Pontifícia Universidade Católica de São Paulo
PUC–SP

Dorival Moreira Machado Junior

Segurança da informação: uma abordagem sobre proteção da privacidade em internet das coisas

Doutorado em Tecnologias da Inteligência e Design Digital

São Paulo
2018

Pontifícia Universidade Católica de São Paulo
PUC–SP

Dorival Moreira Machado Junior

Segurança da informação: uma abordagem sobre proteção da privacidade em internet das coisas

Doutorado em Tecnologias da Inteligência e Design Digital

Tese apresentada à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para obtenção do título de Doutor em Tecnologias da Inteligência e Design Digital e área de concentração modelagem de sistemas de software sob a orientação do Professor Dr. Daniel Couto Gatti.

São Paulo
2018

Banca Examinadora

_____

_____

_____

_____

_____

Este trabalho é dedicado aos meus pais Dorival e Divina, à minha esposa Márcia e aos meus filhos Giovanni e Thiago. Sem o apoio desta equipe, esta pesquisa jamais seria possível!

Agradecimentos

Agradeço à Deus, que na sua infinita bondade proporcionou-me as condições para este aprimoramento de conhecimento.

À minha esposa Márcia, pela paciência, paciência e paciência, mas sobretudo pelo amor e companheirismo que foram fundamentais ao longo desta etapa acadêmica.

Aos meus filhos Giovanni e Thiago, pelo carinho, obediência, alegria e companheirismo. Esta dupla foi essencial para tornar animado o ambiente de estudo.

Aos meus pais Dorival e Divina que nunca mediram esforços para incentivar e proporcionar meus estudos. Seus ensinamentos de família como base para qualquer projeto, bem como o apoio contínuo tornaram possível a conclusão desta etapa.

Ao meu irmão Julio Cesar, pela efetiva ajuda na revisão de texto, etapa essencial para conclusão da tese.

Ao professor Dr. Daniel que me conduziu no desenvolvimento desta tese, delineando e conduzindo a um resultado satisfatório. Pelo companheirismo e troca de informações durante o período de pesquisa.

Aos professores da banca de qualificação, Dr. Demi e Dr. Ítalo, pelas contribuições que ajudaram a nortear o direcionamento desta tese.

À D. Edna secretária do TIDD, pelas co-orientações e auxílios aos quais foram essenciais no decorrer do percurso acadêmico.

Aos professores do TIDD que compartilharam um pouco de seus conhecimentos, proporcionando o enriquecimento desta tese.

Aos professores integrantes da banca de defesa, pelo aceite do convite bem como as contribuições ao trabalho.

"Produzir uma teoria é uma belíssima aventura,
mas tem seus desertos. Quem se arrisca a andar por ares
nunca antes respirados ou pensar fora da curva
tem grandes chances de encontrar pedras no caminho.
No entanto, ninguém é digno de contribuir para a ciência
se não usar suas dores e insônias nesse processo.
Não há céu sem tempestade.
Risos e lágrimas, sucessos e fracassos, aplausos e vaias
fazem parte do currículo de cada ser humano, em especial
daqueles que são apaixonados por produzir novas ideias."
(Augusto Cury)

Resumo

O conceito de *Internet of Things* (IoT) refere-se a uma rede de objetos com capacidade para gerar, coletar e trocar dados entre si. Esta interconexão de objetos inteligentes tende a proporcionar melhorias no bem-estar das pessoas de modo que quanto mais "coisas" adquirindo ou gerando dados, melhor pode ser o resultado propiciado pela IoT. Por outro lado, tem-se que a privacidade é melhor resguardada diante do fornecimento mínimo de dados ou informações pessoais. São caminhos contrários que caracterizam um paradoxo. Com isto, são necessários estudos que apontem possibilidades que favoreçam o crescimento da IoT e ao mesmo tempo não deixe que a privacidade seja totalmente sucumbida à evolução tecnológica. O usuário permeia ambos os fatores, ficando situado ao centro. Este paradoxo bem como a falta de documentação e padronização em termos de proteção da privacidade na IoT torna-se o problema de pesquisa. A hipótese sugere a necessidade de um padrão que possibilite tal proteção. A abrangência de padronização da Internet é muito extensa, fazendo-se necessário determinar os limites de atuação desta tese. Para isto, fez-se o mapeamento do mecanismo pelo qual as regras e padrões da Internet são estabelecidos, bem como definindo um cenário padrão de IoT aplicável em qualquer ambiente em que for inserido. Uma vez estabelecidos estes parâmetros, pôde-se prosseguir através de uma análise exploratória crítica ao contexto que é considerado emergente principalmente pela falta de documentação no que diz respeito à proteção da privacidade na IoT. Como resultado foi sistematizado um direcionamento para proteção da privacidade na IoT por meio de um paradigma. Este tem como características: ser aplicável especificamente ao ambiente de IoT; ter como princípios considerar todos os dados de usuário como privados, bem como adotar uma política restritiva. Caracteriza-se também por uma etapa de validação humana, na qual é requerido que o usuário permita o compartilhamento de seus dados, bem como estabeