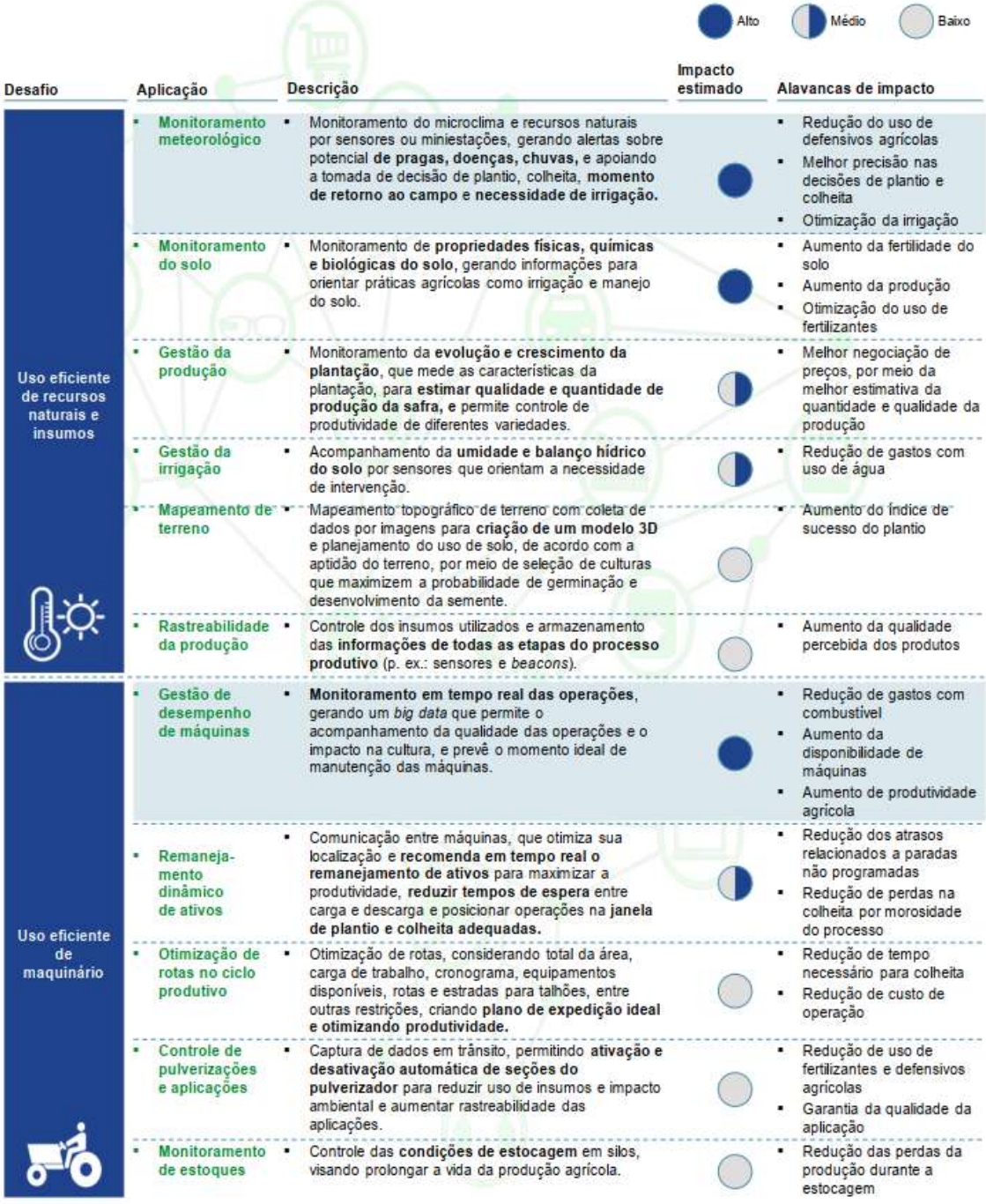
Eixos	Exemplos de desafios e oportunidades	Potenciais aplicações de IoT[1]
Uso eficiente de recursos naturais e insumos	▪ O Brasil é o 4º maior consumidor de defensivos agrícolas por hectare (duas vezes o consumo do Canadá).	▪ Monitoramento do clima ▪ Gestão de pragas
Uso eficiente de maquinário	▪ No Brasil, o índice de máquinas agrícolas por m² é cerca de 10 vezes menor que em Portugal, e 20 vezes menor que na Áustria.	▪ Gestão do desempenho de máquinas ▪ Otimização das rotas de plantio
Segurança sanitária e bem-estar animal	▪ Em 2017, as exportações de carnes *in natura* para os EUA foram bloqueadas por irregularidades sanitárias em 11% das importações (*versus* 1% do padrão mundial).	▪ Monitoramento da localização e comportamento animal ▪ Monitoramento da saúde animal
Ambiente regulatório (fiscal, ambiental e trabalhista)	▪ A carga tributária brasileira passou de 25% para 36% do Produto Interno Bruto (PIB) em 2014.	▪ –
Fundiário	▪ Há pelo menos quatro sistemas distintos de cadastro de imóveis rurais geridos por diferentes órgãos.	▪ –
Produtividade humana	▪ 57% dos trabalhadores do campo são contratados informalmente.	▪ Gestão da produção por *analytics*
Volatilidade e transparência dos preços	▪ Exemplo da cebola: variação de preço de 34% ao consumidor representa variação de 65% dos preços pagos ao produtor.	▪ –
Infraestrutura	▪ Os custos de transporte representam cerca de 47% do total de custos no Brasil, enquanto nos EUA o percentual é de 11%.	▪ Monitoramento de estoques

Aplicações de uso eficiente de insumos e maquinário são as que têm maior impacto com IoT

Fonte: BNDES, 2017h, v. 7C, p. 14.

Após considerações e discussão com especialistas da área, escolheu-se desenvolver quatro dos oito eixos listados. Dentro de cada um desses eixos, foram concebidas aplicações IoT que foram classificadas segundo impacto econômico potencial máximo e as facilidades de adoção. O resultado pôde ser observado no quadro 15 para os eixos Uso eficiente de recursos naturais e insumos e Uso eficiente de maquinário (BNDES, 2017h).

Quadro 15 – Aplicações IoT – Rural, eixos Eficiência em Recursos e Maquinário

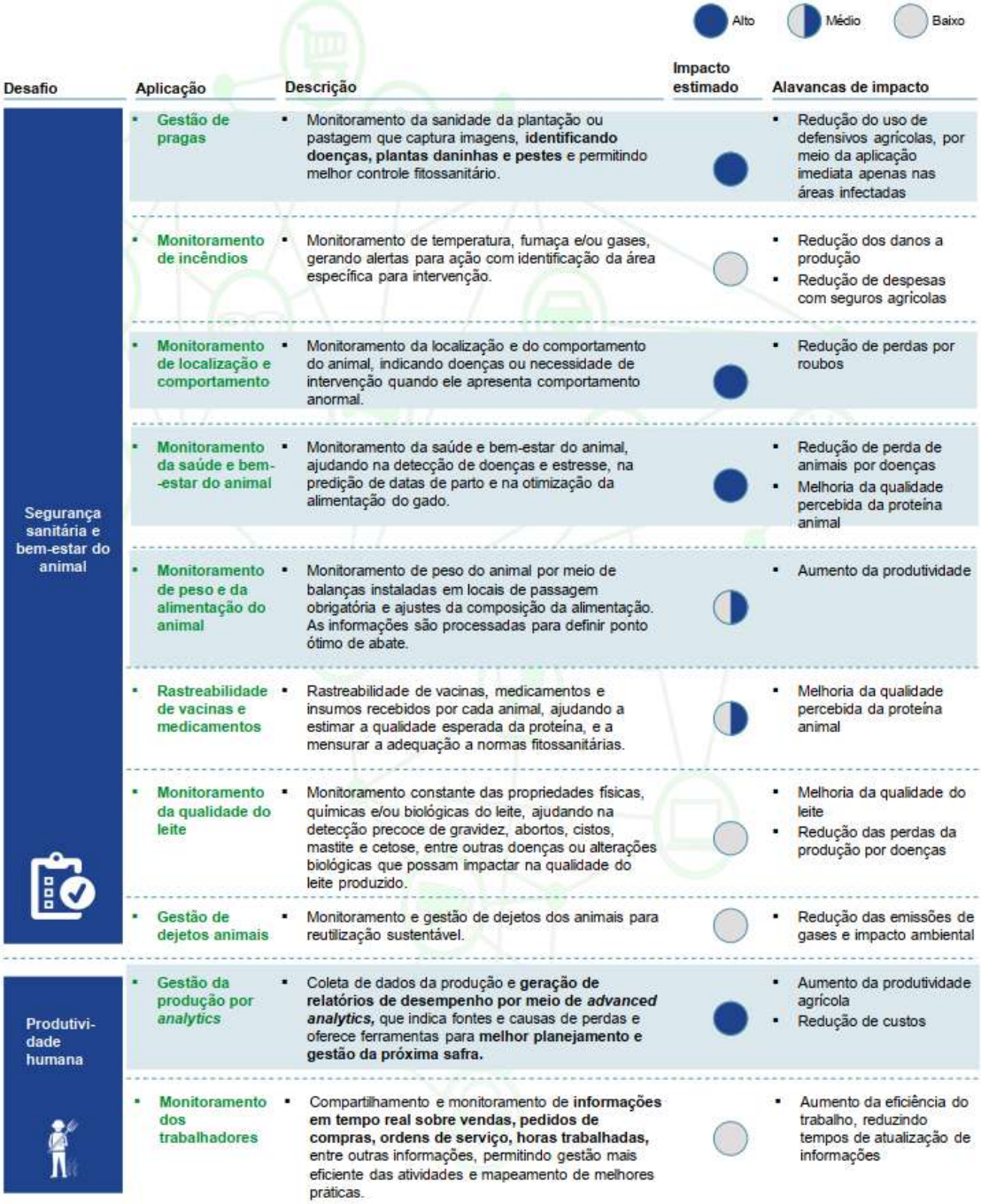


Desafio	Aplicação	Descrição	Impacto estimado	Alavancas de impacto
Uso eficiente de recursos naturais e insumos	Monitoramento meteorológico	Monitoramento do microclima e recursos naturais por sensores ou miniestações, gerando alertas sobre potencial **de pragas, doenças, chuvas,** e apoiando a tomada de decisão de plantio, colheita, **momento de retorno ao campo** e **necessidade de irrigação.**	Alto	Redução do uso de defensivos agrícolas Melhor precisão nas decisões de plantio e colheita Otimização da irrigação
	Monitoramento do solo	Monitoramento de **propriedades físicas, químicas e biológicas do solo**, gerando informações para orientar práticas agrícolas como irrigação e manejo do solo.	Alto	Aumento da fertilidade do solo Aumento da produção Otimização do uso de fertilizantes
	Gestão da produção	Monitoramento da **evolução e crescimento da plantação**, que mede as características da plantação, para **estimar qualidade e quantidade de produção da safra,** e permite controle de produtividade de diferentes variedades.	Médio	Melhor negociação de preços, por meio da melhor estimativa da quantidade e qualidade da produção
	Gestão da irrigação	Acompanhamento da **umidade e balanço hídrico do solo** por sensores que orientam a necessidade de intervenção.	Médio	Redução de gastos com uso de água
	Mapeamento de terreno	Mapeamento topográfico de terreno com coleta de dados por imagens para **criação de um modelo 3D** e planejamento do uso de solo, de acordo com a aptidão do terreno, por meio de seleção de culturas que maximizem a probabilidade de germinação e desenvolvimento da semente.	Baixo	Aumento do índice de sucesso do plantio
	Rastreabilidade da produção	Controle dos insumos utilizados e armazenamento das **informações de todas as etapas do processo produtivo** (p. ex.: sensores e *beacons*).	Baixo	Aumento da qualidade percebida dos produtos
Uso eficiente de maquinário	Gestão de desempenho de máquinas	**Monitoramento em tempo real das operações**, gerando um *big data* que permite o acompanhamento da qualidade das operações e o impacto na cultura, e prevê o momento ideal de manutenção das máquinas.	Alto	Redução de gastos com combustível Aumento da disponibilidade de máquinas Aumento de produtividade agrícola
	Remaneja-mento dinâmico de ativos	Comunicação entre máquinas, que otimiza sua localização e **recomenda em tempo real o remanejamento de ativos** para maximizar a produtividade, **reduzir tempos de espera** entre carga e descarga e posicionar operações na **janela de plantio e colheita adequadas.**	Médio	Redução dos atrasos relacionados a paradas não programadas Redução de perdas na colheita por morosidade do processo
	Otimização de rotas no ciclo produtivo	Otimização de rotas, considerando total da área, carga de trabalho, cronograma, equipamentos disponíveis, rotas e estradas para talhões, entre outras restrições, criando **plano de expedição ideal e otimizando produtividade.**	Baixo	Redução de tempo necessário para colheita Redução de custo de operação
	Controle de pulverizações e aplicações	Captura de dados em trânsito, permitindo **ativação e desativação automática de seções do pulverizador** para reduzir uso de insumos e impacto ambiental e aumentar rastreabilidade das aplicações.	Baixo	Redução de uso de fertilizantes e defensivos agrícolas Garantia da qualidade da aplicação
	Monitoramento de estoques	Controle das **condições de estocagem** em silos, visando prolongar a vida da produção agrícola.	Baixo	Redução das perdas da produção durante a estocagem

Fonte: BNDES, 2017h, v. 7C, p. 17.

Já o quadro 16 apresenta os resultados para os eixos Segurança Sanitária e Produtividade (BNDES, 2017h).

Quadro 16 – Aplicações IoT – Rural, eixos Segurança Sanitária e Produtividade



Fonte: BNDES, 2017h, v. 7C, p. 18.

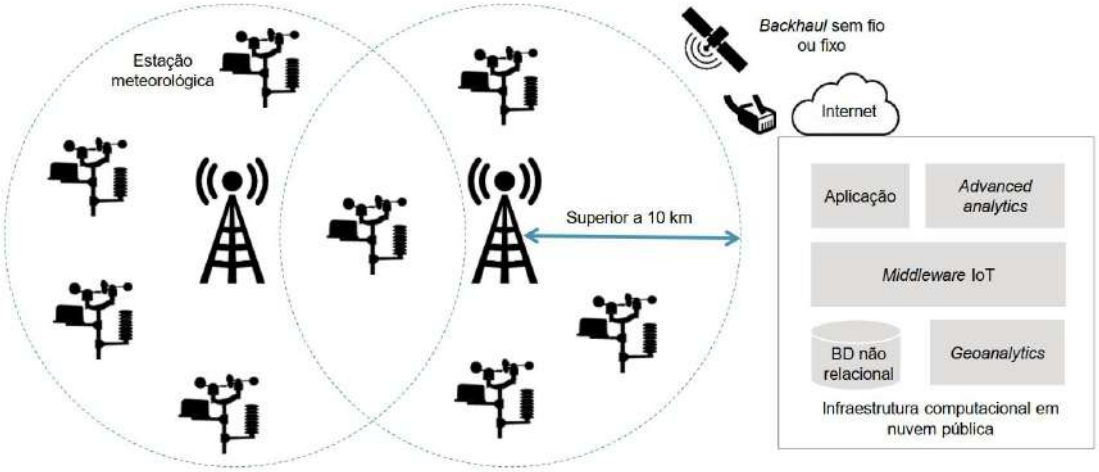
As análises resultaram no detalhamento de sete aplicações: monitoramento de microclima, no eixo uso eficiente de recursos naturais e insumos, gestão de pragas, monitoramento de localização e comportamento, monitoramento de peso e da alimentação do animal, monitoramento de saúde e bem-estar do animal, no eixo segurança sanitária e bem-estar do animal, gestão de desempenho de máquinas, no eixo uso eficiente de maquinário e gestão da

produção por *analytics*, no eixo produtividade humana. Essas aplicações foram examinadas a seguir focando na conectividade da proposta (BNDES, 2017h).

3.4.3.1 Monitoramento de microclima

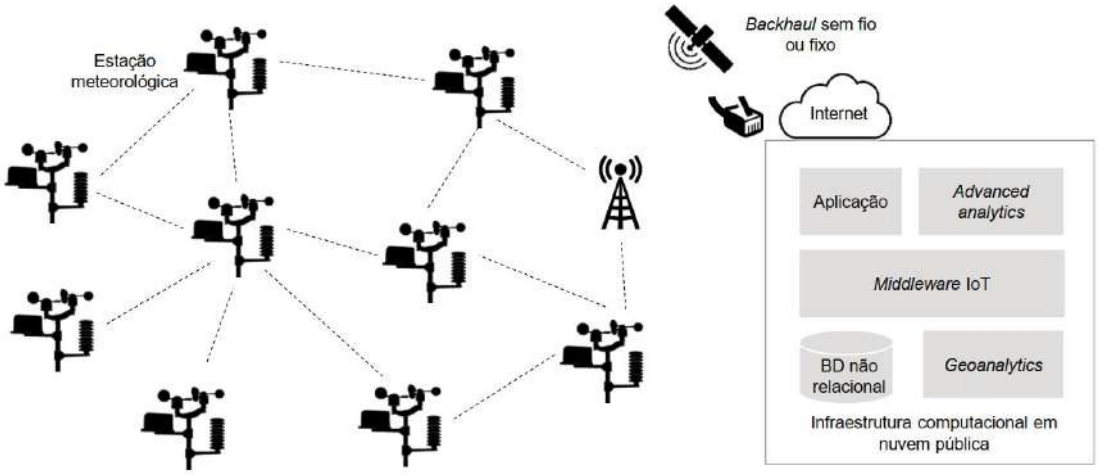
Considerou-se como proposta para monitoramento do microclima, a instalação de pequenas estações meteorológicas para medição de temperatura, pressão atmosférica e umidade e detecção de ventos e chuvas em microrregiões de aproximadamente 500 metros quadrados. Foram concebidas duas soluções: a primeira prevê a interconexão das estações meteorológicas a uma estação rádio base por rede LPWA, conforme figura 13, e a segunda solução, apresentada na figura 14, pressupõe que a própria estação meteorológica estabeleceria a uma rede tipo *mesh* para implementar a interconexão. Os dados coletados seriam transportados até uma infraestrutura computacional para tratamento que subsidiaria a tomada de decisões relacionadas a irrigação, colheita, controle de pragas e doenças, o que poderia resultar em ganhos na produtividade (BNDES, 2017h).

Figura 13 – Monitoramento de microclima – solução 1



Fonte: BNDES, 2017h, v. 7C, p. 43.

Figura 14 – Monitoramento de microclima – solução 2



Fonte: BNDES, 2017h, v. 7C, p. 43.

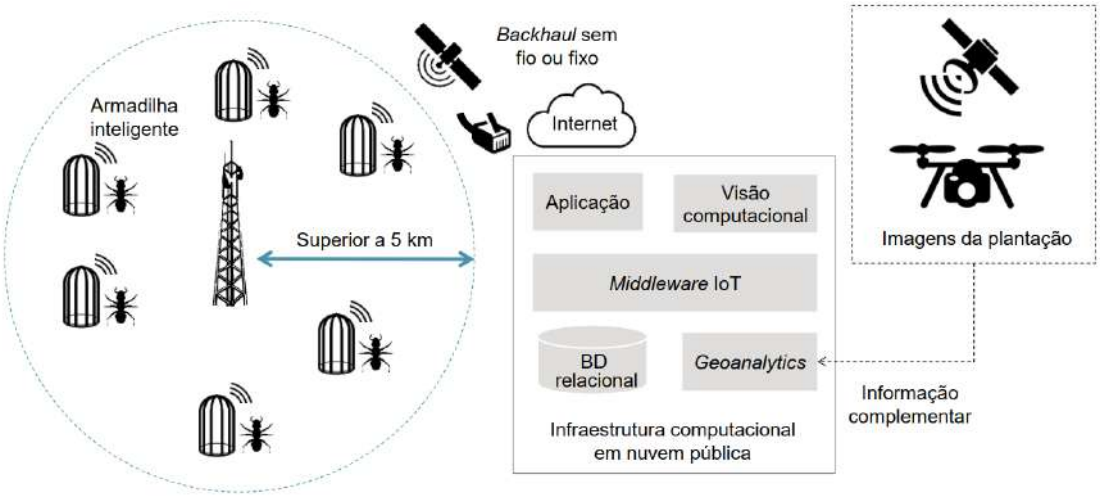
Devido a dispersão geográfica dos atendimentos, as soluções de conectividade deveriam permitir atingir áreas extensas. Na solução 1, as estações rádio base necessitariam de energia elétrica e *backhaul* para conexão com a nuvem via rede cabeada (por cobre ou fibra óptica) ou por rede wireless (via *link* de rádio ou satélite). Essa necessidade também se faz presente na solução 2, mas restrita a poucos elementos da rede que fariam a conexão com a Internet (BNDES, 2017h).

3.4.3.2 Gestão de pragas

Essa aplicação se baseou no envio de imagens de insetos capturadas em pontos da plantação por ‘armadilhas’ inteligentes para permitir sua identificação e tomada de decisão quanto a ações de tratamento de pragas, caso o inseto seja assim considerado. Essa solução foi apresentada na figura 15. Para a correta identificação dos insetos, seria necessário a captura de imagens em alta definição, o que implicaria em arquivos grandes e resultaria na implementação de uma rede capaz de lidar com esse tipo de tráfego (BNDES, 2017h).

Essa solução também exigiria conectividade de área ampla que poderia ser viabilizada por poucas estações rádio base utilizando tecnologia celular IoT (LTE-M) e que seriam dotadas de infraestrutura de energia elétrica e conexão com rede cabeada ou por satélite (BNDES, 2017h).

Figura 15 – Gestão de pragas

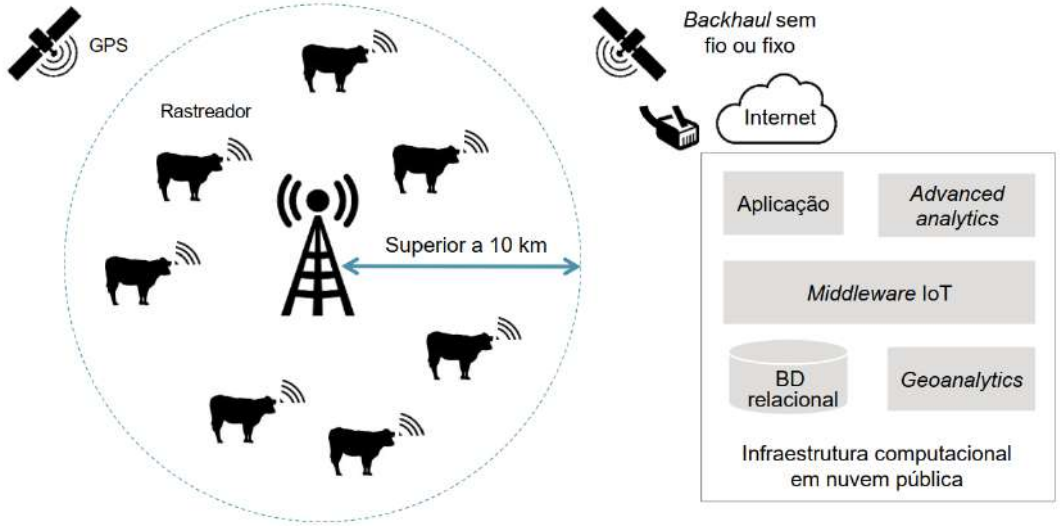


Fonte: BNDES, 2017h, v. 7C, p. 47.

3.4.3.3 Monitoramento de localização e comportamento

Essa aplicação, exibida na figura 16, viabilizaria a localização do gado e identificação de comportamento anormal que pudesse indicar doenças e necessidade de intervenção através de rastreamento periódico do rebanho por módulos GPS. Os dados de localização adquiridos pelos módulos GPS seriam coletados por estações rádio base utilizando a tecnologia LPWA (BNDES, 2017h).

Figura 16 – Monitoramento de localização e comportamento



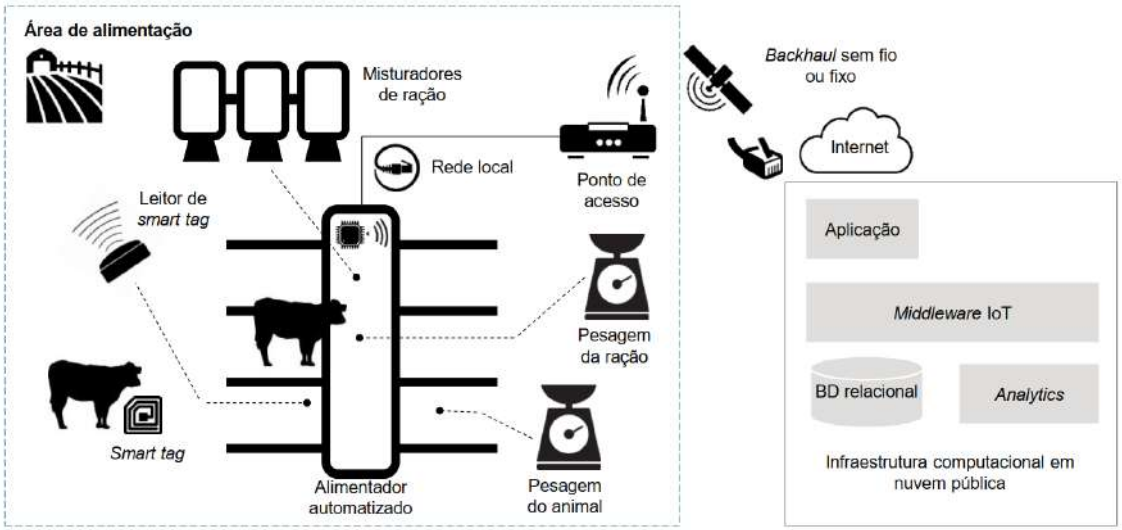
Fonte: BNDES, 2017h, v. 7C, p. 50.

A conectividade de área ampla exigida por essa aplicação e provida pela rede LPWA demandaria poucas estações rádio base que precisariam ser conectadas a infraestrutura computacional por *backhaul* cabeado ou por satélite. Aqui também seria necessária infraestrutura de energia elétrica além da conexão à Internet. A rede precisaria lidar com grande quantidade de pacotes de dados, porém, de tamanho pequeno (BNDES, 2017h).

3.4.3.4 Monitoramento do peso e alimentação do animal

A solução proposta, descrita na figura 17, considerou a instalação de balanças para o gado nos locais de alimentação e também no comedouro dos animais que estariam portando *smart tags* (RFID) para sua identificação. Isso possibilitaria avaliar o peso, quantidade de alimento consumido e necessidades de alimentação de cada animal. Essas necessidades seriam supridas pela mistura da ração mais adequada para o desenvolvimento do gado. A pesagem se faria de forma natural e contínua indicando precisamente o ponto de abate (BNDES, 2017h).

Figura 17 – Monitoramento de peso e alimentação do animal



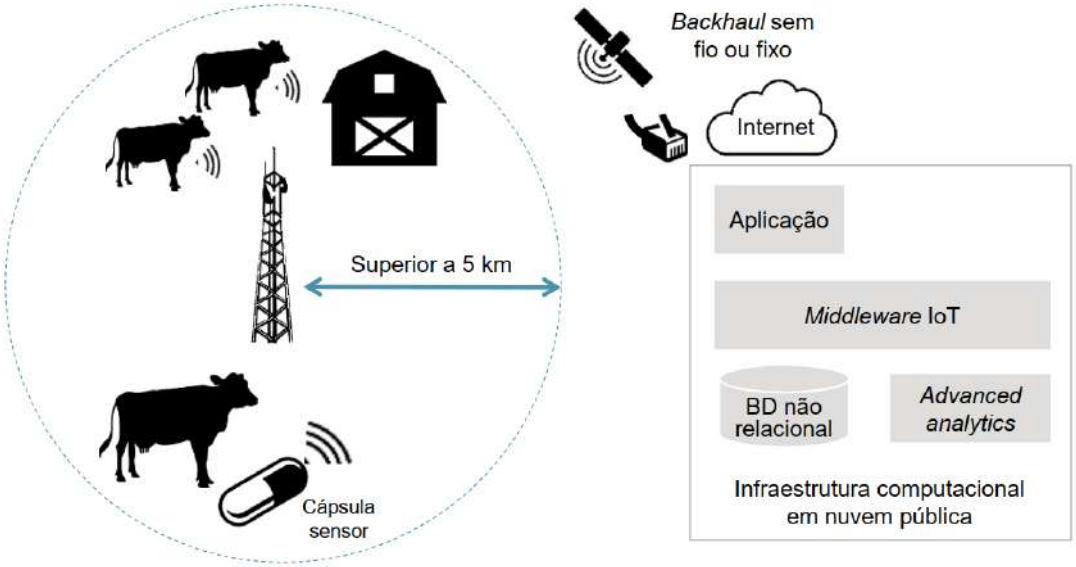
Fonte: BNDES, 2017h, v. 7C, p. 55.

A iteração com os misturadores de ração exigiria infraestrutura que opere em tempo real o que conduziria à implantação de redes locais de alta banda (Wi-Fi) ou rede cabeada (Ethernet) com *backhaul* por cabo ou satélite (BNDES, 2017h).

3.4.3.5 Gestão da saúde do animal

O monitoramento periódico de indicadores de saúde, previsto nessa aplicação e indicado na figura 18, seria viabilizado pela implantação de cápsulas transmissoras no rúmen do animal. Essas cápsulas captariam dados de temperatura corporal e pH do meio e que, após processamento, permitiriam a detecção de doenças, estresse, predição de datas de parto e otimização da alimentação do gado (BNDES, 2017h).

Figura 18 – Gestão da saúde do animal



Fonte: BNDES, 2017h, v. 7C, p. 53.

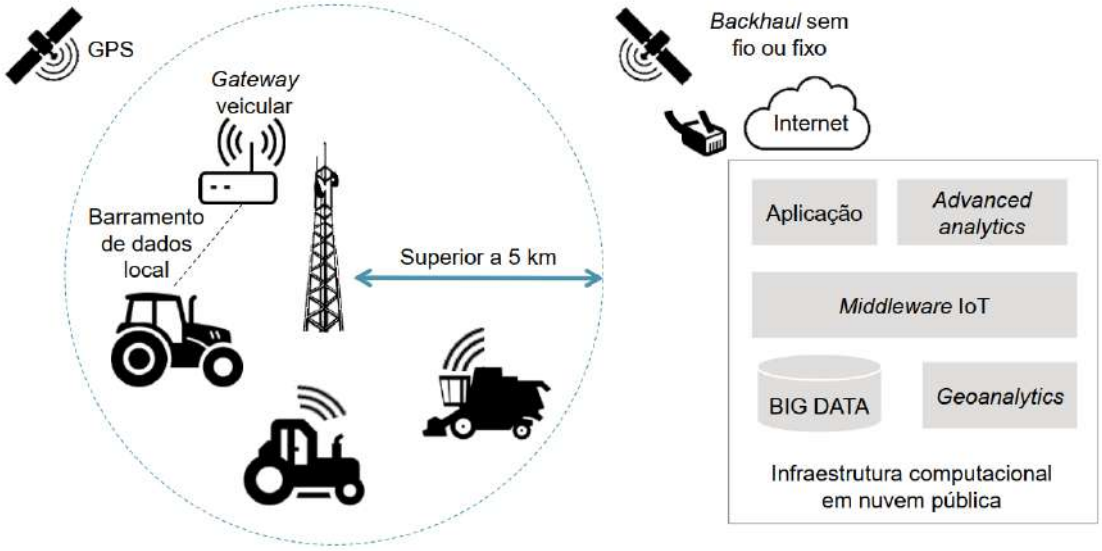
Essa aplicação também exigiria conectividade de área ampla provida por rede LPWA. Seriam necessárias poucas estações rádio base conectadas a infraestrutura computacional por *backhaul* cabeado ou por satélite, além de provimento de energia elétrica para as estações. Novamente, a rede precisaria lidar com grande quantidade de pacotes de dados de tamanho pequeno (BNDES, 2017h).

3.4.3.6 Gestão de desempenho de máquinas

Essa aplicação compreenderia o monitoramento em tempo real de máquinas agrícolas gerando grande volume de dados sobre seu regime de funcionamento, subsidiando a manutenção

preditiva de quebras e promovendo redução com gastos de combustíveis através da definição dinâmica de rotas. Os sensores instalados no maquinário capturariam dados de velocidade, produtividade, consumo de combustível e desgaste de peças. Essa aplicação está esquematizada na figura 19 (BNDES, 2017h).

Figura 19 – Gestão de desempenho de máquinas



Fonte: BNDES, 2017h, v. 7C, p. 58.

A conectividade necessária a essa solução utilizaria *gateways* veiculares conectados à rede celular IoT (LTE-M) capazes de atender ao grande volume de dados esperado e dar suporte em tempo real à aplicação. O *backhaul* se faria por rede cabeada ou satélite (BNDES, 2017h).

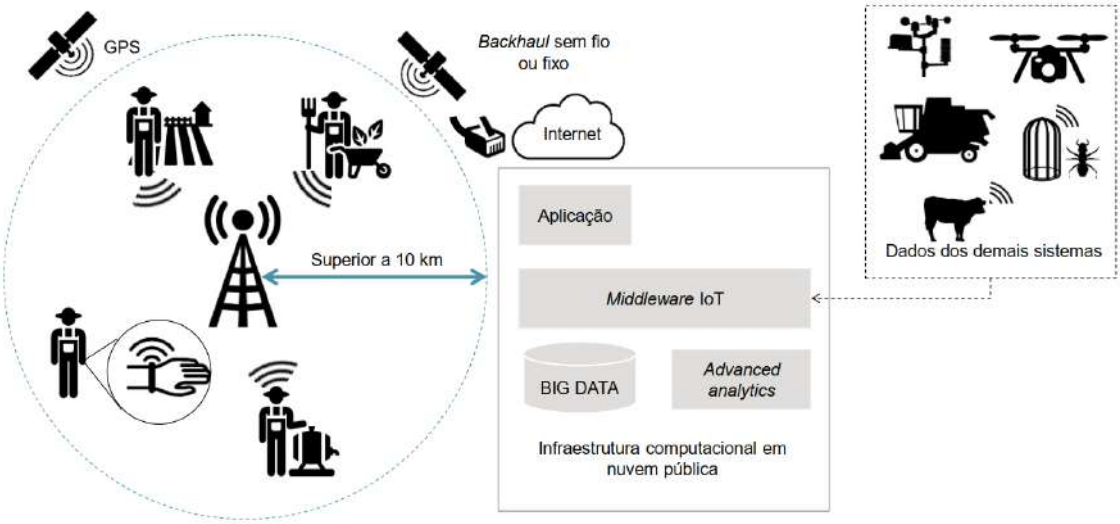
3.4.3.7 Produtividade dos trabalhos por analytics

Para a melhoria geral da produtividade no campo, o BNDES (2017h) colocou como necessário o monitoramento da força de trabalho em conjunto com as outras aplicações IoT previstas. A solução concebida para tal, e apresentada na figura 20, se apoiou em dispositivos vestíveis (*wearables*) que recolheriam dados de localização por GPS dos trabalhadores e os enviariam para processamento em aplicações na nuvem por rede *wireless*.

O baixo tráfego, a tolerância ao atraso no envio de dados e sua eventual perda e a extensa área a ser coberta conduziu à necessidade de poucas estações rádio base apoiadas em tecnologia

LPWA e interligadas por *backhaul* por cabo ou via satélite. Seria esperado grande quantidade de dispositivos, mas gerando poucos dados (BNDES, 2017h).

Figura 20 – Produtividade dos trabalhos por analytics



Fonte: BNDES, 2017h, v. 7C, p. 43.

3.4.3.8 Necessidades e capacidades

As possíveis soluções para as aplicações IoT foram analisadas pelo grau de relevância de cada tecnologia utilizada na solução procurando avaliar suas necessidades essenciais. O quadro 17 apresentou essas necessidades por tecnologia para Conectividade e Segurança da Informação. A Segurança da Informação nesse quadro estaria relacionada às técnicas que procuram garantir a segurança do dispositivo IoT (BNDES, 2017h).

Quadro 17 – Necessidades Tecnológicas – Rural

Aplicação	Nome	Monitoramento de microclima	Gestão de pragas	Monitoramento de localização e comportamento	Monitoramento do peso e alimentação do animal	Gestão da saúde do animal	Gestão de desempenho de máquinas	Produtividade dos trabalhos por *analytics*	Necessidade
Conectividade	▪ Redes *Low Power Wide Area*	✓		✓		✓		✓	◑
	▪ Redes cabeadas				✓				◔
	▪ Redes de celular		✓				✓		◔
	▪ Redes de curto alcance e alta banda				✓				◔
	▪ Redes de curto alcance e baixa banda								○
	▪ Redes *mesh*	✓							◔
	▪ Redes *Ultra Wideband*								○
Segurança da informação	▪ Criptografia embarcada								○
	▪ *Anti jamming*								○
	▪ *Anti tampering*								○
	▪ Assinatura digital								○
	▪ *Blockchain*								○
	▪ Controle de acesso ao dispositivo				✓				◔
	▪ Falha segura				✓				◔
	▪ *Firmware* seguro				✓				◔
	▪ Ingresso seguro à rede de acesso								○
	▪ Prevenção a DDoS								○

Legenda para Necessidades: ● **Alta** ◑ **Média** ○ **Baixa.**

Fonte: Adaptado de BNDES, 2017h, v. 7C, p. 23.

O quadro 18 levantou, a partir de uma análise qualitativa, as necessidades tecnológicas utilizadas nas propostas para a vertical Meio Rural e a respectiva capacidade dos atores locais de provê-las, considerando somente a Conectividade e Segurança da Informação necessárias. Destacou-se como mais relevante a tecnologia LPWA para Conectividade e mostrou-se que pouco mais de 70% dos atores (cinco em sete atores) teriam facilidade para atendê-las. Quanto à Segurança, percebeu-se que a necessidades não são tão relevantes, mas a capacidade local seria suficiente para a maioria das tecnologias com atenção para a tecnologia *firmware* seguro em que há carência na competência dos atores para seu desenvolvimento (BNDES, 2017h).

Quadro 18 – Necessidades e Capacidades para Conectividade e Segurança – Rural

	Tecnologias	Necessidades [%]				Capacidades		
		25	50	75	100			
Conectividade	Redes cabeadas	■						■
	Redes celulares	■					■	
	Redes Low Power Wide Area – LPWA	■	■				■	
	Redes de curto alcance e alta banda	■						■
	Redes de curto alcance e baixa banda							■
	Redes Ultra-Wide Band – UWB							■
	Redes Mesh	■						■
Segurança do dispositivo	Criptografia embarcada						■	
	Anti jamming						■	
	Anti tampering						■	
	Assinatura digital						■	
	Blockchain						■	
	Controle de acesso ao dispositivo	■					■	
	Falha segura	■					■	
	Firmware seguro	■				■		
	Ingresso seguro à rede de acesso						■	
	Prevenção à negação de serviço						■	

Legenda para Capacidades – Status:

■ **- Confiança;**

■ **- Atenção;**

■ **- Dificuldade.**

Fonte: Adaptado de BNDES, 2017h, v. 7C, p. 25 e 27.

3.4.4 Indústria

O volume 7D do estudo do BNDES abordou a implantação de soluções de IoT para a indústria. Foram identificados dois ambientes nesse setor: Fábricas/Manufatura, e Indústrias de Base/Processos. Esses ambientes foram agrupados numa ‘Frente Mobilizadora de Indústrias’ com o objetivo de “impulsionar iniciativas relacionadas com manufatura avançada, lideradas por outros órgãos, associações e confederações”. Foi destacado o impacto positivo que ações no setor industrial podem trazer para os demais setores da economia pela transmissão de ganhos de produtividade sistêmicos e por servir de referência para esses setores. Dentro dos dois ambientes selecionados, foram identificados dois setores por grupo:

a) Indústrias de base:
   - Exploração e produção de petróleo e gás natural;
   - Mineração.

b) Fábricas:
    - Setor automotivo;
    - Setor Têxtil (BNDES, 2017i).

Um dos principais clientes de tecnologia, o setor automotivo apresentou forte expansão nos últimos anos no Brasil. Entretanto, apesar de incentivos governamentais que ampliaram o número de fábricas de 53 em 2011 para 65 em 2015, o setor foi atingido pela crise que sentenciou uma ociosidade de 50% para o setor em 2016. Com uma cadeia produtiva pulverizada em empresas de menor porte, o setor têxtil enfrentou uma concorrência acirrada dos países asiáticos, mas manteve sua importância com uma expectativa de comercialização de 5,4 bilhões de peças e faturamento de US$ 37 bilhões para 2017. O setor de petróleo e gás, com uma cadeia produtiva robusta e empresas de grande porte, também tem enfrentado problemas com a queda de preços internacionais e a retração do seu mercado. A mineração, setor já considerado maduro e competitivo, também sofreu com a desaceleração da China que provocou a diminuição de preços das *commodities*. Esses desafios colocaram as empresas em busca de soluções para aumentar a eficiência nos processos garantindo viabilidade e crescimento. Esse seria o cenário para a implantação de soluções IoT nessa vertical (BNDES, 2017i).

Foram identificados quatro pilares que embasariam avanços tecnológicos na indústria:

a) Interconexão de objetos e pessoas que permitiriam reduzir custos de computação, armazenamento, sensores e hardware;
b) Novos métodos analíticos, com foco descritivo, preditivo e prescritivo, que maximizariam o valor do grande volume de dados do setor;
c) Eliminação da necessidade de intervenção humana através da robótica e automação;
d) Digitalização de processos de negócio.

Os dois primeiros foram foco desse estudo em propostas de Conectividade e Detecção, e *Advanced Analytics*. O primeiro permitiria maior controle do processo produtivo em geral e tem se acelerado devido ao barateamento dos custos dos insumos para essas soluções. Já o segundo pilar se beneficiaria dos avanços em *machine learning* e *Big Data* possibilitando análises mais profundas de dados históricos dos processos de modo a identificar padrões e correlações que poderiam otimizar os processos e impulsionar os ganhos em produtividade (BNDES, 2017i).

Após essas análises, oito grupos de desafios foram selecionados, todos relacionados ao aumento de produtividade e a incorporação de elementos inovadores na produção. O quadro 19 descreve esses desafios e indicou maior impacto de técnicas IoT nos seis primeiros (BNDES, 2017i).

Quadro 19 – Eixos estudados para aplicações IoT no ambiente da indústria

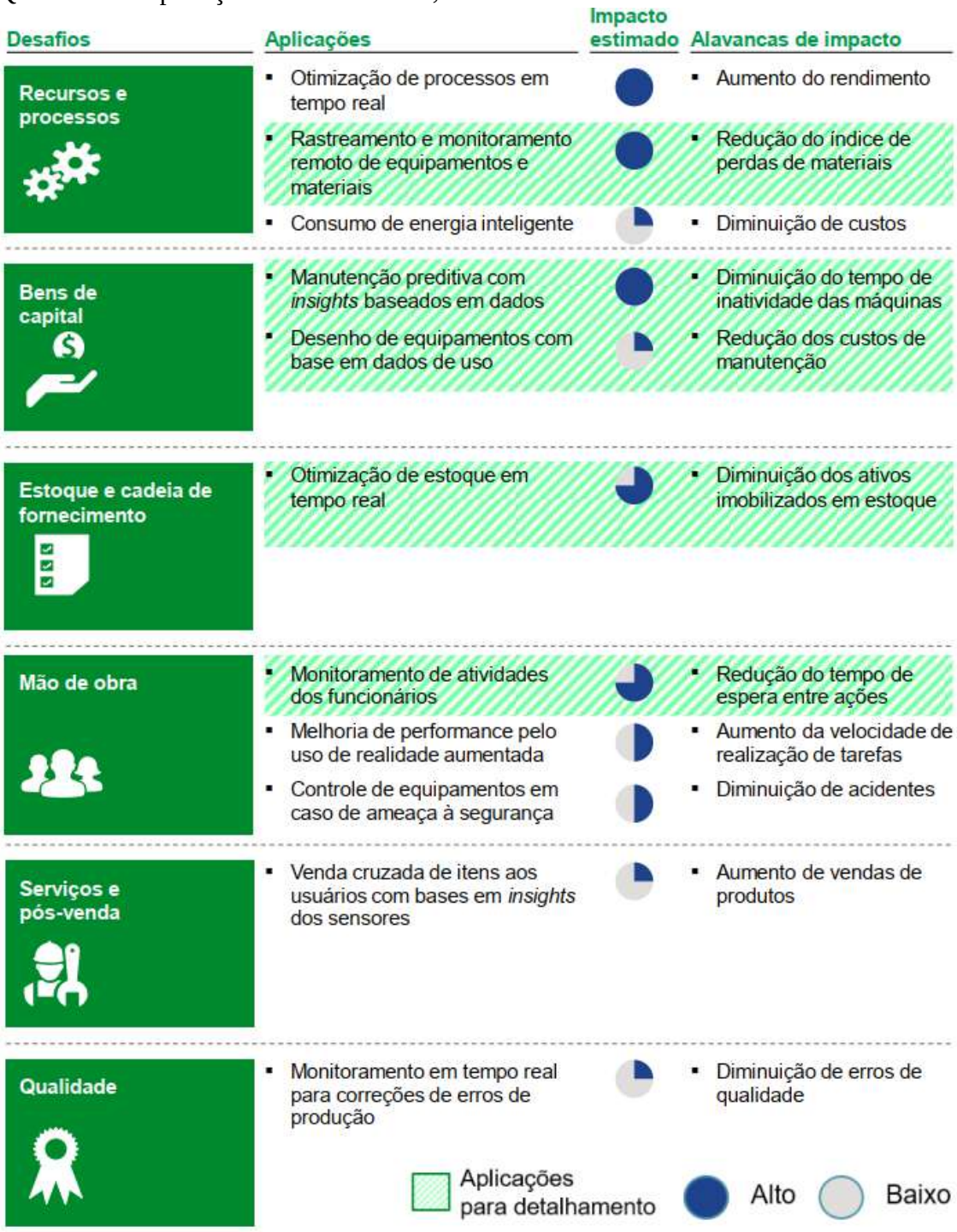
Desafios	Descrição
Recursos e processos	▪ Melhorar processos em termos de consumo de material, velocidade de execução ou rendimento ▪ Aperfeiçoar o desenho dos processos com o uso intensivo de tecnologia
Bens de capital	▪ Incrementar o uso de ativos, diminuindo o tempo de inatividade ▪ Aperfeiçoar o desenho da nova geração de ativos
Estoque e cadeia de fornecimento	▪ Reduzir excesso de estoque para diminuir capital imobilizado ▪ Melhorar a integração entre diferentes elos da cadeia de fornecimento
Mão de obra	▪ Reduzir tempo de espera dos trabalhadores ▪ Aumentar a velocidade das operações ▪ Mudar a forma como escritórios de projetos de engenharia trabalham para incorporar tecnologia de forma mais ampla
Serviços e pós-venda	▪ Criar novos modelos de negócios baseados em serviços ▪ Ofertar soluções para diminuir custos com serviços e tempo de inatividade de maquinas
Qualidade	▪ Melhorar a qualidade dos produtos ▪ Eliminar falhas durante o processo de criação de valor
Adequação de oferta	▪ Otimizar a correspondência de oferta de produtos com base no que os consumidores realmente valorizam e querem comprar
Tempo para mercado	▪ Levar novos produtos para o mercado em menos tempo

Maior impacto de IoT
Menor impacto de IoT

Fonte: BNDES, 2017i, v. 7D, p. 16.

O quadro 20 apresenta o resultado do estudo de aplicações IoT que poderiam solucionar esses seis desafios, indicando aquelas que seriam detalhadas (BNDES, 2017i).

Quadro 20 – Aplicações IoT – Indústria, todos os eixos



Fonte: BNDES, 2017i, v. 7D, p. 17.

Esse detalhamento foi realizado com base em quatro critérios: transbordamento para outros setores, rapidez de adoção, expectativa de adoção a longo prazo e captura de valor esperada. Essa análise culminou na escolha de seis aplicações:

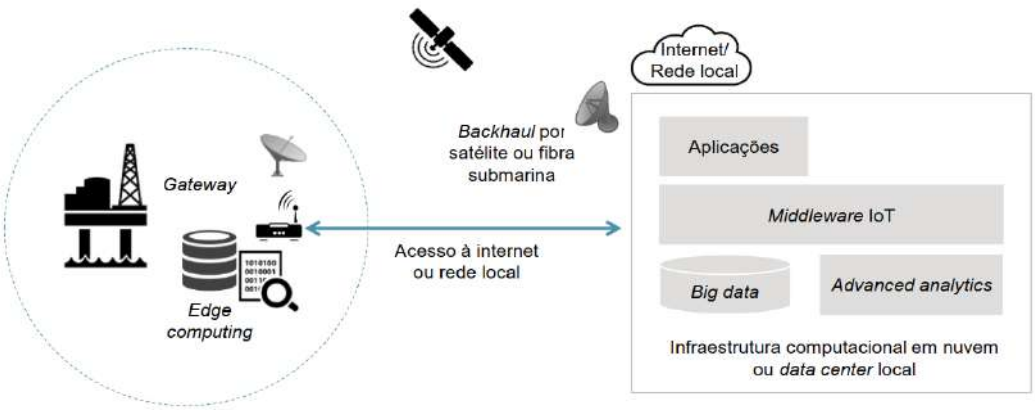
a) Manutenção preditiva de plataformas offshore;
b) Monitoramento de barragens;
c) Monitoramento de ativos de mineração;
d) Otimização de estoque em tempo real;
e) Redesenho de plantas baseado em atividades;
f) Desenho de equipamentos baseado em dados de uso.

Essas aplicações foram exploradas a seguir, focando na conectividade necessária (BNDES, 2017i).

3.4.4.1 Manutenção preditiva de plataformas offshore

Essa solução, apresentada na figura 21, consistiu em um sistema de captura de dados de sensores em tempo real, de ativos críticos a operação das plataformas offshore. Os dados seriam enviados a uma infraestrutura computacional que, por meio de algoritmos preditivos e de inteligência artificial, faria a análise das condições do maquinário indicando a necessidade de parada para manutenção (manutenção preditiva). Essa solução traz como benefícios o aumento da eficiência operacional da plataforma, a diminuição do tempo de inatividade das máquinas e a redução dos custos de manutenção (BNDES, 2017i).

Figura 21 – Manutenção preditiva de plataformas offshore



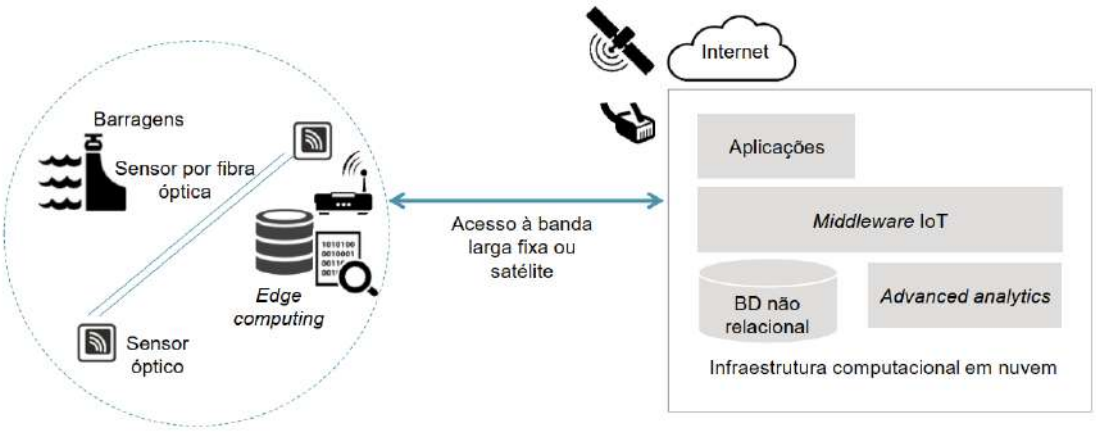
Fonte: BNDES, 2017i, v. 7D, p. 45.

A conectividade da solução se faria por redes cabeadas ou *wireless* de alta banda para aquisição dos dados das máquinas e que seriam conectados a um *gateway* para conexão com a infraestrutura computacional remota via satélite ou por cabo de fibras ópticas submarino (BNDES, 2017i).

3.4.4.2 Monitoramento de barragens

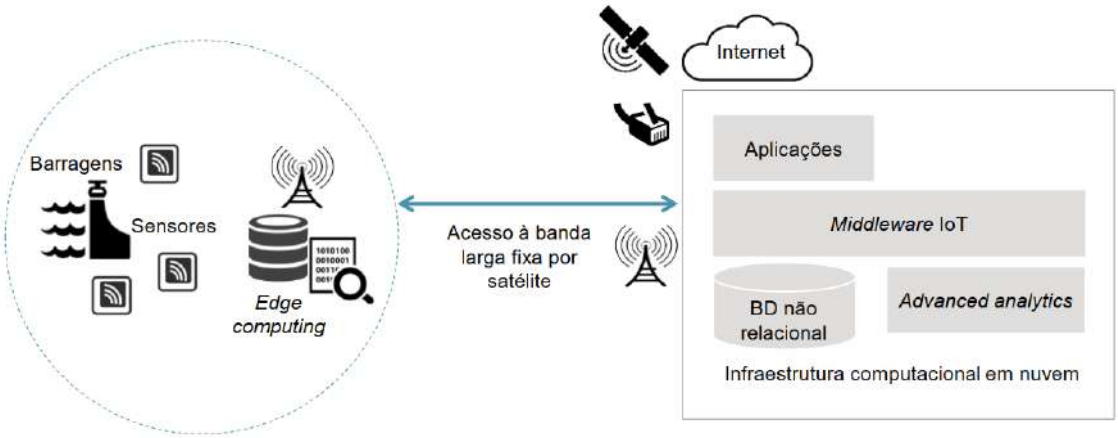
Foi considerada uma aplicação IoT para o monitoramento de barragens, problema tão sensível pelas questões ambientais e de segurança pública envolvidas. Previu-se a instalação de sensores que fariam a medição em tempo real do deslocamento ou deformação de juntas nas barragens bem como dilatação de trincas e fissuras, recalque de estruturas, nível e pressão de água e vazão da infiltração. Foram concebidas duas soluções, apresentadas nas figuras 22 e 23. Na solução 1, sensores ópticos fariam a medição por meio de variação na refração da luz em fibras ópticas instaladas em pontos de interesse. Já a solução 2, o sensoriamento se faria por sensores piezoelétricos, eletrostáticos ou eletromagnéticos. Os benefícios esperados seriam a diminuição do impacto ambiental, mitigação do risco de perda de vidas e redução de perdas associadas a moradias e equipamentos no caso de acidentes (BNDES, 2017i).

Figura 22 – Monitoramento de barragens – solução 1



Fonte: BNDES, 2017i, v. 7D, p. 48.

Figura 23 – Monitoramento de barragens – solução 2



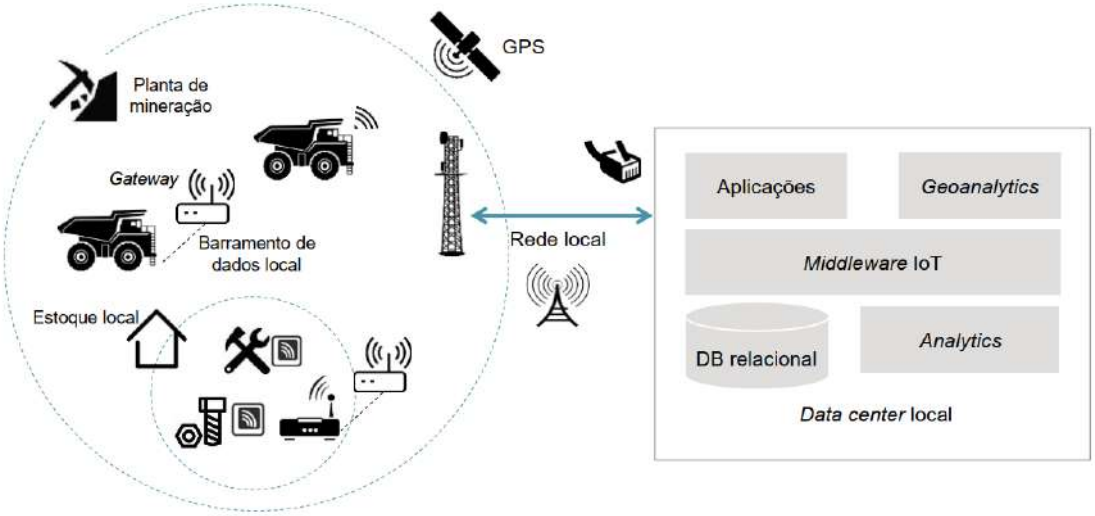
Fonte: BNDES, 2017i, v. 7D, p. 49.

Na solução 1, por fibra óptica, a conectividade se faria por rede cabeada. Já na solução 2, a interligação se faria através de rede sem fio de área ampla (LPWA). Nesse último caso, poderia ser necessário levar infraestrutura de energia e *backhaul* até as estações rádio base. Em ambas as soluções, um *gateway* faria a concentração dos dados para envio à rede local ou à nuvem por satélite ou acesso fixo a banda larga (BNDES, 2017i).

3.4.4.3 Monitoramento de ativos de mineração

A solução considerada, apresentada na figura 24, previu o monitoramento da localização de veículos em plantas de mineração, suas condições e o controle do estoque de peças visando otimizar a operação. Para esse monitoramento, foi considerada instalação de *gateways* veiculares para acompanhamento em tempo real das condições de uso da frota e *smart tags* em peças e equipamentos para auxílio a manutenção. Os dados seriam capturados por redes sem fio e enviados a aplicações em nuvem para suporte a tomada de decisão (BNDES, 2017i).

Figura 24 – Monitoramento de ativos de mineração



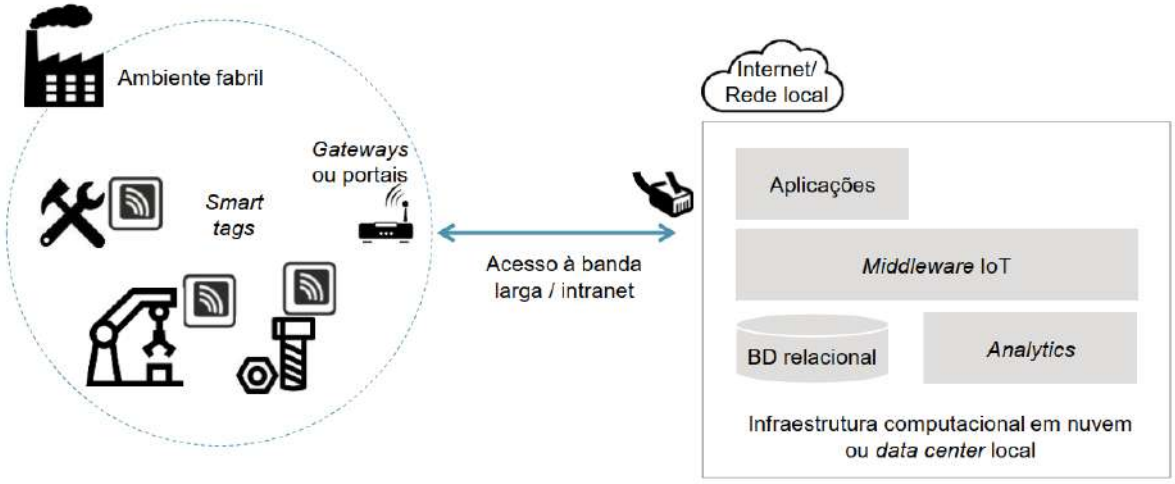
Fonte: BNDES, 2017i, v. 7D, p. 53.

Para conectividade com os *gateways* veiculares, seriam instaladas estações rádio base que viabilizariam o acesso de área ampla e alta banda como em redes celulares LTE-M. Já para os smart tags, a conectividade se faria por leitores de RFID de curto alcance e baixa banda. O *backhaul* se faria por rede cabeada (Ethernet, GPON, ADSL) (BNDES, 2017i).

3.4.4.4 Gestão de estoque

A gestão de estoque através do rastreamento por tecnologia IoT no ambiente fabril traria muitos benefícios como a diminuição de ativos imobilizados no estoque, melhor uso dos insumos a disposição e prevenção de roubos e fraudes. A solução concebida na figura 25 faria o monitoramento em tempo real de ativos utilizando *smart tags* RFID. Nos casos em que há necessidade de precisão na localização do bem poderiam ser utilizadas RFID ativas, pontos de acesso *Bluetooth* ou redes UWB (BNDES, 2017i).

Figura 25 – Gestão de estoque



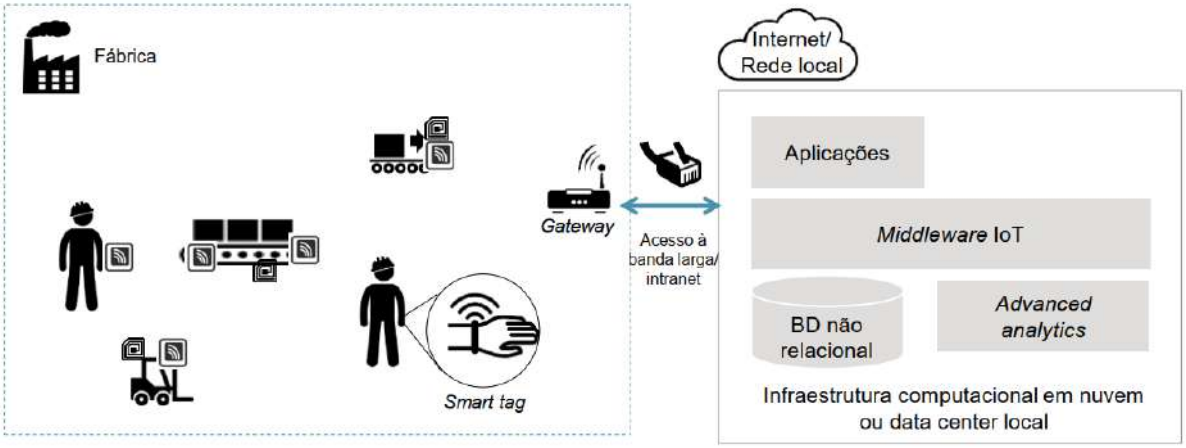
Fonte: BNDES, 2017i, v. 7D, p. 41.

A conectividade com as etiquetas se faria por redes de curto alcance e baixa banda (leitores RFID) e redes *Ultra-Wide Band* – UWB para precisão na localização. Já a conexão com a infraestrutura computacional que daria suporte à aplicação se faria por rede LAN – *Local Area Network* (BNDES, 2017i).

3.4.4.5 Integração da planta produtiva

Para melhorar a eficiência dos processos produtivos, essa aplicação, apresentada na figura 26, propôs o monitoramento de máquinas e funcionários com a utilização de *smart tags e wearables*, respectivamente. Os dados coletados seriam enviados a aplicações em nuvem que os confrontariam com dados de outros sistemas visando otimizar os processos fabris (BNDES, 2017i).

Figura 26 – Integração da planta produtiva



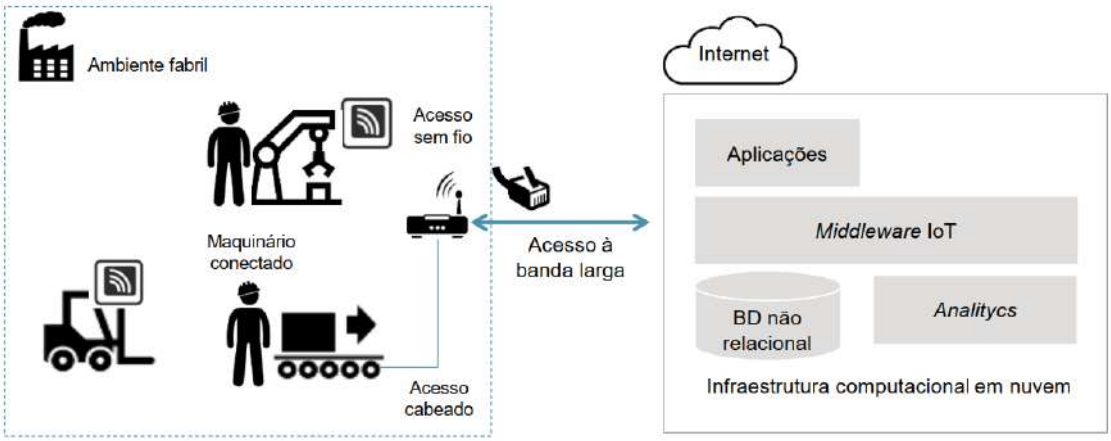
Fonte: BNDES, 2017i, v. 7D, p. 58.

A conectividade da aplicação se faria por rede cabeada ou redes de curto alcance, baixa e alta banda para conexão com os *smart tags e wearables*, e coletada por leitores RFID. Novamente, se for necessária precisão na localização poderiam ser usados *beacons* BLE. A conexão com a nuvem que proveria o suporte à aplicação se faria por rede LAN – *Local Area Network* (BNDES, 2017i).

3.4.4.6 Engenharia de produtos baseada em dados de sensores

No contexto dessa solução, esquematizada na figura 27, somente algumas máquinas e equipamentos seriam monitorados visando levantar dados sobre a forma como seriam utilizados, se todas as suas funcionalidades estariam sendo empregadas e se existiria alguma funcionalidade ausente, mas necessária. A solução capturaria dados do *log* da interface homem máquina – IHM dos equipamentos que seriam enviados para aplicações em nuvem que permitiriam ao fabricante das máquinas e equipamentos aperfeiçoarem seus produtos (BNDES, 2017i).

Figura 27 – Engenharia de produtos baseada em dados de sensores



Fonte: BNDES, 2017i, v. 7D, p. 56.

A conectividade se faria por acesso cabeado (Ethernet) ou sem fio de curto alcance e alta banda (Wi-Fi) para as máquinas e equipamentos e rede cabeada banda larga para conexão com aplicações dos fabricantes dos equipamentos na nuvem (BNDES, 2017i).

3.4.4.7 Necessidades e capacidades

O quadro 24 apresentou as necessidades para atender essa vertical considerando somente os aspectos de Conectividade e Segurança da Informação destacando-se o grau de relevância de cada tecnologia para esse ambiente. Novamente, Segurança da Informação nesse quadro se referiu às técnicas que procuram garantir a segurança do dispositivo IoT (BNDES, 2017i).

Quadro 21 – Necessidades tecnológicas – Indústria

Aplicação	Nome	Manutenção preditiva de plataformas *offshore*	Monitoramento de barragens	Monitoramento de ativos de mineração	Gestão de estoque	Integração da planta produtiva	Engenharia de produtos baseada em dados de sensores	Necessidade
Conectividade	▪ Redes *Low Power Wide Area*		✓					◔
	▪ Redes cabeadas	✓	✓			✓	✓	◑
	▪ Redes de celular			✓				◔
	▪ Redes de curto alcance e alta banda	✓				✓	✓	◑
	▪ Redes de curto alcance e baixa banda			✓	✓	✓	✓	◑
	▪ Redes *mesh*							○
	▪ Redes *Ultra Wideband*				✓			◔
Segurança da informação	▪ Criptografia embarcada						✓	◔
	▪ *Anti jamming*							○
	▪ *Anti tampering*							○
	▪ Assinatura digital						✓	◔
	▪ *Blockchain*							○
	▪ Controle de acesso ao dispositivo						✓	◔
	▪ Falha segura						✓	◔
	▪ *Firmware* seguro	✓					✓	◔
	▪ Ingresso seguro à rede de acesso							○
	▪ Prevenção a DDoS						✓	◔

Legenda para Necessidades: ● **Alta** ◑ **Média** ○ **Baixa.**

Fonte: Adaptado de BNDES, 2017i, v. 7D, p. 23.

Já o quadro 22 apresentou um panorama das necessidades de cada tecnologia e sua capacidade local para Conectividade e Segurança da Informação. O quadro destacou as redes cabeadas e de curto alcance como mais relevantes do ponto de vista de Conectividade para a Indústria. Também indicou que 60% dos atores da vertical tem capacidade para explorar essas tecnologias. Esse quadro fez a mesma análise para a Segurança da Informação. Acentuou-se que as necessidades de segurança na Indústria não são tão relevantes como em outras verticais e que a capacidade tecnológica local tem menos de 30% de atores com competência para seu desenvolvimento (BNDES, 2017i).

Quadro 22 – Necessidades e Capacidades para Conectividade e Segurança – Indústria

	Tecnologias	Necessidades				Capacidades		
Conectividade	Redes cabeadas							
	Redes celulares							
	Redes Low Power Wide Area – LPWA							
	Redes de curto alcance e alta banda							
	Redes de curto alcance e baixa banda							
	Redes Ultra-Wide Band – UWB							
	Redes Mesh							
Segurança do dispositivo	Criptografia embarcada							
	Anti jamming							
	Anti tampering							
	Assinatura digital							
	Blockchain							
	Controle de acesso ao dispositivo							
	Falha segura							
	Firmware seguro							
	Ingresso seguro à rede de acesso							
	Prevenção à negação de serviço							

Legenda para Capacidades – Status:

- Confiança;

- Atenção;

- Dificuldade.

Fonte: Adaptado de BNDES, 2017i, v. 7D, p. 25 e 27.

3.5 Segurança da Informação

A definição de Informação é relativamente difícil e assunto bem debatido dentro da Ciência da Informação. Davenport (1998) a definiu comparando-a com Dados e Conhecimento. Nesse contexto, Dados seriam observações sobre o estado do mundo, fatos brutos, realizados por pessoas ou por dispositivos tecnológicos. Para definir Informação, esse autor usou a definição de Peter Drucker (1988): Informação seriam "dados dotados de relevância e propósito". A relevância e o propósito da Informação seriam dados pela interferência humana, ou seja, pessoas transformam Dados em Informação. E, finalmente, o Conhecimento seria a Informação dentro de um contexto que lhe confere um significado, uma interpretação. Esse autor destacou que o processo de transformação de Dados em Informação e Conhecimento pode ser "incorporado em máquinas" ou, numa visão mais atual, em sistemas que contextualizem os dados adquiridos. Davenport ressaltou que essas definições seriam imprecisas pois a

Informação envolveria todas as três definições e essas definições variariam dentro de contextos específicos.

Silva & Pinto (2005) apresentaram uma definição mais recente de Informação: “conjunto estruturado de representações de representações mentais codificadas (signos, símbolos), socialmente contextualizadas e passíveis de serem registadas num qualquer suporte material (papel, filme, banda magnética, disco compacto, etc.), comunicadas de forma assíncrona e multi-direccionada”. Silva (2009) destacou o caráter transdisciplinar da Ciência da Informação que evoluiu de um paradigma custodial, patrimonialista e historicista (a Informação como um objeto de posse) para o pós-custodial, mais informacional e científico, pertencente ao século XXI. Esse último paradigma permitiu a Informação ser multiplicada e reproduzida, a princípio, sem limites embora ainda pesassem sobre ela as questões de propriedade.

Essa característica de bem simultaneamente material e imaterial direcionou à necessidade de meios que permitam dar segurança a Informação. Citado por Freire *et al.* (2017), Fontes (2006) definiu Segurança da Informação como: "... o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada".

Kurose & Ross (2003) definiram Segurança da Informação por suas caraterísticas: confidencialidade, autenticação, integridade e não repúdio da mensagem, disponibilidade e controle de acesso. Destacaram que, além dessas características relacionadas com a proteção da comunicação, a Segurança da Informação deveria envolver não somente a detecção de falhas na segurança e ataques à infraestrutura de rede como também a resposta a esses ataques.

Baars *et al.* (2018) também procuraram uma definição baseada em características a serem preservadas: confidencialidade, integridade e disponibilidade da informação. Outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, também poderiam ser adicionadas.

Kurose & Ross (2003) mencionaram que as características confidencialidade, autenticação, integridade e não repúdio da mensagem foram consideradas inicialmente como componentes chave da Segurança da Informação e a disponibilidade e controle de acesso surgiram depois, motivadas pelo desenvolvimento das infraestruturas de rede.

Baars *et al.* (2018) afirmaram que essas características evoluíram a partir de três atributos clássicos da segurança, chamado de triângulo CIA: confidencialidade, integridade e disponibilidade que, no inglês, seriam *confidentiality, integrity, avaliability*. A esses atributos se acrescentaram: posse ou controle, autenticidade e utilidade formando um conjunto de seis elementos de Segurança da Informação. Esses autores destacaram que os atributos não podem ser divididos em partes constituintes e representam aspectos únicos da informação. Qualquer violação seria então descrita como aquilo que afetaria a um ou mais desses atributos.

Vroom & Von Solms (2004) apresentaram uma definição baseada no Código de Prática para Gerenciamento de Segurança da Informação do *British Standards Institution* (BS7799, 1999): "As políticas de segurança da informação da organização lidam com os processos e procedimentos que o funcionário deve aderir para proteger a confidencialidade, a integridade e a disponibilidade de informações e outros ativos valiosos". Além de destacar a importância das pessoas na questão da Segurança da Informação, essa definição também se baseou nos atributos considerados clássicos.

O padrão britânico BS7799 deu origem ao padrão sobre Segurança da Informação da *International Organization for Standardization* – ISO, uma organização não governamental independente que conta com 164 instituições padronizadoras nacionais incluindo a ABNT – Associação Brasileira de Normas Técnicas. O conjunto de normas que regula a Segurança da Informação foi publicada internacionalmente pela ISO, em conjunto com o IEC – *International Electrotechnical Commission*, dentro da família ISO/IEC 27000. O conjunto de normas é composto de sete documentos com destaque para a norma ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação (ISO 27000, 2005). Essa norma apresentou a seguinte definição para Segurança da Informação: "preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas" (ABNT NBR ISO/IEC 27002, 2005)

Apesar das pequenas divergências na sistematização, definiu-se a seguir os atributos considerados básicos: Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade:

a) Confidencialidade: estabeleceu que o acesso e uso da informação deveria se restringir a aqueles que necessitariam dela (FONTES, 2010; MANOEL, 2014) ou seja, a informação não deveria ser disponibilizada ou divulgada para pessoas, entidades ou processos que não estivessem previamente autorizados (BAARS, 2018). Kurose & Ross (2003) destacaram que, para garantir a confidencialidade, a mensagem precisaria necessariamente ser criptografada de alguma maneira;
b) Integridade: esse atributo estipulou que a informação acessada deveria estar correta, na mesma condição em que foi disponibilizada, garantindo-se que não foi corrompida, por acidente ou maliciosamente (MANOEL, 2014; FONTES, 2010) Kurose & Ross (2003) concordaram com essa definição e a relacionaram ao não repúdio da sua autoria. Fontes (2010) salientou que a informação deve registrar o usuário que a gerou ou alterou impedindo que ele negue a autoria;
c) Disponibilidade: atributo que determinou que a informação gerada, adquirida ou disponibilizada por um indivíduo da organização deveria estar acessível àqueles autorizados (FONTES, 2010; MANOEL, 2014). Kurose & Ross (2003) acrescentaram que a disponibilidade estaria diretamente relacionada ao controle de acesso à informação;
d) Autenticidade: às vezes chamada de autenticação, esse atributo estabeleceu que as entidades envolvidas no processo de troca de informações deveriam ser quem dizem ser e que a informação trocada não poderia ser alterada durante o seu envio e recebimento (MANOEL, 2014; KUROSE & ROSS, 2003);
e) Legalidade: determinou que o uso da informação deveria estar em conformidade com leis e regulamentos vigentes no local assim como contratos e licenças entre as partes envolvidas. Além disso, deveria atender aos princípios éticos que regem a organização e a sociedade (MANOEL, 2014; FONTES, 2010).

O contexto dessas definições ressaltou o momento no desenvolvimento das redes de computadores em que foram estabelecidas. Elas destacaram o foco inicial na comunicação entre indivíduos e entidades e, logo em seguida, entre computadores trocando informações sobre suas rotinas e processos. No contexto da IoT, as definições devem ser expandidas para a comunicação entre dispositivos com todas suas características e limitações.

Considerando a quantidade de dispositivos que seriam acessados com a difusão de aplicações IoT, o volume um do plano IoT do BNDES previu a multiplicação dos desafios em segurança e privacidade resultantes da implantação dessas soluções destacando-se o acesso não autorizado

a dados pessoais e seu mau uso, a facilitação de ataques a sistemas e os riscos à segurança pessoal. (BNDES, 2017a). Essas preocupações se fundamentariam na quantidade, extensão e difusão previstas pelos meios de comunicação propostos nas soluções.

4 DISCUSSÕES

Apresentou-se a seguir uma compilação das tecnologias de Conectividade e de Segurança de Dispositivo apresentadas no plano IoT do BNDES. Avaliou-se ainda como os atributos de Segurança da Informação seriam considerados por essas tecnologias.

4.1 Tecnologias de Conectividade propostas

Ao se analisar as propostas de conectividade em cada vertical e entre elas, destacou-se uma superposição de soluções por ambiente de aplicação. Várias soluções propostas tiveram soluções semelhantes em outras verticais ou até mesmo dentro da própria vertical. Por exemplo:

a) Dentro da vertical Cidades, a solução de conectividade para as aplicações Medidores inteligentes e gestão da demanda de energia (item 3.4.1.4) e Iluminação pública inteligente (item 3.4.1.5) foi a mesma: celular, LPWA, PLC e rede *Mesh*;
b) O problema a ser solucionado pelas aplicações Localização de ativos e pessoas nas unidades de saúde (item 3.4.2.1), na vertical Saúde, Gestão de desempenho de máquinas (item 3.4.3.6) e Produtividade dos trabalhos por *analytics* (item 3.4.3.7), ambas na vertical Meio Rural, e Monitoração de ativos de mineração (item 3.4.4.3) e Gestão de estoque (item 3.4.4.4), na vertical Indústria, foi basicamente o mesmo, localização de pessoal e equipamentos, embora as soluções de conectividade propostas para todos eles não sejam semelhantes. Entretanto, para as aplicações em ambiente *indoor* nos itens 3.4.2.1 e 3.4.4.4, a proposta foi a mesma: Redes de curto alcance e baixa banda e UWB. De modo semelhante, no ambiente *outdoor*, as soluções propostas foram semelhantes (itens 3.4.3.6 e 3.4.4.3);
c) O monitoramento das condições climáticas nas aplicações Identificação e controle de epidemias (item 3.4.2.5), na vertical Saúde, e Monitoramento de microclima (item 3.4.3.1), na vertical Meio Rural, também conduziu a soluções de conectividade muito semelhantes.

Essa superposição de soluções no mesmo ambiente de aplicação ou em ambientes diferentes poderia representar um facilitador para a implantação dessas soluções pelo rateio do custo de instalação entre várias aplicações. O quadro 23 apresentou todas as propostas de conectividade do plano do BNDES.

Quadro 23 – Tecnologias de Conectividade Propostas

		Tecnologias de Conectividade						
					Curto Alcance			
	Aplicações	**LP WA**	**Redes a Cabo**	**Rede Celular**	**Alta banda**	**Baixa banda**	**Rede *Mesh***	***Ultra Wide Band***
Cidades	Controle de tráfego		X	X		X		
	Monitoramento - crimes	X		X				
	Monitoramento - vídeo		X					
	Medidores inteligentes	X	X	X			X	
	Iluminação inteligente	X	X	X			X	
Saúde	Localização - ativos/pessoas					X		X
	Monitoramento - diabetes				X	X		
	Diagnóstico descentralizado		X		X			
	Diagnóstico - Sepse					X		
	Controle de epidemias	X		X				
Rural	Monitoramento - Microclima	X					X	
	Gestão de pragas			X				
	Mon. comportamento animal	X						
	Mon. peso/alimentação animal		X		X			
	Gestão de saúde animal	X						
	Gestão desempenho máquinas			X				
	Produtividade dos trabalhos	X						
Indústrias	Manut. preditiva plataformas		X		X			
	Monitoramento - barragens	X	X					
	Mon. ativos de mineração			X		X		
	Gestão de estoque					X		X
	Integração da planta produtiva		X		X	X		
	Engenharia - base em sensores		X		X	X		

Fonte: Elaborado pelo autor.

4.2 Conectividade e Segurança da Informação

As tecnologias de conectividade propostas podem ser agrupadas em dois grandes grupos: redes cabeadas e redes sem fio, cada uma delas com suas particularidades do ponto de vista de Segurança da Informação.

4.2.1 Redes cabeadas

O termo redes cabeadas se refere a comunicações que usam um meio físico confinado para a transmissão de sinais, ou seja, um meio que limita sua propagação. Essas redes evoluíram a

partir das redes metálicas feitas com fios de cobre que viabilizaram os primeiros sistemas telefônicos. Com o advento da comunicação de dados por redes telefônicas, as redes metálicas existentes se mostraram incapazes de permitir as taxas de transmissão de dados necessárias à época. Uma solução para resolver esse problema ainda utilizando cabos metálicos foi a introdução dos cabos de pares trançados, bastante utilizados na implantação de redes de computadores até hoje pela facilidade de instalação e baixo custo. Outra solução foi a utilização de cabos coaxiais, mais apropriados para a transmissão de altas taxas de dados e com alta banda passante (da ordem de GHz). A evolução da necessidade de maiores taxas e banda passante conduziu ao uso de materiais diferentes como a sílica que culminou com o aparecimento das primeiras fibras ópticas na década de 70 (BNDES, 2017f; COELHO, 2003; RIBEIRO, 2005).

Apesar de ser um meio confinado, essas redes cabeadas estão sujeitas a invasão pela conexão de dispositivos não credenciados. Sob esse ponto de vista, as redes metálicas estão mais sujeitas a esses eventos por ser mais simples a conexão com o par trançado ou com a rede coaxial. Em redes ópticas, a inserção e retirada de sinais não seria impossível e, geralmente, implicaria na interrupção temporária do sinal no cabo. Também acarretaria uma perda de sinal perceptível e na necessidade de uma interface óptica compatível, o que dificultaria a conexão. Desse modo, o meio mais eficaz de proteger essas redes seria fazer com que os dispositivos que usam o meio de comunicação estejam em conformidade com os atributos da Segurança da Informação.

4.2.2 Redes sem fio

As redes sem fio usam o ar como meio físico para a transmissão dos sinais. Apesar do uso de antenas que poderiam direcionar o sinal, a propagação dos sinais não é confinada, ou seja, qualquer dispositivo que esteja no caminho de propagação do sinal poderia recebê-lo. Essas redes evoluíram com os primeiros sistemas telegráficos sem fio de Guglielmo Marconi em 1901. A partir daí, surgiram as emissoras de rádio em *broadcasting* AM e FM, iniciadas em 1906, de TV, em 1927 e as transmissões via rádio ponto a ponto, em 1947. As redes de comunicação móvel tiveram seu início no auxílio a atividade policial na cidade de Detroit em 1921. Esses primeiros sistemas se valiam de um transceptor potente colocado em um ponto alto que cobrisse toda a área de interesse. Os sistemas de comunicação móvel celular surgiram na Escandinávia em 1981 com o *Nordic Mobile Telephone* – NMT, seguido do sistema AMPS – *Advanced Mobile Phone Service*, em 1983. Em 1988, o sistema celular digital GSM – *Global*

System for Mobile Communications começou a ser implantado na Europa (HAYKIN & MOHER, 2008a; HAYKIN & MOHER, 2008b).

Foerster *et al.* (2001) comentaram que, considerando o problema geral que todos os sistemas de comunicação tentam resolver, os sistemas sem fio deveriam ser capazes de enviar muitos dados, muito longe, muito rápido, para muitos usuários e tudo de uma vez. Infelizmente, é impossível obter todos os cinco atributos simultaneamente para sistemas que suportam fluxos de comunicação únicos, privados e bidirecionais; um ou mais desses atributos precisam ser sacrificados para que os outros se saiam bem. Os sistemas sem fio originais foram construídos para vencer grandes distâncias, a fim de conectar duas partes. No entanto, a história da telecomunicação moderna mostra uma clara tendência de melhoria nos outros quatro atributos em detrimento da distância. A telefonia celular é o exemplo mais óbvio. Distâncias mais curtas permitiram a reutilização do espectro radioelétrico, atendendo assim a mais usuários e a comunicação entre estações é suportada por uma infraestrutura cabeada.

O conceito de canal de comunicação evoluiu com os sistemas de comunicação. Fora do universo técnico, a palavra canal está associada ainda hoje à emissora ou estação que transmite o sinal. Essa ideia veio dos primeiros sistemas de rádio e TV em que a frequência central de transmissão do sinal indicava a estação. Esses sistemas, chamados de FDM – *Frequency Division Multiplexing* ou multiplexação por divisão de frequência, baseavam-se na divisão do espectro eletromagnético em trechos limitados por uma frequência inicial e final que indicavam os limites de operação da estação. Surgiu então o conceito de largura de canal, ou seja, a diferença entre a frequência final e a inicial, expressa na unidade Hertz – Hz. A divisão do espectro foi importante para evitar a interferência de uma transmissão nas outras e é regulada hoje por organismos nacionais (FCC – *Federal Communications Commission*, nos EUA, ANATEL – Agência Nacional de Telecomunicações, no Brasil) e internacionais (ITU – *International Telecommunications Union*). O termo multiplexação teria a conotação de multiplicação de uso do meio de transmissão e surgiu em consequência da expansão do *broadcast* de rádio a partir de 1906. A ideia da multiplexação evoluiu para os sistemas TDM – *Time-Division Multiplexing* em que cada comunicação ocuparia todo o espectro destinado àquele serviço, e não parte dele, mas por um intervalo de tempo especificado.

Haykin & Moher (2008a) definiram canal como "o caminho físico de transporte de sinal gerado pelo transmissor e que proporciona a entrega da informação ao receptor" (p. 22). Essa definição

é ampla o suficiente para cobrir as redes cabeadas e aquelas sem fio. Especificamente para sistemas sem fio, os canais de comunicação sofrem os seguintes efeitos do meio de transmissão:

a) Atenuação: perdas de potência do sinal irradiado relacionadas às condições do meio (pressão atmosférica, umidade), à dispersão do sinal na direção de propagação e à presença de obstáculos que dificultam ou impedem sua passagem; a atenuação é diretamente proporcional à frequência do sistema;
b) Distorção: efeito causado pela chegada de múltiplos sinais refletidos no receptor que provocam interferências construtivas e destrutivas;
c) Variação das condições de propagação no meio: devido a mudanças atmosféricas e à mobilidade entre as unidades transceptoras;
d) Interferência acidental ou intencional: causadas por fontes radioelétricas na mesma faixa de frequência do sinal transmitido;
e) Ruído: sinais interferentes de ampla faixa causados por fontes naturais (Sol, descargas atmosféricas, radiação cósmica) ou artificiais como processos industriais, interferência de sistemas elétricos e ignição de veículos (HAYKIN & MOHER, 2008ª).

Por ser um meio não confinado, as redes sem fio são mais vulneráveis à invasão desde que o dispositivo invasor esteja dentro do alcance da rede. O invasor poderia não somente retirar informações da rede como também poderia alterá-las. Nesses casos, caberia aos dispositivos que usam a rede garantirem a Segurança da Informação. Outra forma de ataque às redes sem fio seria pela radiodifusão de um sinal interferente dentro do espectro destinado ao serviço (*jamming*).

4.2.3 Sistemas Celulares

Conceitualmente, os primeiros sistemas de comunicação móvel eram bem diferentes dos sistemas celulares. Nos primeiros, o princípio foi cobrir toda a área de interesse com um único transceptor potente que pudesse alcançar as unidades móveis. Todos as unidades móveis se comunicavam na mesma frequência, ou canal, o que limitava a quantidade de comunicações simultâneas. O conceito de célula colocou vários transceptores fixos, chamados de estações rádio base ou ERBs, na área de prestação do serviço, todos com potência limitada de modo a cobrir apenas uma determinada área no seu entorno, a sua célula. Colocando o transceptor da ERB de cada célula em um conjunto de canais pré-definidos, as unidades móveis poderiam se

comunicar enquanto estivessem dentro da célula. As células vizinhas seriam alocadas em um conjunto de canais diferentes para não interferir na comunicação umas das outras. Esse último conceito é chamado reuso de frequências.

Os sistemas celulares criaram o conceito de *acesso múltiplo* ao meio de comunicação. Nesse conceito, a faixa de frequência destinada ao serviço de comunicação é compartilhada de forma dinâmica por todas as unidades transceptoras da rede. As técnicas propostas evoluíram a partir das técnicas de multiplexação anteriores, a saber:

a) FDMA (*Frequency-Division Multiple Access*): a faixa de frequência destinada ao serviço é dividida em vários canais menores, de frequência específica, fixos ou variáveis;
b) TDMA (*Time-Division Multiple Access*): os usuários do sistema têm acesso completo ao espectro de frequências destinado ao serviço por um determinado intervalo de tempo, fixo ou variável;
c) CDMA (Code-Division Multiple Access): técnica que evoluiu junto com a capacidade de processamento de dados, baseia-se num método de codificação do sinal a ser transmitido (modulação por espalhamento espectral) em que cada usuário tem sua comunicação 'criptografada' por um código específico e transmitida junto com a comunicação de todos os outros usuários ocupando todo o espectro de frequência alocado para o serviço, o tempo todo. A separação da comunicação de cada usuário se dá pelo uso de códigos distintos para cada um. Define-se modulação de um sinal, elétrico ou de rádio, como a variação de suas características (amplitude, frequência ou fase) proporcionalmente à informação de modo a permitir sua transmissão e recuperação;
d) SDMA (*Space-Division Multiple Access*): essa técnica de acesso utiliza antenas inteligentes que se aproveitam da distribuição espacial dos usuários direcionando o sinal para cada terminal de usuário.

Os sistemas celulares usam a combinação dessas técnicas para maximizar a utilização do espectro de frequência disponível (HAYKIN & MOHER, 2008a).

Os primeiros sistemas celulares utilizavam tecnologia analógica para comunicação. Nesses sistemas, chamados de primeira geração ou 1G, os aparelhos eram grandes e pesados pois, por não fazerem o controle da potência irradiada, necessitavam de baterias maiores e, mesmo assim,

de curta duração. A tecnologia de baterias da época também fazia com que os aparelhos fossem volumosos e pesados. A próxima evolução levou aos sistemas 2G, que introduziram a tecnologia digital, a criptografia na transmissão e inauguraram os serviços de transmissão de dados móveis através do SMS – *Short Message Service*. Dois padrões surgiram nessa época: o GSM e o D-AMPS ou, Digital-AMPS, que utilizavam TDMA e uma combinação de TDMA e FDMA como técnica de acesso, respectivamente. Uma evolução dentro dos sistemas 2G, chamado de geração 2,5G foi a introdução do GPRS – *General Packet Radio Service* dentro das redes GSM, o que significou um avanço na capacidade de transmissão de dados móveis permitindo a oferta de vários serviços como MMS – *Multimedia Messaging Service* e serviços P2P – *Point-to-Point*. Os sistemas 3G seguiram o aprimoramento da tecnologia através da introdução da técnica de acesso CDMA nas redes celulares com aumento na taxa de transmissão de dados. O aprimoramento dos sistemas conduziu à geração 4G que possibilitou o acesso móvel em banda larga a Internet por *laptops* e *smartphones*. Dentro dessa geração, foi introduzido o padrão de comunicação banda larga LTE – *Long-Term Evolution* que foi adotado também pelos sistemas GSM como EDGE – *Enhanced Data rates for GSM Evolution*. A próxima evolução, os sistemas 5G, já está em desenvolvimento prometendo taxas de transmissão de dados ainda maiores, melhoria na cobertura e na eficiência do uso do espectro radioelétrico, dentre outras vantagens.

A evolução dos sistemas celulares foi coordenada por órgãos reguladores internacionais e nacionais e representantes dos fabricantes. Essas redes operam em faixas do espectro radioelétrico pré-determinadas e que devem ser licenciadas. No Brasil, as empresas que podem explorar o serviço devem ter uma concessão, autorização ou permissão, concedida pela ANATEL, para exploração no espectro licenciado para do serviço de telefonia celular.

Forte *et al.* (2019, p. 152) identificaram duas partes em uma rede celular: a rede de acesso, que interliga as unidades móveis às ERBs, e a rede principal, que interliga as ERBs. Destacaram que o desempenho da interface aérea, ou seja, o link entre duas estações rádio na comunicação móvel, incluída na rede de acesso, aumentou drasticamente com a evolução dos sistemas, proporcionando alta taxa de transferência e baixa latência. Isso permitiu atender as expectativas dos usuários em termos de "velocidade bruta" de transmissão de dados. As mudanças na rede principal, por outro lado, teriam sido muito mais lentas e incrementais. Além disso, sua complexidade aumentou drasticamente devido à necessidade comercial de garantir o suporte de tecnologias mais antigas, como 2G (ou seja, GSM) e 2,5G (GPRS). Salientaram que a arquitetura geral não mudou significativamente ao longo dos anos.

Algumas tecnologias de transmissão de dados dentro das redes celulares estariam diretamente relacionadas a IoT e estariam sendo desenvolvidas para atendê-las. Nesse contexto, Durant *et al.* (2019, p. 2) destacaram que a IoT de banda estreita (NB-IoT – *Narrow Band – Internet of Things*), também conhecida como LTE Categoria NB1, seria um padrão de comunicação LPWA suportado por operadoras de rede celular, desenvolvida para atender aos novos requisitos de cobertura estendida em locais rurais e em ambientes internos em que dispositivos de IoT estariam presentes. O NB-IoT suportaria uma conexão IoT de menor potência do que o padrão GPRS atual permitindo assim vários anos de conectividade para aplicativos de IoT movidos a bateria. Esses autores destacaram que o NB-IoT seria suportado por mais de trinta operadoras de rede móvel do mundo, tanto em GSM/GPRS quanto em LTE.

Dao *et al.* (2017) relataram que organizações de padronização celular como 3GPP (*3rd Generation Partnership Project* – Projeto de Parceria da Terceira Geração) estariam trabalhando ativamente para os próximos estágios do padrão LTE a fim de oferecer suporte à comunicação de tipo de máquina MTC ou *Machine-Type Communication*, também conhecida como LTE-M – *Long-Term Evolution – Machine-Type Communications*. Segundo esses autores, o MTC definiria a comunicação de dados entre dispositivos sem ajuda humana, o que se aplicaria principalmente a dispositivos de baixo teor de dados e de baixa potência. Assim, o MTC seria considerado uma abordagem promissora para a disseminação de plataformas de detecção da Internet das Coisas que geralmente envolvem baixa taxas de dados. Utilizando os benefícios da infraestrutura LTE-M, espera-se que as plataformas de detecção de IoT cubram uma área geográfica maior com um custo economicamente viável, uma vez que o MTC tem um relacionamento muito próximo com os dispositivos de IoT.

As redes celulares apresentam um grau de segurança maior hoje que no seu início quando a clonagem de telefones móveis provocou prejuízos para as operadoras e muitas dúvidas nos usuários. No caso dos sistemas GSM, a criptografia esteve presente desde sua concepção inicial. Já nas redes que utilizam a técnica de acesso CDMA, a segurança é obtida com a codificação do sinal a ser transmitido por espalhamento espectral.

4.2.4 Redes Wi-Fi

Classificadas no plano do BNDES com redes de curto alcance e alta banda, consideram-se Redes Wi-Fi todas aquelas que utilizam o padrão de comunicação 802.11 do IEEE – *Institute*

of Electrical and Electronics Engineers. Tanenbaum (2003, p. 292 e 293) relatou que, a partir do padrão original do IEEE, desenvolveram-se variantes específicas para atender a diversos sistemas e que alteraram a estrutura do protocolo de comunicação e as técnicas de modulação e transmissão de dados. Essas técnicas de transmissão utilizariam comunicação por infravermelho e por ondas de rádio. No escopo desse trabalho, destacou-se as técnicas de transmissão Wi-Fi via rádio, todas variações da modulação por espalhamento espectral associadas ao modo de transmissão CDMA, a saber:

a) Espalhamento espectral por sequência direta (DSSS – *Direct Sequence Spread Spectrum*): Nessa técnica, a informação binária a ser transmitida é multiplicada com uma sequência de bits muito maior, chamada de sequência de espalhamento, gerando um sinal de banda larga. Vários sinais podem ocupar a mesma banda desde que utilizem sequências de espalhamento diferentes. Como os sinais são transmitidos em banda larga, são relativamente mais imunes ao ruído que mais comumente ocupa uma faixa estreita do espectro. Na demodulação do sinal DSSS, é preciso conhecer exatamente a sequência de espalhamento o que implica numa relativa Segurança da Informação;
b) Espalhamento espectral por salto de frequência (FHSS – *Frequency Hoping Spread Spectrum*): Essa técnica faz com que a informação a ser transmitida ocupe um canal estreito dentro de uma faixa mais larga, mas que muda a frequência de transmissão do canal segundo um padrão pseudoaleatório. Para demodular esse sinal, é preciso conhecer o padrão pseudoaleatório de salto e o tempo de permanência do canal em cada frequência;
c) Multiplexação por divisão de frequências ortogonais (OFDM – *Orthogonal Frequency Division Multiplexing*): técnica de modulação e transmissão considerada uma forma de modulação por espalhamento espectral, diferente do CDMA e do FHSS, em que a informação a ser transmitida é dividida em feixes paralelos que são transmitidos em canais menores dentro da faixa o que conduz a mais imunidade ao ruído;
d) Espalhamento espectral por sequência direta de alta taxa (HR-DSSS – *High Rate Direct Sequence Spread Spectrum*): variação do DSSS que garante maiores taxas de transmissão de dados. (TANENBAUM, 2003, p. 294 e 295; GUIMARÃES & SOUZA, 2012, p. 227, 228, 255 a 260).

O padrão 802.11 também implementou, em sua versão original, um protocolo na camada de enlace chamado WEP (*Wired Equivalence Privacy*) que apresentava um nível de segurança em redes sem fio tão bom como em redes cabeadas. Como esse protocolo não garantia bom nível

de segurança, a Wi-Fi *Alliance*, empresa criadora da tecnologia, implementou os formatos WPA (*Wired Protected Access*) e WPA2 baseados em técnicas de criptografia mais robustas (TANENBAUM, 2003).

A combinação de modulação e transmissão por espalhamento espectral e criptografia mais robusta garantem ao Wi-Fi um bom nível de segurança. Entretanto, como a modulação e transmissão são padronizadas e as frequências e características do tratamento do sinal a ser transmitido são de conhecimento público persiste uma certa facilidade para a invasão. Outra questão é que a segurança e criptografia precisam ser configuradas pelo usuário e, por seu descuido, ainda existem casos de intrusão em redes Wi-Fi.

4.2.5 Redes LPWA

As redes definidas como LPWA são aquelas específicas para comunicação sem a interferência humana entre dispositivos e máquinas. Podem ser implementadas dentro de redes celulares existentes ou em outras redes. Begishev *et al.* (2018, p. 1) afirmaram que os exemplos mais bem-sucedidos de sistemas que se baseiam em comunicações M2M incluem o LTE-M, o GSM baseado em GPRS/EDGE e o NB-IoT, que operam dentro das redes celulares e já foram apresentados, e também LoRa e o Sigfox, fora dos sistemas celulares.

Diferente de LTE-M e NB-IoT, o LoRa funciona em uma faixa do espectro definida como não licenciada, ou seja, não há necessidade de reservar junto a órgãos reguladores nacionais uma faixa de frequência para o uso. Também, em sistemas não licenciados, a potência irradiada é limitada buscando minimizar as interferências. Qin *et al.* (2019, p. 4 e 5) reportaram que a LoRa *Alliance*, organização mundial de fabricantes para o desenvolvimento dessa tecnologia, definiu o uso da técnica de espalhamento espectral, semelhante ao CDMA, e de componentes mais baratos que conduzem a um custo reduzido dos dispositivos. A opção por espectro não licenciado dificulta o controle do uso do sistema. Esses mesmos autores informaram que a alta flexibilidade e escalabilidade do sistema LoRa atraiu interesses crescentes do setor e da academia, tornando-o uma das tecnologias LPWA mais amplamente implantadas em todo o mundo, mas, a interferência de dispositivos LoRa que compartilham o mesmo slot de tempo, frequência e fator de espalhamento degradariam o ambiente do canal e reduziriam a probabilidade de cobertura dos *gateways* LoRa. O uso do espectro não licenciado tornaria o

problema de interferência mais crítico nas redes LoRa, especialmente quando dispositivos de outras redes trabalhando na mesma frequência estivessem presentes.

Outro sistema que compete com o LoRa é o Sigfox. Durant *et al.* (2019) apresentaram a Sigfox como uma tecnologia proprietária originada na França que tem como objetivo fornecer conectividade de ponta a ponta para IoT em redes LPWA. Os dispositivos finais usariam um canal de 200 kHz em torno da faixa central de 868 MHz para transmitir mensagens via modulação de banda estreita para estações base em uma topologia em estrela. A modulação utilizada resultaria em níveis de ruído muito baixos, o que significa maior sensibilidade do receptor e, portanto, os dispositivos poderiam se beneficiar do baixo consumo de energia e de antenas baratas. Os rádios da estação base, que recebem mensagens enviadas pelos dispositivos e transmitem mensagens para eles, seriam implantados por operadores de rede Sigfox. A rede limitaria a comunicação a 140 mensagens de *uplink* (do dispositivo para o *gateway*) e 8 mensagens de *downlink* por dia por dispositivo.

Ikpehai *et al.* (2019) compararam os dois modelos de negócio: a Sigfox implantaria e operaria a rede, mas forneceria livremente a especificação do protocolo aos fabricantes de chips e a LoRa forneceria um chipset fechado, mas rede aberta onde até redes privadas seriam possíveis. Assim, o Sigfox seria uma rede fechada, mas com chipset aberto e a LoRa, o contrário. Nesses modelos, a Semtech, fabricante dos chips LoRa, controlaria a produção, suporte e preço dos chipsets, enquanto a Sigfox controlaria o fornecimento, acesso e preço dos recursos da rede.

Outras propostas de redes LPWA seriam a RPMA – *Random Phase Multiple Access* e a Weightless. A RPMA seria uma tecnologia proprietária pela Ingenu baseada em espalhamento espectral por sequência direta. A tecnologia Weightless foi desenvolvida por um grupo de empresas que inclui Accenture, ARM, M2COMM, Sony-Europe e Telensa. Essa última utilizaria uma combinação das técnicas de acesso FDMA e TDMA em seu padrão dedicado a IoT. Ambas trabalhariam em faixas de espectro não licenciado.

Como já mencionado, as redes sem fio estão sempre sujeitas a interferência. No caso de uso de soluções em espectro não licenciado, a questão é agravada pois não há a reserva de um espaço no espectro radioelétrico para a prestação do serviço. Assim, qualquer rede pode usar o espectro a qualquer momento, comprometendo a sua disponibilidade. O uso de criptografia e técnicas semelhantes ao CDMA pelas redes LPWA assegura a confidencialidade da comunicação.

4.2.6 Redes Bluetooth

O sistema *Bluetooth*, considerado no plano do BNDES como uma rede de curto alcance e baixa banda, surgiu do interesse de várias companhias dos setores de comunicação e hardware para computação em conectar dispositivos sem fio. Esse interesse logo se expandiu para o estabelecimento de redes wireless que pudessem competir com o padrão 802.11 do Wi-Fi. Planejadas para ter alcance mais restrito, essas redes foram normalizadas pelo IEEE pelo padrão 802.15 e classificadas como PAN – *Personal Area Networks* (TANENBAUM, 2003, p. 310). A modulação utilizada no *Bluetooth* é o FHSS com boa imunidade a interferência de outras fontes dentro da sua faixa de transmissão de 2,4 GHz (BHAGWAT, 2001).

Qin *et al.* (2019) relataram que o sistema *Bluetooth* inicial evoluiu até que, em 2010, foi lançado o BLE – *Bluetooth Low Energy*, que faria parte da especificação principal do *Bluetooth* 4.0 e não mais compatível com o *Bluetooth* 'clássico'. O BLE funcionava na faixa não licenciada de 2,4 GHz e teria alcance da transmissão de até 100 metros. Posteriormente, com o *Bluetooth* 5 lançado em 2016, o alcance da transmissão pode ser quadruplicado através do aumento da potência de transmissão. Em 2017, o grupo de interesse especial do *Bluetooth* ratificou uma especificação para configuração *mesh*, permitindo que os dispositivos atuassem como retransmissores de informação com base nas tecnologias BLE. Em comparação com o *Bluetooth* clássico, o BLE foi caracterizado como baixo consumo de corrente mesmo quando o dispositivo se encontra em condição de consumo de pico, médio ou quando encontra-se ocioso, permitindo que os dispositivos BLE funcionem por anos com uma célula de bateria comum, do tipo moeda. Esses autores reportaram ainda que o BLE tem várias aplicações em dispositivos de baixo custo e alimentados por bateria, em áreas como *healthcare* e *smart home*. Uma característica exclusiva do BLE, em contraste com o LoRa, é que a maioria dos telefones celulares já suporta esse padrão. Com uma conexão celular existente, um *smartphone* pode atuar naturalmente como um nó de retransmissão para fornecer conexão LTE indireta a dispositivos IoT.

O BLE também padece das consequências do uso de espectro não licenciado, ou seja, pode sofrer interferência de outros sistemas operando na mesma faixa. Quanto a Segurança da Informação, o BLE utiliza criptografia semelhante ao protocolo WPA.

4.2.7 Redes UWB

A tecnologia de banda ultra larga (UWB – *Ultra-Wide Band*) foi inicialmente desenvolvida na década de 80 para sistemas do tipo RADAR – *Radio Detection And Ranging* ou Detecção e Telemetria por Rádio devido à natureza de banda larga do sinal que resulta em maior precisão na telemetria de objetos. Atualmente, é considerada uma alternativa para sistema de comunicação de alta capacidade e também para indicação de posição dos receptores em ambiente *indoor*. Embora o termo banda ultra larga não seja muito descritivo, ajuda a separar essa tecnologia dos sistemas de banda estreita e banda larga normalmente mencionados na literatura que descreve os sistemas celulares. Existem duas diferenças principais entre o UWB e esses outros sistemas. Primeiro, a largura de banda dos sistemas UWB, conforme definido pela *Federal Communications Commission* (FCC), deve ser superior a 20% de uma frequência central ou 500 MHz. Como a faixa de frequência para o sistema foi regulamentada pelo FCC entre 3,1 e 10,6 GHz, esse percentual conduziria a uma largura de banda de 620 MHZ, no mínimo, muito maior que a largura de banda normalmente usada pelas tecnologias de comunicação. A segunda diferença seria que o UWB é normalmente implementado sem a inserção de uma portadora. Os sistemas convencionais de banda estreita e banda larga usam portadoras de radiofrequência para transladar o sinal no domínio da frequência da banda base do sinal para a frequência da portadora real, ou seja, para a frequência na qual o sistema pode operar e que será transmitida. Como já são sinais de alta frequência, as implementações de UWB podem modular diretamente um sinal de transmissão do tipo ‘impulso’, um sinal de onda quadrada que possui um tempo de subida e queda muito acentuado, resultando em um sinal transmitido que pode ocupar vários GHz de largura de banda (FOERSTER *et al.*, 2001).

Apesar de reclamações de interferência com sistemas de geolocalização por satélite relacionadas com a faixa de frequências previamente alocada para o UWB, esse sistema foi padronizado dentro do padrão IEEE 802.15 para redes PAN em 2007 (DIVIS, 2019).

Ha & Schaumont (2007) reportaram que é difícil ‘bisbilhotar’ o sistema UWB devido ao baixo nível de energia das transmissões UWB. Afirmaram ainda que as transmissões UWB são mais robustas à interferência do que as transmissões de banda estreita, difíceis de obstruir e permitem múltiplas transmissões na mesma banda. Entretanto, destacaram que o UWB não tem criptografia de dados.

4.2.8 RFID e NFC

Gubbi *et al.* (2013) descreveram a tecnologia RFID – *Radio-Frequency IDentification* como uma grande inovação no paradigma de comunicação incorporado, que permite o design de microchips para comunicação de dados sem fio. Esses chips ajudariam na identificação automática de qualquer coisa a que estejam ligados, atuando como um código de barras eletrônico. As etiquetas (*tags*) RFID passivas não são alimentadas por bateria e usam a potência do sinal de interrogação para comunicar sua identificação ao leitor RFID. Isso resultou em muitas aplicações, principalmente no varejo e no gerenciamento da cadeia de suprimentos. As etiquetas passivas podem ser encontradas nos aplicativos de transporte (substituição de passagens, adesivos de registro) e controle de acesso. As *tags* passivas estão sendo usadas atualmente em muitos cartões bancários e etiquetas de pedágio, que estão entre as primeiras implantações globais. As etiquetas RFID ativas têm sua própria fonte de bateria e podem iniciar a comunicação. Das várias aplicações para etiquetas RFID ativas, esses autores destacaram o uso em contêineres portuários para monitoramento de cargas.

Want (2006) descreveu como se processa a transmissão de sinais nas etiquetas RFID. Existem basicamente dois métodos: o NFC – *Near Field Communication* ou comunicação por campo próximo, e o *Far Field* ou comunicação por campo distante. No primeiro, que dá nome a esse tipo de comunicação, o leitor emite constantemente um sinal magnético na frequência do sistema e, quando a etiqueta se aproxima, ela sofre a indução de uma tensão elétrica que dá carga no seu circuito. Como nesse sistema tanto o leitor como a etiqueta possuem bobinas, o efeito poderia ser comparado ao de um transformador. Então, variando a carga inserida no circuito da etiqueta (o secundário do transformador) varia-se a sua corrente que pode ser detectada no leitor (que seria o primário do transformador). Assim, variando a carga segundo um código pré-definido, é possível fazer a transmissão do código da etiqueta. Esse método é chamado de modulação em carga. Entretanto, o alcance da indução varia inversamente com a frequência, ou seja, quanto maior a frequência do sistema, menor a distância para a indução da tensão. Outra limitação desse sistema seria que a energia do sinal do leitor diminui com a expansão volumétrica da onda, ou seja, com o cubo da distância entre a bobina do leitor e a etiqueta. Esses fatores, aliados à necessidade de muitos bits de informação em sistemas NFC, conduziram a projetos de etiquetas passivas baseadas na comunicação por campo distante.

Na comunicação por campo distante são utilizadas antenas do tipo dipolo magnético tanto no leitor como na etiqueta. A indução de tensão nas *tags* passivas se processa da mesma forma,

mas, como elas estariam fora do alcance do campo próximo, não podem ser usadas técnicas semelhantes a modulação em carga. Nesse caso, a técnica utilizada seria o espalhamento de retorno que funciona com o descasamento proposital da impedância entre o transmissor e a antena na etiqueta diminuindo a energia irradiada. O descasamento seria codificado segundo as informações a serem transmitidas de modo que a energia retornada para o leitor transmitiria o código. O alcance dos sistemas de comunicação por campo distante depende basicamente da quantidade de energia irradiada que chega até as etiquetas e da sensibilidade do leitor para receber o sinal de resposta. Valores típicos de alcance estariam na faixa de 3 a 6 metros. Como as etiquetas possuem um número de série, é possível fazer a leitura simultânea de muitas etiquetas (WANT, 2006).

4.3 Compilação de informações sobre Conectividade

Considerando as tecnologias de conectividade propostas, apresentou-se a seguir uma compilação de informações relativas a essas tecnologias e sua relação com os atributos de Segurança da Informação. Primeiramente, o quadro 24 apresentou as características das tecnologias sem fio para IoT apresentadas.

Quadro 24 – Tecnologias sem fio para IoT

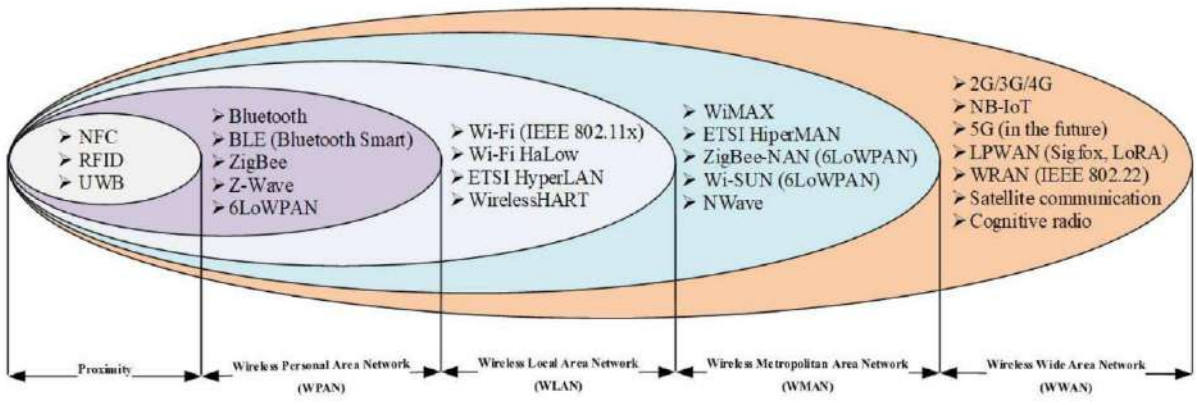
	LTE-M	NB-IoT	Wi-Fi	LoRa	Sigfox	BLE	RFID	NFC	UWB
Classifi-cação	1	2	3	2		4			3
Sistema	Celular LPWA		Wi-Fi	LPWA		BT	*Smart Tags*		UWB
Tipo de multiplex	GSM*, CDMA		CDMA				Modulação Direta		
Espectro	Licenciado		Não licenciado						
Tipo de rede	WWAN		WLAN	WWAN		WPAN	WBAN NFC		WLAN
Segurança	Muito boa		Baixa	Baixa	Baixa	Baixa	Razoável		Boa
Criptogra-fia	Sim	Sim	WPA2	Não	Não	Tipo WPA	Não	Não	Não

Legenda:
1 – Longo Alcance e Alta Banda **2 – Longo Alcance e Baixa Banda**
3 – Curto Alcance e Alta Banda **4 – Curto Alcance e Baixa Banda**
GSM* = FDMA-TDMA **Valores máximos**

Fonte: Elaborado pelo autor.

Čolaković & Hadžialić (2018) reuniram na figura 28 todas as tecnologias sem fio utilizadas para IoT classificadas segundo a distância, muitas delas já apresentadas.

Figura 28 – Alcance das tecnologias sem fio



Fonte: Čolaković & Hadžialić, 2018, p.23.

O quadro 25 apresentou uma relação entre as tecnologias de conectividade propostas e os atributos de Segurança da Informação. Nesse quadro, as redes cabeadas e as redes celulares foram consideradas sob dois aspectos: a segurança do meio de comunicação usado e da tecnologia de conectividade usada.

Quadro 25 – Conectividade x Atributos da Segurança da Informação

		Atributos da Segurança da Informação				
		Confidencialidade	**Integridade**	**Disponibilidade**	**Autenticidade**	**Legalidade**
Tecnologias de Conectividade	**Redes Cabeadas – meio**	**N**	**N**	**A**	**N**	**A**
	Redes Cabeadas – acesso	**A**	**A**	**A**	**A**	**A**
	Redes sem fio – meio	**N**	**N**	**N**	**N**	**A**
	Redes Celulares – acesso	**A**	**A**	**N**	**A**	**A**
	LPWA	**N**	**A**	**N**	**A**	**A**
	Curto Alcance – Baixa banda	**N**	**A**	**N**	**A**	**A**
	Curto Alcance – Alta banda	**N**	**A**	**N**	**A**	**A**
	Redes *Ultra-Wide Band*	**A**	**A**	**N**	**A**	**A**
	Redes *Mesh*	**N**	**A**	**N**	**A**	**A**

Legenda: A – Atende, N – Não atende.

Fonte: Elaborado pelo autor.

Apresentaram-se algumas ponderações sobre o quadro 25:

a) O espaço como meio de propagação das redes sem fio não atende a confidencialidade devido a facilidade de interceptação dos sinais; entretanto, quando implementada uma tecnologia de transmissão ou criptografia que dificulta o entendimento da mensagem, a tecnologia atende a confidencialidade;
b) Os meios de transmissão em si (cabo ou espaço) não atendem a integridade da informação já que dificultam a passagem dos sinais devido a atenuação, distorção, interferência e ruído; entretanto, a implementação de métodos simples de checagem de integridade da mensagem até uma criptografia mais complexa melhora o desempenho desse atributo;

c) Devido às condições de propagação variáveis, não há como afirmar com certeza que a disponibilidade da informação em sistemas sem fio será atendida; entretanto, as redes cabeadas podem atendê-la já que utilizam um meio confinado e, portanto, mais controlado; uma restrição a esse último argumento pode ser feita no caso de redes cabeadas externas;
d) Ambos os meios de transmissão de sinais estudados podem ser invadidos, o que não atenderia a autenticidade da informação; entretanto, métodos de controle de acesso implementados nas tecnologias consideradas podem atendê-la;
e) Todos os sistemas estudados foram objeto de padronização internacional por órgãos públicos ou de fabricantes e desenvolvedores, mesmo os que operam em faixas não licenciadas; esses padrões foram considerados pela ANATEL e têm permissão de uso no Brasil, atendendo assim ao atributo legalidade; pode-se destacar ainda o esforço dos organismos internacionais para evitar que um sistema interfira no outro em frequências não licenciadas.

4.4 Tecnologias de Segurança de Dispositivos propostas

Constatou-se que os dispositivos que acessam a rede IoT sofrem influência direta da concepção do sistema sob vários aspectos:

a) Dimensão: o dispositivo de acesso tem sua dimensão física e peso relacionada ao objeto ou função na rede; por exemplo, um *gateway* veicular a ser instalado numa máquina agrícola pode ser mais volumoso e pesado do que um dispositivo de controle de funcionários numa fábrica;
b) Faixa de frequência: nos sistemas *wireless*, a faixa de frequência escolhida influencia diretamente o dispositivo pois ela exerce influência direta nas dimensões da antena e no alcance do sistema; via de regra, frequências mais altas implicam em antenas menores e menor alcance do sistema (maior atenuação);
c) Sensores: a necessidade de monitorar parâmetros do objeto implica em dispositivos com sensores próprios ou que necessitam ser conectados;
d) Capacidade de processamento e armazenamento: dependendo das necessidades do sistema, o dispositivo deverá possuir maior capacidade de processamento para aquisição e transmissão de sinais ou criptografia e também armazenagem de informações em redes tipo *stop-and-foward*;

e) Necessidade de energia: Esse é um grande problema para os dispositivos; várias características do sistema influenciam no consumo de energia do dispositivo: processamento de sinais para captura ou transmissão, criptografia, armazenamento, técnica de transmissão utilizada e alcance da rede; usualmente, quanto mais tratamento de informação ocorrer e maior alcance for necessário, mais energia o dispositivo vai necessitar; a necessidade de muita energia pode conduzir a dispositivos mais volumosos devido ao tamanho das baterias necessárias, ou a uma manutenção mais frequente para a sua troca;
f) Custo: geralmente, dispositivos mais sofisticados e que apresentam grande consumo de energia têm um custo maior de implantação e reposição.

BNDES (2017a) destacou que a grande quantidade de dispositivos previstos para as redes IoT resultaria numa infraestrutura de conectividade mais complexa com diferentes necessidades no que diz respeito ao consumo de energia do dispositivo, cobertura da rede e largura de banda necessária.

Com relação ao consumo de energia, Dao *et al.* (2017) destacaram que apesar de uma grande variedade de técnicas de eficiência energética tenham sido propostas em redes celulares, existiria apenas um número limitado de esquemas para LTE-M. Essas técnicas de eficiência energética existentes e que poderiam ser utilizadas em outros sistemas para IoT, seriam classificadas nas categorias de controle de potência, programação, e redução de dados a transmitir. Com relação ao consumo de energia, os métodos de controle de potência se concentrariam na adaptação dos níveis de potência de transmissão às condições variáveis no tempo do canal. Essas adaptações seriam realizadas usando relatório periódicos de medição de canal. Já as abordagens de programação reprogramariam operações temporizadas negociadas entre os dispositivos e a rede em relação aos modos de suspensão/ativação dos dispositivos, frequência de rastreamento para o relatório de posição do dispositivo e períodos de medição de canal para monitoramento ambiental. Essas operações seriam otimizadas dinamicamente com base nos recursos de mobilidade dos dispositivos aguardando condições mais favoráveis de transmissão. A abordagem de redução de dados visaria economizar energia, reduzindo a quantidade de dados desnecessários e de cabeçalho transmitidos. A agregação/compactação de dados (isto é, razão de transporte de dados) e codificação/roteamento eficazes (isto é, redução de processamento de cabeçalho) seriam bons exemplos de redução de dados.

O quadro 26 apresentou as tecnologias de segurança de dispositivos propostas no plano do BNDES para as quatro verticais.

Quadro 26 – Tecnologias de Segurança de Dispositivos Propostas

		Tecnologias de Segurança de Dispositivos									
	Aplicações	Criptografia embarcada	*Anti jamming*	*Anti tampering*	Assinatura digital	*Blockchain*	Controle de acesso	Falha segura	*Firmware* seguro	Ingresso seguro	Prevenção a DDoS
Cidades	Controle de tráfego	X	X	X			X	X	X	X	X
	Monitoramento - crimes									X	
	Monitoramento - vídeo						X		X		X
	Medidores inteligentes	X		X	X	X	X	X	X	X	X
	Iluminação inteligente						X	X	X	X	X
Saúde	Localização - ativos/pessoas										
	Monitoramento - diabetes	X									
	Diagnóstico descentralizado	X			X	X					
	Diagnóstico - Sepse										
	Controle de epidemias										
Rural	Monitoramento - Microclima										
	Gestão de pragas										
	Mon. comportamento animal										
	Mon. peso/alimentação animal						X	X	X		
	Gestão de saúde animal										
	Gestão desempenho máquinas										
	Produtividade dos trabalhos										
Indústrias	Manut. preditiva plataformas								X		
	Monitoramento - barragens										
	Mon. ativos de mineração										
	Gestão de estoque										
	Integração da planta produtiva										
	Engenharia - base em sensores	X			X		X	X	X		X

Fonte: Elaborado pelo autor.

Atzori (2010) reportou que a IoT seria extremamente vulnerável a ataques por vários motivos. Primeiro, frequentemente seus dispositivos passariam a maior parte do tempo sem vigilância e, portanto, seria fácil atacá-los fisicamente. Segundo, a maioria das comunicações é sem fio, o que torna a escuta extremamente simples. Finalmente, a maioria dos dispositivos IoT seria caracterizada por baixos recursos em termos de energia e computação (especialmente, os

componentes passivos) e, portanto, eles não poderiam implementar esquemas complexos de segurança. Mais especificamente, os principais problemas relacionados à segurança dizem respeito à autenticação e à integridade dos dados. A autenticação é difícil, pois geralmente requer infraestrutura e servidores de autenticação apropriados que atingem seu objetivo por meio da troca de mensagens apropriadas com outros nós. Na IoT, essas abordagens não são viáveis, uma vez que as etiquetas RFID passivas não podem trocar muitas mensagens com os servidores de autenticação. O mesmo raciocínio se aplica (de maneira menos restritiva) aos nós dos sensores. Esses argumentos são válidos, mas, de 2010 em diante, muitos avanços ocorrem na concepção das redes, na criptografia e na infraestrutura de acesso para autenticação.

4.5 Segurança de Dispositivos e Segurança da Informação

O quadro 27 apresentou uma relação entre as tecnologias de segurança de dispositivos propostas e os atributos de Segurança da Informação. Foram relacionados alguns comentários:

a) As tecnologias *anti jamming*, falha segura, e prevenção ao DDoS não atendem a confidencialidade e a integridade da informação já que estão relacionadas a interferências, funcionamento seguro do objeto e ataques à rede que visam indisponibilizar o serviço; o restante das tecnologias de segurança de dispositivo está relacionado a inviolabilidade dos dados e registro de usuários na rede e, portanto, atendem a confidencialidade e a integridade da informação;
b) As tecnologias que atendem a disponibilidade da informação são *anti jamming*, *anti tampering*, falha segura, firmware seguro e prevenção de DDoS pois procuram impedir ataques que desabilitem a capacidade de conexão da rede;
c) As tecnologias de segurança de dispositivo que não atendem a autenticidade da segurança da informação são *anti jamming*, falha segura e prevenção de DDoS; o restante das tecnologias está relacionado de alguma forma com o processo de autenticação e identificação dos dispositivos na rede;
d) O termo legalidade como atributo da Segurança da Informação tem uma conotação diferente da relacionada no quadro 25 que diz respeito a conectividade. Do ponto de vista de segurança de dispositivo, o uso legal da rede está relacionado a identificação dos dispositivos na rede, atendida pelas tecnologias assinatura digital, controle de acesso e acesso seguro. O restante das tecnologias de segurança de dispositivos não está relacionado a sua identificação na rede.

Quadro 27 – Segurança da Informação x Atributos da Segurança da Informação

		Atributos da Segurança da Informação				
		Confidencialidade	**Integridade**	**Disponibilidade**	**Autenticidade**	**Legalidade**
Tecnologias de Segurança de Dispositivos	**Criptografia embarcada**	**A**	**A**	**N**	**A**	**N**
	Anti jamming	**N**	**N**	**A**	**N**	**N**
	Anti tampering	**A**	**A**	**A**	**A**	**N**
	Assinatura digital	**A**	**A**	**N**	**A**	**A**
	Blockchain	**A**	**A**	**N**	**A**	**N**
	Controle de acesso	**A**	**A**	**N**	**A**	**A**
	Falha segura	**N**	**N**	**A**	**N**	**N**
	***Firmware* seguro**	**A**	**A**	**A**	**A**	**N**
	Ingresso seguro	**A**	**A**	**N**	**A**	**A**
	Prevenção ao DDoS	**N**	**N**	**A**	**N**	**N**

Legenda: A – atende, N – não atende.

Fonte: Elaborado pelo autor.

4.6 Conectividade e Segurança de Dispositivos

O quadro 28 fez um resumo de quais tecnologias de segurança de dispositivo seriam mais importantes no contexto de cada tecnologia de conectividade.

Quadro 28 – Importância de Segurança de Dispositivos para a Conectividade

		Tecnologias de Segurança									
		Criptografia embarcada	***Anti jamming***	***Anti tampering***	**Assinatura digital**	***Blockchain***	**Controle de acesso ao dispositivo**	**Falha segura**	***Firmware* seguro**	**Ingresso seguro à rede de**	**Prevenção de DDoS**
Tecnologias de Conectividade	**Redes Cabeadas**	**X**		**X**	**X**	**X**	**X**		**X**	**X**	**X**
	Redes Celulares		**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**
	LPWA		**X**	**X**				**X**	**X**		**X**
	Curto Alcance – Baixa banda		**X**	**X**		**X**					**X**
	Curto Alcance – Alta banda	**X**	**X**	**X**		**X**	**X**			**X**	**X**
	Redes *Ultra-Wide Band*			**X**			**X**			**X**	**X**
	Redes *Mesh*		**X**	**X**		**X**	**X**			**X**	**X**

Fonte: Elaborado pelo autor.

Seguiram-se alguns comentários sobre o quadro 28:

a) As tecnologias mais importantes para as redes cabeadas são aquelas que dificultam a invasão física da rede;
b) Considerando que os dispositivos IoT são frequentemente deixados desatendidos por longos períodos, as tecnologias que impedem a violação do dispositivo (*anti tampering*) são essenciais ao bom funcionamento dos sistemas;
c) Para as redes celulares, também são importantes as tecnologias que dificultam a invasão; considerando as técnicas de transmissão utilizadas, as tecnologias de criptografia não são fundamentais;

d) É preciso destacar a importância das técnicas que minimizam a interferência (*jamming*) em todas as redes sem fio;
e) Considerando o alcance das redes celulares e LPWA, as tecnologias de falha segura e *firmware* seguro procuram garantir a continuidade do provimento do serviço facilitando a manutenção da rede;
f) Os problemas apresentados anteriormente para redes de curto alcance e alta banda (Wi-Fi), confirmam a importância de criptografia mais robusta para essas redes e técnicas de controle de acesso;
g) Usualmente, as redes de curto alcance e baixa banda do tipo RFID não estão expostas a invasão devido à pequena cobertura e, portanto, não se pode considerar importante as técnicas de controle de acesso; essas redes têm necessidade de criptografia mais robusta, mas que não exijam muito poder de processamento; o *Blockchain* aparece como uma solução para esse caso;
h) Para as redes de curto alcance e baixa banda do tipo *Bluetooth Low Energy* – BLE e redes Mesh, a importância das tecnologias de segurança de dispositivo se assemelha mais com a das redes de curto alcance e alta banda com exceção da criptografia embarcada que demanda capacidade de processamento e, consequentemente, mais energia do dispositivo;
i) O modo de transmissão UWB em que o nível do sinal transmitido está pouco acima do nível de ruído do canal não chama atenção para técnicas de criptografia e disponibilidade; devido à ausência de qualquer dessas medidas, as técnicas de controle de acesso à rede assumem importância nessas redes;
j) A prevenção de ataques do tipo DDoS é essencial em todas as redes IoT devido ao potencial de danos considerando a quantidade de dispositivos que poderiam ser transformados em atacantes.

O quadro 29 totalizou as necessidades de cada tecnologia e suas capacidades locais para Conectividade e Segurança dos Dispositivos em todas as quatro verticais. Na Conectividade, destaca-se a importância das redes sem fio celulares e sistemas de curto alcance. As redes cabeadas aparecem com destaque devido à necessidade de conexão com a Internet e infraestruturas em nuvem que dão suporte às aplicações. Quanto à capacidade de atender às aplicações por atores locais, existem pontos de atenção em algumas tecnologias de conectividade, mas o resultado geral é bom. Já na segurança de dispositivos, a maior necessidade em todas as aplicações se concentrou em técnicas de controle de acesso e resiliência a falhas.

Quadro 29 – Necessidades e Capacidades para Conectividade e Segurança – Geral

	Tecnologias	Necessidades [%]				Capacidades
		25	50	75	100	
Conectividade	Redes cabeadas					S I C R
	Redes celulares					C S R I
	Redes Low Power Wide Area – LPWA					C S R I
	Redes de curto alcance e baixa banda					I C S R
	Redes de curto alcance e alta banda					C S R I
	Redes Ultra-Wide Band – UWB					I C S R
	Redes Mesh					C S R I
Segurança do dispositivo	Criptografia embarcada					C S R I
	Anti jamming					C S R I
	Anti tampering					C I R S
	Assinatura digital					C R S I
	Blockchain					C S R I
	Controle de acesso ao dispositivo					C S R I
	Falha segura					C S R I
	Firmware seguro					C R S I
	Ingresso seguro à rede de acesso					C S R I
	Prevenção à negação de serviço					C S R I

Legenda para Capacidades:

Status:

- **– Confiança;**
- **– Atenção;**
- **– Dificuldade.**

Verticais:

- **C – Cidades;**
- **S – Saúde;**
- **R – Rural;**
- **I – Indústria.**

Fonte: Elaborado pelo autor.

Por fim, cabe destacar que a literatura consultada indica problemas em redes IoT com relação a criptografia, e violação e interferência nos dispositivos, o que não aparece em destaque na totalização. O quadro de capacidades para a segurança de dispositivos é mais preocupante pois percebe-se a ausência de atores locais com aptidão em áreas consideradas necessárias.

5 TRABALHOS RELACIONADOS

Com relação a trabalhos que destacam a conectividade em IoT, foram encontrados dois documentos de interesse. Pitta (2018) propôs, em sua dissertação de mestrado, um mecanismo para a detecção da qualidade da conectividade utilizada em soluções IoT que necessitam um fluxo constante e ininterrupto de dados. Com maior foco em computação e arquitetura de rede, o autor desenvolveu uma aplicação de comunicação inovadora que prestaria um serviço pago de monitoramento constantemente redes IoT. Andreev *et al*. (2015) apresentaram um panorama da conectividade para IoT via rádio para dar suporte a comunicação M2M. Os autores fizeram uma revisão das tecnologias de transmissão via rádio mais recentes com mais atenção à tecnologia LTE. Esses autores destacaram que a comunicação M2M ou do tipo máquina foi identificada como um dos principais tópicos para aprimoramento adicional no 3GPP devido a uma diversidade de aplicativos e às correspondentes demandas dos consumidores.

Vale mencionar o trabalho de Pessoa & Branco Jr. (2016) que destaca o papel das telecomunicações em sistemas IoT principalmente na área de *Supply Chain Management* – SCM.

5.1 Ações de Governo

O BNDES (2017a) apresentou vários trabalhos governamentais de planejamento, apoio técnico e financeiro e outras atividades de fomento à IoT. Nesses trabalhos, observa-se que os Estados escolhem ou um papel mais ativo, como na Coréia do Sul, União Europeia, Japão, Cingapura e China, ou menos ativo, como na Rússia, Índia e Suécia. Há ainda países que atuariam pontualmente em questões relacionadas a IoT como Estados Unidos e Reino Unido. A atuação mais direta se daria em temas considerados chave, como privacidade e segurança, e em verticais em que seriam necessários investimentos expressivos como *smart energy* e cidades inteligentes.

O volume 1 do documento do BNDES destacou várias iniciativas apresentadas a seguir segmentadas por países ou blocos:

a) União Europeia:
   - *Digital Single Market* (DSM): organização política da Comissão Europeia que elabora leis e direciona financiamento para o setor de TIC e IoT;
   - *Alliance for IoT Innovation* (AIOTI): aliança que promove parcerias entre os setores público e privado, define estratégias de pesquisa em IoT e influencia a elaboração de políticas públicas;
   - *Horizon* 2020: principal programa Europeu de fomento à pesquisa e inovação (BNDES, 2017a);
b) Coreia do Sul:
   - *IoT Innovation Center*: tem como objetivo promover parcerias entre empresas nacionais e internacionais e oferecer apoio técnico, financeiro e treinamento para empresas e empreendedores;
   - *Korea IoT Association*: associação da indústria para promoção de novas tecnologias, difusão de serviços, treinamento da força de trabalho e organização de conferências internacionais (BNDES, 2017a);
c) Estados Unidos:
   - SMART (*Systems and Modeling for Accelerated Research in Transportation*) *Mobility Consortium*: criado pelo Departamento de Energia dos Estados Unidos, tem o objetivo de melhorar o entendimento dos impactos da energia e das alterações climáticas decorrentes dos futuros sistemas de mobilidade;
   - *Smart City Challenge*: concurso entre cidades americanas para o desenvolvimento de sistemas de transporte inteligente e interligado. Participaram 78 cidades e a vencedora, a cidade de Columbus em Ohio, recebeu uma dotação de US$ 40 milhões e alavancou outros US$ 350 milhões em fundos públicos e privados para a implantação dos projetos;
   - *White House Smart Cities Initiative*: programa de investimento da Casa Branca com orçamento superior a US$ 160 milhões para custeio de projetos nas áreas de mudanças climáticas, transporte e saúde além de infraestrutura para cidades inteligentes;
   - *Smart Manufacturing Innovation Institute*: parceria público-privada com foco na pesquisa e desenvolvimento de tecnologia para a manufatura inteligente;
   - *Smart Grid Investiment Grant Program*: programa de modernização dos sistemas de transmissão e distribuição de energia elétrica dos EUA (BNDES, 2017a);

d) Alemanha:
   - *High Tech Strategy*: Iniciativa multidisciplinar por meio de concessões não reembolsáveis para estimular a inovação e sua conversão em produtos, processos e serviços;
   - *Plattform Industrie* 4.0: Iniciativa para o engajamento de diversos atores na definição das políticas públicas para a indústria 4.0 incluindo o IoT (BNDES, 2017a);

e) Reino Unido:
   - IoTUK: Programa de investimento de US$ 40 milhões, lançado em 2015 para auxiliar os setores público e privado a desenvolverem capacidade em IoT;
   - Petras *Consortium*: consórcio de nove universidades com um orçamento de US$ 12 milhões para estudo de questões relacionadas a privacidade, ética, confiabilidade, aceitabilidade e segurança;
   - CityVerve *Project*: projeto de pesquisa e desenvolvimento da cidade de Manchester com dotação de US$ 12 milhões e que visa demonstrar a capacidade de IoT em saúde, transporte, energia e meio ambiente no contexto urbano;
   - *Health and Care Test Beds*: parceria com o *National Health Service* – NHS para que profissionais de saúde auxiliem na avaliação do uso de *wearables* no bem-estar e monitoramento de condições de pacientes em casa (BNDES, 2017a);

f) China:
   - *China IoT Technology Innovation Alliance*: agência criada pelo MITI – Ministério da Indústria e Tecnologia da Informação que tem o objetivo de estimular a cooperação entre governo, indústria, academia e outros atores para o desenvolvimento da IoT;
   - *Made in China 2025* (*Manufacturing 2025*): iniciativa do governo chinês inspirada no *Plattform Industrie* 4.0 alemão, visa conceber ações de planejamento e desenvolvimento da indústria manufatureira chinesa (BNDES, 2017a);

g) Japão:
   - *IoT Acceleration Consortium* (ITAC): consórcio criado pelo governo japonês que coordena as ações de diferentes atores e define áreas prioritárias de investimento;
   - *IoT Policy Committee*: comitê de governo que elabora políticas públicas relevantes para IoT;

- *New Industrial Structure Committee*: plano governamental em parceira com a Alemanha para definição de áreas de investimento com foco em manufatura avançada (BNDES, 2017a);

h) Índia:
   - *Digital India Programme*: programa do governo indiano que ambiciona transformar a Índia numa sociedade digital e que tem em seu escopo a criação de centros de incubação para IoT chamados de *National Centre of Excellence for IoT* – CoE-IoT;
   - *Smart Cities Project*: parte do programa anterior que almeja transformar cem cidades selecionadas em cidades inteligentes (BNDES, 2017a);

i) Cingapura:
   - *Smart Nation Singapore*: plano governamental que tem a IoT como elemento central que visa direcionar investimentos, formar parcerias com o setor privado, definir padrões e leis e capacitar profissionais para a área (BNDES, 2017a);

j) Suécia:
   - *Internet of Things Sverige*: principal programa do governo sueco em IoT cujo maior objetivo é reunir atores dos setores público e privado para alavancar a inovação em IoT (BNDES, 2017a);

k) Emirados Árabes Unidos:
   - *Dubai Smart City*: programa que busca desenvolver soluções inteligentes utilizando IoT para melhorar a qualidade de vida da população dentro da *Happiness Agenda* do governo de Dubai (BNDES, 2017a);

l) Rússia:
   - *Internet Initiatives Development Fund* (IIDF): fundo apoiado pelo governo russo, estatais e empresas privadas para o financiamento de tecnologias em TIC e IoT e que criou a *Internet of Things Association*, uma parceria com a *Bauman Moscow State Technical University* cujo objetivo é definir padrões e protocolos para IoT;
   - *Russian Association of Industrial Internet*: associação das empresas Rostelecom e Megafon, do setor de telecomunicações, Peter Service, da área de TI, Kaspersky, do segmento de segurança cibernética, e Rosseti, do setor de energia, para promover o mercado russo de IoT (BNDES, 2017a).

6 CONSIDERAÇÕES FINAIS

Essa dissertação discorreu sobre as propostas de conectividade contidas no documento ‘Internet das Coisas: Um Plano de Ação para o Brasil’ elaborado pelo BNDES em 2017 e que propôs um plano estratégico para a implantação de sistemas de Internet das Coisas no país para as verticais Cidades, Saúde, Meio Rural e Indústria. Além de descrever os sistemas propostos destacando as soluções de conectividade apresentadas, o trabalho apresentou uma visão sistêmica dessa conectividade e procurou verificar a aderência dessas propostas aos atributos de Segurança da Informação: Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade.

O trabalho se baseou em pesquisas em bibliotecas físicas e virtuais e bases de dados digitais elaborando uma revisão ampla, mas não exaustiva, sobre as tecnologias de conectividade e os atributos de Segurança da Informação além da análise do próprio documento do BNDES. A pesquisa teve um caráter exploratório, bibliográfico, documental e qualitativo e procurou seguir a teoria da Análise de Conteúdo de Bardin (2002) através da pré-análise do material, sua exploração e identificação, e o tratamento dos resultados pela sua interpretação e inferências.

O assunto IoT tem atraído muito interesse mundial devido ao impacto econômico estimado para 2025 de mais de US$ 11 trilhões em todo o globo e US$ 200 bilhões só no Brasil.

Foi discutido no trabalho que as aplicações IoT propostas trariam inúmeras vantagens sociais e econômicas para os ambientes públicos e privados nas verticais destacadas no plano do BNDES. Nas Cidades, a implantação de soluções IoT propostas trariam benefícios no transporte, segurança e eficiência energética com ganho estimado de US$ 27 bilhões até 2025. Na Saúde, os benefícios da implantação das aplicações propostas estariam na melhoria da qualidade de vida da população em geral pelo combate mais efetivo a epidemias e melhor atendimento no serviço público advindo do aumento da eficiência das unidades de saúde. Estimou-se ganhos de até US$ 39 bilhões até o horizonte de 2025. Previu-se ganhos em produtividade, redução de custos com insumos, e melhoria da competitividade no Meio Rural com ganho estimado até 2025 de até US$ 21 bilhões. E na Indústria, com soluções para fábricas e indústria de base e seus processos, estimou-se um ganho de até 37 bilhões no mesmo horizonte. Todo o plano traria um ganho estimado total de até US$ 124 bilhões até 2025.

Além dos benefícios diretos das aplicações IoT nessas verticais, outros ganhos indiretos poderiam ser destacados: melhoria da qualidade de vida e segurança nas cidades e no campo,

melhoria das condições de trabalho e maior cobertura de serviços de telecomunicações em geral. O que se pôde perceber na análise das aplicações propostas foi uma superposição de soluções de conectividade ou seja, uma mesmo sistema de comunicação serviria a várias aplicações propostas.

Deduziu-se dessa dissertação que essas soluções também poderiam alavancar outras aplicações. Por exemplo, a infraestrutura de redes celular e *Low Power Wide Area* – LPWA proposta na vertical Cidades para aplicações de controle de tráfego, segurança pública e gestão de energia poderiam impulsionar soluções para proteção contra vandalismo de outros ativos públicos (praças, sinalização, parques), controle de inundações e outras ações relacionadas a defesa civil ou sistemas de informação sobre o transporte público como o horário de chegada de ônibus aos seus pontos de parada. O uso de *smart tags* nas unidades de saúde proposto na vertical Saúde poderia fomentar aplicações de rastreio de medicamentos e identificação de pacotes nos centros de distribuição hospitalar. As propostas na vertical Meio Rural certamente melhorariam a comunicação de voz e acesso à Internet nesse ambiente. E as propostas de monitoramento e gestão propostas na vertical Indústrias poderiam auxiliar a implantação de outras aplicações em diversos setores para automatização de trabalhos monótonos e repetitivos com consequente melhoria das condições de trabalho.

Uma das preocupações apresentadas no plano do BNDES ‘Internet das Coisas: Um Plano de Ação para o Brasil’ destacada nesse trabalho foi a falta de mão de obra especializada. Nas tecnologias de Conectividade, a capacidade dos atores está razoavelmente resolvida com alguns pontos de atenção específicos para determinadas tecnologias. Mas, na Segurança de Dispositivos existem várias tecnologias com carência de capacidade o que representa oportunidade para profissionais e empreendedores. Essas conclusões estão bem destacadas no quadro 29 desse trabalho. Além disso, o interesse atual pela temática de IoT pôde ser observado pelo aumento do número de atores ofertantes de TIC. Esse interesse não significa necessariamente que as necessidades de cada vertical vão ser atendidas.

Foi realizada uma análise sistêmica das soluções de Conectividade propostas sob o ponto de vista dos atributos da Segurança da Informação que destacou algumas questões inerentes às tecnologias utilizadas. Quanto ao meio de transmissão de sinais utilizado, tanto redes cabeadas como redes sem fio poderiam ser invadidas o que comprometeria diretamente a confidencialidade e integridade da comunicação. Dentre as cabeadas, as redes ópticas seriam mais seguras devido à dificuldade de inserção e retirada do sinal óptico direto da fibra. Por

usarem um meio não confinado, as redes sem fio seriam mais vulneráveis considerando que área de operação da rede alcance o invasor. O uso de técnicas de controle de acesso e identificação de usuários, técnicas ligadas ao atributo autenticidade na Segurança da Informação, minimizaria essas vulnerabilidades em ambas as redes.

Concluiu-se do trabalho que, nas redes sem fio, as modernas tecnologias digitais de transmissão e multiplexação de sinais utilizadas em sistemas celulares, redes Wi-Fi, LPWA, *Bluetooth* e UWB – *Ultra-Wide Band* dificultariam a invasão seja pela codificação do sinal transmitido ou pelo seu espalhamento no espectro radioelétrico o que exigiria equipamento de comunicação sofisticado para a sua interceptação. Entretanto, o uso de frequências não licenciadas e equipamentos fabricados em série como para BLE – *Bluetooth Low Energy* e Wi-Fi aumentariam os riscos de invasão pelo amplo conhecimento dos protocolos de comunicação e disponibilidade de equipamentos. O uso de técnicas de criptografia tanto em redes cabeadas como em redes sem fio poderia garantir a confidencialidade, integridade e autenticidade da comunicação. Entretanto, alguns dispositivos (RFID – *Radio-Frequency IDentification* e NFC – *Near Field Communication*) geralmente não suportariam essas técnicas devido ao elevado poder de processamento e consumo de energia necessário.

O atributo disponibilidade da Segurança da Informação foi estudado considerando o tipo de meio utilizado. Devido às questões de propagação de sinais e interferência, foi considerado que as redes em fio não poderiam garantir o bom desempenho nesse atributo. No caso da interferência, considerou-se tanto aquelas naturais, quanto as maliciosas e até as advindas do excesso de dispositivos na mesma faixa de frequência do sistema.

Foram citadas nessa dissertação as tecnologias de segurança utilizadas nos dispositivos IoT. Constatou-se que essas tecnologias teriam uma relação de dependência recíproca com a concepção do sistema, o que influenciaria diretamente aspectos como dimensão e peso do dispositivo, sua faixa de frequência, capacidade de processamento, necessidade de energia e custo. As tecnologias de segurança que apareceram em destaque foram controle de acesso ao dispositivo e *firmware* seguro. Também se destacou no plano do BNDES e nas fontes consultadas a prevenção de ataques do tipo DDoS – *Distributed Denial of Service* já que as redes IoT teriam muitos dispositivos o que potencializaria esse tipo de ataque.

No levantamento de trabalhos relacionados ao tema, verificou-se a preocupação tanto de países do primeiro mundo como das economias emergentes com projetos de IoT. Tal se justificaria

considerando um impacto estimado global de US$ 11 trilhões dessa tecnologia. Foram listados vários trabalhos na etapa de planejamento, programas de investimento, projetos-piloto e sistemas já implantados.

O estudo desse tema foi relevante na medida que contribuiu para apresentar as propostas de IoT concebidas para o Brasil, estudar suas características e conjuntura sob a luz da Segurança da Informação verificando o alinhamento e evidenciando pontos de atenção, além de destacar desafios e oportunidades. Foi possível ainda, tangenciar as questões sociais e econômicas que envolvem a inclusão da 'inteligência' no ambiente cotidiano por esses sistemas.

Especificamente, o trabalho contribui com:

a) Uma visão geral da conectividade proposta para sistemas IoT no Brasil;
b) A discussão sobre as características das propostas de conectividade e questões relacionadas a comunicação para sistema IoT;
c) Uma análise qualitativa e sistêmica das propostas de conectividade e sua aderência aos atributos da Segurança da Informação;
d) Uma discussão sobre a segurança dos dispositivos IoT e seu impacto nas características desses dispositivos;
e) O conhecimento do ambiente IoT no Brasil e as ideias em estudo nesse ambiente.

O plano do BNDES poderia ser usado como base para vários outros estudos sobre Internet das Coisas tanto técnicos como sociais. Na área técnica, poderiam ser concebidas outras aplicações com base nas que foram propostas. Poderiam ainda serem realizados estudos semelhantes a essa dissertação, mas com o foco no uso de dispositivos IoT e suporte às aplicações propostas. Na área social, o plano do BNDES poderia ser usado como exemplo em estudos em que se discute o papel do estado no fomento e regulamentação da tecnologia e seu impacto na qualidade de vida e atividade econômica tanto pública quanto privada.

Outros trabalhos não relacionados diretamente com o documento do BNDES, mas com sistemas IoT poderiam fazer uma avaliação no tráfego de dados a ser inserido nas diversas redes considerando a entrada de grande quantidade de dispositivos previstas nas aplicações IoT e seu impacto nos sistemas de telecomunicação e de transmissão de dados, no uso do espectro radioelétrico, na arquitetura de informação e nos ambientes em nuvem para processamento e armazenagem. Outra questão de estudo interessante seria avaliar o impacto em BI – *Business Intelligence* que a captura automática de dados via IoT provocaria.

O trabalho se justificou ao avaliar a aderência das propostas de conectividade para IoT no Brasil aos atributos da Segurança da Informação e levantar características e pontos de atenção nesse contexto. O estudo de tecnologias que façam a aquisição automática de dados, transformando-os em informações e conhecimento, é de grande importância notadamente se considerarmos as demandas de segurança no ambiente das Cidades, a criticidade e urgência das informações de Saúde e os impactos econômicos desses sistemas no Meio Rural e na Indústria. Contribuem para a complexidade desses sistemas o volume de dados esperados e a diversidade de ambientes em que essas informações são necessárias. A diversidade de atores, tecnologias e métodos de aquisição, transmissão e processamento desses dados terminam por montar o contexto das aplicações em IoT.

REFERÊNCIAS

ABINC. História. **ABINC**, 2019. Disponível em <https://abinc.org.br/abinc/>. Acesso em 15 out. 2019.

ABNT NBR ISO/IEC 27002, 2005. **ABNT Catalogo**. Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=385777>. Acesso em 13 jan. 2020.

ANDREEV, S.; GALININA, O.; PYATTAEV, A.; *et al*. Understanding the IoT connectivity landscape: a contemporary M2M radio technology roadmap. **IEEE Communications Magazine**, v. 53, n. 9, p. 32–40, 2015.

ASHTON, K. That 'Internet of Things' thing. **RFID Journal**, June, 2009. Disponível em: <http://www.rfidjournal.com/articles/view?4986>. Acesso em 19 mai. 2016.

ATZORI, L.; IERA, A.; MORABITO, G. The Internet of Things: A survey. **Computer Networks**, p. 19, 2010. Disponível em <https://s2.smu.edu/~eclarson/teaching/ubicomp/papers/iot_survey.pdf>. Acesso em 15 out 2019.

BAARS, H; HINTZBERGEN, K.; HINTZBERGEN, J.; SMULDERS, A. Fundamentos de Segurança da Informação, com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018. Disponível em: < https://plataforma.bvirtual.com.br/Leitor/Publicacao/160044/pub>. Acesso em 14 out. 2019.

BHAGWAT, P. Bluetooth: technology for short-range wireless apps. **IEEE Internet Computing**, v. 5, n. 3, p. 96–103, 2001.

BARDIN, L. **Análise de conteúdo**. Lisboa: Edições 70, 2002.

BASSI, A.; HORN, G. Internet of Things in 2020: Roadmap for the future. **Internet of Things**, p. 27, 2008. Disponível em: <https://docbox.etsi.org/erm/Open/CERP%2020080609-10/Internet-of-Things_in_2020_EC-EPoSS_Workshop_Report_2008_v1-1.pdf>. Acesso em 15 out 2019.

BAUER, M.; GASKELL, G. **Pesquisa Qualitativa com Texto, Imagem e Som**. Um manual prático. 7. ed. Petrópolis: Editora Vozes, 2002.

BEGISHEV, V.; PETROV, V.; SAMUYLOV, A.; *et al*. Resource allocation and sharing for heterogeneous data collection over conventional 3GPP LTE and emerging NB-IoT technologies. **Computer Communications**, v. 120, p. 93–101, 2018.

BNDES. Benchmark de iniciativas e políticas públicas. *In*: **Internet das Coisas: um plano de ação para o Brasil**. Brasília: BNDES, 2017a, v. 1, p. 227. 14v. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/48fff464-7a3c-442b-98c3-aa4634ad08d8/Relatorio-de-benchmark-fase-1-20170516_Produto_Frente_1_Benchmark_ENTREGA_FORMAL_FinalRevisado.pdf?MOD=AJPERES&CVID=lNGCXmw>. Acesso em: 3 set. 2019.

BNDES. Roadmap tecnológico - Sumário. *In*: **Internet das Coisas: um plano de ação para o Brasil**. Brasília: BNDES, 2017b, v. 2A, p. 30. 14v. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/1970e8af-33d4-48a5-9522-d6335c931e26/170614_Produto_Parcial_Frente+2_Sumario_Executivo_Roadmap_Final.pdf?MOD=AJPERES&CVID=lOOitOz>. Acesso em: 3 set. 2019.

BNDES. Análise de oferta e demanda - Delimitação de verticais de aplicação de Internet das Coisas. *In*: **Internet das Coisas: um plano de ação para o Brasil**. Brasília: BNDES, 2017c, v. 3B, p. 32. 14v. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/91fa1f24-dd58-4747-8e8e-54b9e716ff50/170609_Prroduto_Parcial_Frente+3_Delimitacao_Verticais_Final.pdf?MOD=AJPERES&CVID=lOOig1Q>. Acesso em: 3 set. 2019.

BNDES. Relatório de entrevistas e pesquisas - Fase II. *In*: **Internet das Coisas: um plano de ação para o Brasil**. Brasília: BNDES, 2017d, v. 4B, p. 50. 14v. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/f9dc4f85-5a94-4ee2-aa21-921ea30d7b13/relatorio-de-entrevistas-e-pesquisas-fase-2-produto-4b.pdf?MOD=AJPERES&CVID=lR.kH06>. Acesso em: 3 set. 2019.

BNDES. Internet das Coisas: um plano de ação para o Brasil - Relatório final da priorização de verticais e horizontais. *In*: **Internet das Coisas: um plano de ação para o Brasil**. Brasília: BNDES, 2017e, v. 6, p. 139. 14v. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/9cc660de-bb54-408a-a7e9-322f5dbc3f03/Produto+6_Relat%C3%B3rio_Final_Prioriza%C3%A7%C3%A3o_v1_atualizado.pdf?MOD=AJPERES&CVID=m0SUIir>. Acesso em: 3 set. 2019.

BNDES. Aprofundamento de Verticais - Cidades. *In*: **Internet das Coisas: um plano de ação para o Brasil**. Brasília: BNDES, 2017f, v. 7A, p. 68. 14v. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/776017fa-7c4a-43db-908f-c054639f1b88/relatorio-aprofundamento+das+verticais-cidades-produto-7A.pdf?MOD=AJPERES&CVID=m3rPg5Q>. Acesso em: 3 set. 2019.

BNDES. Aprofundamento de Verticais - Saúde. *In*: **Internet das Coisas: um plano de ação para o Brasil**. Brasília: BNDES, 2017g, v. 7B, p. 64. 14v. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/9e481a5b-a851-4895-ba7f-aa960f0b69a6/relatorio-aprofundamento-das-verticais-saude-produto-7B.pdf?MOD=AJPERES&CVID=m3mTltg>. Acesso em: 3 set. 2019.

BNDES. Aprofundamento de Verticais - Rural. *In*: **Internet das Coisas: um plano de ação para o Brasil**. Brasília: BNDES, 2017h, v. 7C, p. 63. 14v. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/2fa8f7d1-9939-441d-b8ce-ed3459fcfd4d/relatorio-aprofundamento-das-verticais-rural-produto-7C.pdf?MOD=AJPERES&CVID=m3rPopG>. Acesso em: 3 set. 2019.

BNDES. Aprofundamento de Verticais - Indústrias. *In*: **Internet das Coisas: um plano de ação para o Brasil**. Brasília: BNDES, 2017i, v. 7D, p. 60. 14v. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/cfbd69ff-56d7-43f4-82df-f05b40459ec7/relatorio-aprofundamento-das-verticais-industria-produto-7D.pdf?MOD=AJPERES&CVID=m3xwf3m>. Acesso em: 3 set. 2019.

BNDES. Relatório do Plano de Ação - Iniciativas e Projetos Mobilizadores. *In*: **Internet das Coisas: um plano de ação para o Brasil**. Brasília: BNDES, 2017j, v. 8A, p. 65. 14v. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/269bc780-8cdb-4b9b-a297-53955103d4c5/relatorio-final-plano-de-acao-produto-8-alterado.pdf?MOD=AJPERES&CVID=m0jDUok>. Acesso em: 3 set. 2019.

BNDES. Relatório Final do Estudo. *In*: **Internet das Coisas: um plano de ação para o Brasil**. Brasília: BNDES, 2018, v. 9A, p. 95. 14v. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/d22e7598-55f5-4ed5-b9e5-543d1e5c6dec/produto-9A-relatorio-final-estudo-de-iot.pdf?MOD=AJPERES&CVID=m5WVIld>. Acesso em: 3 set. 2019.

CHIZZOTTI, A. **Pesquisa em ciências humanas e sociais**. 2. ed. São Paulo: Cortez, 2006.

COELHO, P. E. **Projeto de Redes Locais com Cabeamento Estruturado**. Belo Horizonte: P. E. Coelho, 2003.

ČOLAKOVIĆ, A.; HADŽIALIĆ, M. Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. **Computer Networks**, v. 144, p. 17–39, 2018.

CRESWELL, J. W. **Projeto de pesquisa: métodos qualitativo, quantitativo e misto**. 2. ed. Porto Alegre: Artmed, 2007.

DAVENPORT, T. H. **Ecologia da Informação**. São Paulo: Futura, 1998.

DAO, N.; PARK, M.; KIM, J.; *et al*. Adaptive MCS selection and resource planning for energy-efficient communication in LTE-M based IoT sensing platform. **PLOS ONE**, v. 12, n. 8, p. e0182527, 2017.

DIVIS, D. FCC Weighs Broad Changes in Ultra-Wideband Rules. **Inside GNSS**, 8 ago. 2019. Disponível em: <https://insidegnss.com/fcc-weighs-broad-changes-in-ultra-wideband-rules/>. Acesso em: 21 nov. 2019.
DOJOT. Sobre o Dojot. **DOJOT**, 2019. Disponível em <http://www.dojot.com.br/sobre-a-dojot-iot/>. Acesso em 15 out. 2019.

DURAND, T. G.; VISAGIE, L.; BOOYSEN, M. J. Evaluation of next-generation low-power communication technology to replace GSM in IoT-applications. **IET Communications**, v. 13, n. 16, p. 2533–2540, 2019.

FLEISCH, E. What is the internet of things? **An economic perspective. Economics, management, and financial markets**, 5 (2) (2010), pp. 125-157. 2010.

FLICK, U. **Introdução à pesquisa qualitativa**: um guia para iniciantes. Porto Alegre: Penso, 2013.

FOERSTER, J.; GREEN, E.; SOMAYAZULU, S.; *et al*. Ultra-Wideband Technology for Short- or Medium-Range Wireless Communications. **Intel Technology Journa**l, Q2, (2001) p. 11, 2001.

FONTES, E. **Segurança da Informação**: o usuário faz a diferença. São Paulo: Saraiva, 2010. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788502122185/cfi/4!/4/4@0:9.07>. Acesso em 14 out. 2019.

FORTE, A. G.; WANG, W.; VELTRI, L.; *et al*. A Next-Generation Core Network Architecture for Mobile Networks. **Future Internet**, v. 11, n. 7, p. 152, 2019.

FREIRE, R. F. P.; SILVA, H. C. C.; QUEIROZ, R. G.; *et al*. O fator humano como uma vulnerabilidade em segurança da informação. **Revista Brasileira de Administração Científica**, v. 8, n. 3, p. 146–157, 2017.

FUMEC. **Regulamento do Curso de Mestrado Profissional em Sistemas de Informação e Gestão do Conhecimento**, 2017. Disponível em: <http://ppg.fumec.br/sigc/wp-content/uploads/2013/03/mestrado-20170602.pdf>. Acesso em 07 abr. 2019.

FUMEC. **Pós-Graduação em Sistemas de Informação e Gestão do Conhecimento: Trilhas de Pesquisa**, 2019. Disponível em: <http://ppg.fumec.br/sigc/pesquisa/trilhas-de-pesquisa/>. Acesso em 07 abr. 2019.

GALOV, N. 77+ Big Data Stats for the Big Future Ahead. **Hostingtribunal.com Blog**, 2019. Disponível em: <https://hostingtribunal.com/blog/big-data-stats/>. Acesso em: 29 nov. 2019.

GOOGLE ACADÊMICO. Busca pelas strings: 'IoT'. **Google**, 2019. Disponível em: <https://scholar.google.com.br>. Acesso em 13 dez. 2017 e 27 mar. 2019.

GONÇALVES, C. A.; MEIRELLES, A. M. **Projetos e Relatórios de Pesquisa em Administração**. São Paulo: Atlas, 2004.

GUBBI, J., BUYYA, R., MARUSIC, S.; PALANISWAMI, M. Internet of Things: A vision, architectural elements and future directions. **Future Generation Computer Systems**, 29(7), 1645-1660, 2013. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167739X13000241>. Acesso em 6 jun. 2016.

GUIMARÃES, D. A.; SOUZA, R. A. A. **Transmissão Digital**: princípios e aplicações. São Pulao: Erica, 2012.

HA, D.; SCHAUMONT, P. Replacing Cryptography with Ultra-Wide band (UWB) Modulation in Secure RFID. In: **2007 IEEE International Conference on RFID**. Grapevine, Texas, USA: IEEE, 2007, p. 23–29. Disponível em: <http://ieeexplore.ieee.org/document/4143506/>. Acesso em: 21 nov. 2019.

HAYKIN, S.; MOHER, M. **Sistemas Modernos de Comunicação Wireless**. Porto Alegre: Bookman, 2008a.

HAYKIN, S.; MOHER, M. **Introdução a Sistemas de Comunicação Wireless**. 2ª. ed. Porto Alegre: Bookman, 2008b.

HELP NET SECURITY. Number of connected devices reached 22 billion, where is the revenue? **Help Net Security**, 2019. Disponível em: <https://www.helpnetsecurity.com/2019/05/23/connected-devices-growth/>. Acesso em 22 out. 2019.

IOT ANALYTICS. Who we are and how we do IoT market research. **IoT Analytics**, 2017. Disponível em: <https://iot-analytics.com/about/>. Acesso em 15 out. 2019.

IKPEHAI, A.; ADEBISI, B.; RABIE, K. M.; *et al*. Low-Power Wide Area Network Technologies for Internet-of-Things: A Comparative Review. **IEEE Internet of Things Journal**, v. 6, n. 2, p. 2225–2240, 2019.

IoT ONE. IoT ONE 500 Industrial IoT Companies. **IoT ONE Insights**, 2018. Disponível em: <
https://www.iotone.com/files/pdf/newhome/IoT%20ONE%20500%20&%20IoT%20ONE%2010%20(2018)%20-%20Top%20Industrial%20IoT%20Companies.pdf>. Acesso em 8 out. 2019.

IS0 27000, 2005. **International Organization for Standardization, ISO**. Disponível em: <http://www.iso.org/cms/render/live/en/sites/isoorg/home.html>. Acesso em 13 jan. 2020.

ITU-T. Overview of the Internet of Things, **Recommendation ITU-T**, Y.2060, 06/2012. Disponível em <https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-E&type=items>. Acesso em: 22 out. 2019.

KUROSE, J. F.; ROSS, K. W. **Computer Networking**. A Top-Down Approach Featuring the Internet. 2. ed. Amsterdam: Addison Wesley Longman, 2003.
LOHR, S. The Age of Big Data. **The New York Times**, New York, 11 fev. 2012. Disponível em: <
https://s3.amazonaws.com/academia.edu.documents/34393761/2_The_New_York_Times_on_The_Age_of_Big_Data.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1515880216&Signature=0jImomLmi8K%2FXvcXbAL%2BpGorM34%3D&response-content-disposition=inline%3B%20filename%3D2_The_New_York_Times_on_The_Age_of_Big_D.pdf>. Acesso em 8 jan. 2018.

MANOEL, S. S. **Governança de Segurança da Informação**: Como criar oportunidades para o seu negócio. Rio de Janeiro: Brasport, 2014. Disponível em: < https://plataforma.bvirtual.com.br/Leitor/Publicacao/160684/epub>. Acesso em 20 out. 2019.

MANYIKA, J.; CHUI, M.; BROWN, B.; BUGHIN, J.; DOBBS, R.; ROXBURGH, C.; BYERS, A. H. Big data: The next frontier for innovation, competition, and productivity. **McKinsey Global Institute**, mai. 2011. Disponível em: < https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_full_report.ashx>. Acesso em 8 jan. 2018.

MANYIKA, J.; CHUI, M.; BISSON, P.; *et al*. Unlocking the potential of the Internet of Things. **McKinsey Global Institute**, jun. 2015a. Disponível em: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>. Acesso em 8 out. 2019.

MANYIKA, J.; CHUI, M.; BISSON, P.; *et al*. The Internet of Things: Mapping the value beyond the hype. **McKinsey Global Institute**, jun. 2015b. Disponível em: <https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.ashx>. Acesso em 8 out. 2019.

McAFEE, A.; BRYNJOLFSSON, E. Big Data: The Management Revolution. **Harvard Business Review**, out. 2012. Disponível em: < http://tarjomefa.com/wp-content/uploads/2017/04/6539-English-TarjomeFa-1.pdf>. Acesso em 8 jan. 2018.

MERKER, J. CPqD lança plataforma aberta de IoT. **Baguete**, 13 dez. 2017. Disponível em: <https://www.baguete.com.br/noticias/13/09/2017/cpqd-lanca-plataforma-aberta-de-iot>. Acesso em 13 dez. 2017.

MINGERS, J. Combining IS research methods: towards a pluralist methodology. **Information Systems Research**. V.12, n.3, p.240-259. Set. 2001.

MIGLIACCI, P. Companhias investem em internet das coisas para otimizar processos. **Folha de São Paulo**, São Paulo, 3 jul. 2017. Disponível em: <http://www1.folha.uol.com.br/mercado/2017/07/1897879-companhias-investem-em-internet-das-coisas-para-otimizar-processos.shtml>. Acesso em 13 dez. 2017.

MOZZATO, A. R.; GRZYBOVSKI, D. Análise de conteúdo como técnica de análise de dados qualitativos no campo da Administração: potencial e desafios. **Revista de Administração Contemporânea**, v.15, n.4, p.731. 2011.

OLIVEIRA, F. Projetos de internet das coisas serão testados em ‘minicidade’ no Rio. **Folha de São Paulo**, São Paulo, 13 set. 2017. Disponível em: <http://www1.folha.uol.com.br/mercado/2017/09/1917925-projetos-de-internet-das-coisas-serao-testados-em-minicidade-no-rio.shtml>. Acesso em 13 dez. 2017.

PACHECO, F. B.; KLEIN, A. Z.; RIGHI, R. R. Modelos de negócio para produtos e serviços baseados em internet das coisas: uma revisão da literatura e oportunidades de pesquisas futuras. **REGE – Revista de Gestão**, 14 mai. 2016. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1809227616300054>. Acesso em 8 jan. 2018.

PESSOA, C. R. M.; BRANCO JR, M. R. F. A Telecommunications Approach in Systems for Effective Logistics and Supply Chains. **Handbook of Research on Information Management for Effective Logistics and Supply Chains**. Hershey, PA: IGI Global, cap. 23, p. 437-452, 2016.

PITTA, L. G. O. **Uma abordagem para o problema de conectividade em plataformas multilaterais de IoT**. Dissertação (Mestrado em Informática) – Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2018. Disponível em: <http://www.maxwell.vrac.puc-rio.br/Busca_etds.php?strSecao=resultado&nrSeq=34618@1>. Acesso em: 28 nov. 2019.

QIN, Z.; LI, F.Y.; LI, G. Y.; et al. Low-Power Wide-Area Networks for Sustainable IoT. **arXiv:1810.10761 [cs, math]**, 2018. Disponível em: <http://arxiv.org/abs/1810.10761>. Acesso em: 12 nov. 2019.

RIBEIRO, J. A. J. **Comunicações Ópticas**. 7. ed. São Paulo: Érica, 2005.

SCHULTZ, J. How Much Data is Created on the Internet Each Day**? Micro Focus Blog**, jul. 2019. Disponível em: <https://blog.microfocus.com/how-much-data-is-created-on-the-internet-each-day/>. Acesso em: 29 nov. 2019.

SHAH, S. K.; CORLEY, K. G. Building better theory by bridging the quantitative-qualitative divide. **Journal of Management Studies**, 43(8), 1821-1835. Doi: 10.1111/j.1467-6486.2006.00662.x. 2006.

SILVA, A. M.; PINTO, M. M. G. A. Um modelo sistémico e integral de gestão da informação nas organizações. 2005. **Repositório Aberto da Faculdade de Letras da Universidade do Porto**. Disponível em: <https://repositorio-aberto.up.pt/handle/10216/13461>. Acesso em: 10 jan. 2020.

SILVA, A. M. Mediações e mediadores em Ciência da Informação. **PRISMA.COM**, v. 0, n. 9, p. 68–104, 2009. Disponível em: <http://ojs.letras.up.pt/index.php/prismacom/article/view/2057>. Acesso em 10 jan. 2020.

SUNDMAEKER, H.; GUILLEMIN, P.; FRIESS, P.; WOELFFLÉ, S. Vision and challenges for realizing the Internet of Things. **Cluster of European Research Projects on the Internet of Things—CERP IoT**, 2010. Disponível em: <https://www.researchgate.net/publication/228664767_Vision_and_Challenges_for_Realizing_the_Internet_of_Things>. Acesso em 8 jan. 2018.

TANENBAUM, A. S. **Computer Networks**. 4a. ed. New Jersey: Prentice Hall, 2003.

VROOM, C.; VON SOLMS, R. Towards information security behavioral compliance. **Computers & Security**, v. 23, n. 3, p. 191–198, 2004.

WANT, R. An Introduction to RFID Technology. **Pervasive Computing**, Jan-Mar 2006. Disponível em <https://www.computer.org/csdl/magazine/pc/2006/01/b1025/13rRUxlgxLD>. Acesso em: 22 nov. 2019.

Apêndice 1

O método inicial de pesquisa, realizado entre os dias 13.12.2017 e 20.01.2018, caracterizou-se pela busca em bases de dados *online* por arquivos sobre aspectos de hardware e software de arquiteturas de informação que utilizam Internet das Coisas e que seriam mais adequados para gestão de informações de saúde humana, arquivos esses classificados geralmente por relevância. A pesquisa foi feita na Sala de Estudos do Programa de Pós-Graduação Fumec que permite uma maior quantidade de respostas e em diferentes bases de dados. Os resultados são apresentados nos quadros 30 e 31

Quadro 30 – Resultados da primeira pesquisa 1/2

	Número de resultados	**Resultados considerados**	**Baixados diretamente**	**Sem conseguir acesso**	**Sem interesse**
Base: Google Acadêmico. **String: 'IoT' + 'saude'**	**2.500**	**10**	**4**	**0**	**6**
Base: Google Acadêmico. **String: *'IoT' + 'health'***	**60.200**	**10**	**2**	**6**	**2**
Base: Google Acadêmico. **String: 'IoT' + 'casa' + 'dispositivos'**	**1.890**	**20**	**4**	**0**	**16**
Base: Google Acadêmico. **String: '*smarthome*' + '*devices*'**	**2.870.000**	**20**	**1**	**4**	**15**
Base: Google Acadêmico. **String: '*big data*'**	**4.910.000**	**10**	**3**	**1**	**6**
Base: EBSCO. **String: 'IoT' + 'saúde'**	**1**	**1**	**1**	**0**	**1**
Base: EBSCO. **String: 'IoT' + '*health*'**	**264**	**10**	**8**	**2**	**8**
Base: EBSCO. **String: 'IoT' + 'casa'**	**6**	**6**	**6**	**0**	**6**
Base: EBSCO. **String: 'IoT' + 'dispositivos'**	**8**	**8**	**8**	**0**	**8**

Fonte: Elaborado pelo autor.

Quadro 31 – Resultados da primeira pesquisa 2/2

	Número de resultados	**Resultados considerados**	**Baixados diretamente**	**Sem conseguir acesso**	**Sem interesse**
Base: EBSCO. **String: '*smarthome*' + '*devices*'**	**14**	**14**	**13**	**1**	**13**
Base: EBSCO. **String: '*big data*'**	**12.126**	**20**	**20**	**0**	**20**
Base: Periódicos CAPES. **String: 'IoT' + 'saúde'**	**23**	**10**	**10**	**0**	**9**
Base: Periódicos CAPES. **String: 'IoT' + '*health*'**	**6.103**	**10**	**9**	**1**	**9**
Base: Periódicos CAPES. **String: 'IoT' + 'casa'**	**90**	**30**	**30**	**0**	**30**
Base: Periódicos CAPES. **String: 'IoT' + 'dispositivos'**	**58**	**58**	**58**	**0**	**58**
Base: Periódicos CAPES. **String: '*smarthome*' + '*devices*'**	**142**	**30**	**27**	**3**	**27**
Base: Periódicos CAPES. **String: '*big data*'**	**1.105.686**	**10**	**9**	**1**	**9**
Base: ScienceDirect. **String:** 'IoT' + 'saúde'	**21**	**10**	**10**	**0**	**10**
Base: ScienceDirect. **String:** 'IoT' + '*health*'	**3.923**	**10**	**10**	**0**	**10**
Base: ScienceDirect. **String:** 'IoT' + 'casa'	**136**	**30**	**29**	**1**	**27**
Base: ScienceDirect. **String:** 'IoT' + 'dispositivos'	**101**	**30**	**30**	**0**	**29**
Base: ScienceDirect. **String:** '*smarthome*' + '*devices*'	**169**	**10**	**9**	**1**	**8**
Base: ScienceDirect. **String:** '*big data*'	**588.400**	**10**	**8**	**2**	**6**

Fonte: Elaborado pelo autor.

Procedeu-se à leitura exploratória do resumo, introdução e conclusões dos 19 arquivos selecionados acima. Após essa leitura, foram estudados 8 textos que seriam utilizados na elaboração desse trabalho nesse contexto e também considerados 4 artigos de conhecimento prévio do autor, 1 capitulo de livro de sua coautoria sobre o assunto, totalizando 13 textos ao final.

Apêndice 2

Nesse novo contexto, o projeto de dissertação manteve a mesma orientação metodológica, embora tenha ocorrido alteração no objetivo geral, nos tópicos a serem desenvolvidos na fundamentação teórica e, consequentemente, nas fontes de informações a serem abordadas e seus inter-relacionamentos. O trabalho focou então em conceitos de IoT, arquitetura de informação e contexto nacional para a área de saúde.

Para os Conceitos de IoT e Arquitetura da Informação, assuntos diretamente relacionados ao objetivo do projeto, foi realizada pesquisa nas bases *on line* Google Acadêmico, Periódicos CAPES e ScienceDirect com as *strings* 'arquitetura da informação' + 'saúde' + 'IoT' e '*information architecture'* + *'healthcare'* + 'IoT'. Em alguns casos, foram retirados acentos e letras maiúsculas por estarem afetando a quantidade de resultados obtidos. Os resultados da pesquisa foram ordenados por sua relevância. Alguns artigos foram descartados diretamente por estarem repetidos dentro da mesma pesquisa ou por serem meramente informativos. Dois artigos estavam em sua língua original (japonês e búlgaro) e foram descartados. A falta de acesso a artigos se deveu, preponderantemente, à sua inclusão em bases de dados pagas que cobram por inscrição ou por artigo baixado. A base de dados EBSCO estava indisponível no período em que foi realizada a pesquisa. Muitos dos resultados das pesquisas pela *string* 'IoT' no Portal de Periódicos da CAPES retornaram arquivos relacionados a IOT – Instituto de Ortopedia e Traumatologia, sem relação com o objetivo desse projeto e, portanto, não foram considerados. A pesquisa no site de Periódicos da CAPES apresentou algumas dificuldades como, por exemplo: (i) informava na página de pesquisa que o texto estaria disponível e, muitas vezes, não estava, (ii) ao clicar no link para o arquivo, o que abria era a página da revista onde o arquivo foi publicado gerando mais esforço de pesquisa para se localizar o artigo de interesse em edições anteriores da revista e (iii) os artigos pesquisados abriam em outra página do browser sem que a função 'voltar' estivesse disponível, sendo necessário retornar ao início da pesquisa para continuar o trabalho. No total, foram selecionados 55 arquivos. Os resultados iniciais são apresentados no quadro 32. Essas pesquisas também foram realizadas na Sala de Estudos do Programa de Pós-Graduação Fumec, em 28.03, 11.04 e 16.04.2019. Também foi realizada pesquisa visando encontrar as fontes primárias para as citações mais relevantes e pesquisa específica sobre o tema Arquitetura da Informação, no Google Acadêmico. Foi feita a leitura dos resumos dos arquivos que não estavam disponíveis diretamente nas bases pesquisadas, quando estavam disponíveis. Os arquivos identificados como de interesse para a pesquisa foram procurados diretamente no *browser* Google Chrome, na tentativa de obtê-los.

Quadro 32 – Resultados da segunda pesquisa

	Número de resultados	Resultados considerados	Baixados diretamente	Sem conseguir acesso	Sem interesse
Base: Google Acadêmico. String: 'arquitetura da informação' + 'saude' + 'iot'	**71**	**30**	**24**	**6**	**0**
Base: Google Acadêmico. String: 'information architecture' + 'health' + 'iot'	**602**	**30**	**4**	**25**	**1**
Base: Periódicos CAPES. String: 'arquitetura da informação' + 'saúde'	**29**	**20**	**3**	**16**	**1**
Base: Periódicos CAPES. String: 'saúde'+'IoT'	**36**	**20**	**7**	**3**	**10**
Base: Periódicos CAPES. String: 'arquitetura da informação' + 'IoT'	**2**	**2**	**1**	**0**	**1**
Base: Periódicos CAPES. String: 'information architecture' + 'health'	**1.970**	**20**	**1**	**17**	**2**
Base: Periódicos CAPES. String: 'health'+'IoT'	**11.937**	**20**	**7**	**13**	**0**
Base: Periódicos CAPES. String: 'information architecture' + 'IoT'	**155**	**20**	**7**	**8**	**5**
Base: ScienceDirect. String: 'arquitetura da informação' + 'saúde' + 'IoT'	**3**	**3**	**1**	**2**	**0**
Base: ScienceDirect. String: 'information architecture' + 'health' + 'IoT'	**2.219**	**10**	**0**	**9**	**1**

Fonte: Elaborado pelo autor.

Também foram considerados os 8 textos inicialmente selecionados na pesquisa inicial, 4 artigos de conhecimento prévio do autor além de um capitulo de livro de sua coautoria sobre o assunto.

Apêndice 3

Ao se estudar o contexto nacional com foco na área de saúde, o documento IoT – Um plano de ação para o Brasil, de responsabilidade do BNDES, chamou a atenção pela organização e amplitude. A questão de estudar a conectividade surgiu, a princípio somente para a área da saúde e, posteriormente, se estendendo às quatro verticais: cidades, saúde, meio rural e indústrias. Foram pesquisadas as palavras chaves representativas dos sistemas de comunicação que provêm a conectividade necessária às aplicações IoT propostas pelo plano do BNDES, conforme apresentado no quadro z. As bases consultadas nessa etapa foram Ebsco, *Web of Science* e Google Acadêmico. A pesquisa foi realizada preferencialmente na Sala de Estudos do Programa de Pós-Graduação Fumec, entre outubro e novembro de 2019 considerando os 10 primeiros arquivos ordenados por relevância (número de citações). Foi feita a leitura flutuante daqueles que puderam ser baixados e selecionados os arquivos que apresentavam uma versão sistêmica sobre a conectividade proposta no documento do BNDES. No total, foram selecionados 34 arquivos. Outros documentos identificados como de interesse para a pesquisa foram procurados diretamente no browser Google Chrome e na biblioteca, no caso de livros. Os textos inicialmente nas duas pesquisas anteriores também foram utilizados quando dentro do novo escopo.

Quadro 33 – Resultados da terceira pesquisa

Base pesquisada ->	**Ebsco**		**Web of Science**		**Google Acadêmico**	
String pesquisada	**Número de resultados**	**Arquivos considerados**	**Número de resultados**	**Arquivos considerados**	**Número de resultados**	**Arquivos considerados**
‘gsm technology’	**741**	**1**	**2.614**	**1**	**690.000**	**0**
‘lte technology’	**2.641**	**1**	**4.451**	**0**	**671.000**	**1**
‘gprs cellular’	**82**	**0**	**1.349**	**0**	**87.100**	**1**
‘LTE-M’	**230**	**1**	**24**	**0**	**17.200**	**0**
‘wired networks’	**3.018**	**0**	**-**		**1.470.000**	**1**
‘redes por cabo’	**5**	**0**	**0**	**0**	**1.650.000**	**1**
‘NB-IoT’	**10**	**1**	**343**	**1**	**18.700**	**1**
‘GPON technology’	**110**	**0**	**439**	**0**	**11.800**	**1**
‘LPWA’	**264**	**1**	**133**	**2**	**517**	**0**
‘LoRa’	**7.530**	**0**	**969**	**1**	**386.000**	**1**
‘sigfox’	**337**	**0**	**98**	**1**	**5.650**	**1**
‘rpma’	**73**	**0**	**54**	**1**	**6.990**	**0**
‘wifi technology’	**659**	**0**	**8.197**	**1**	**348.000**	**1**
‘bluetooth technology’	**8.510**	**0**	**-**		**721.000**	**1**
‘BLE’	**2.827**	**0**	**2.138**	**0**	**4.120.000**	**1**
‘NFC’	**15.795**	**1**	**3.744**	**0**	**308.000**	**0**
‘rfid technology’	**16.402**	**2**	**22.117**	**1**	**1.070.000**	**1**
‘uwb technology’	**856**	**1**	**3.892**	**0**	**281.000**	**1**
‘segurança da informação’	**40**	**1**	**0**	**0**	**786.000**	**0**
‘information security’	**64.508**	**1**	**76.068**	**0**	**3.790.000**	**1**

Fonte: Elaborado pelo autor.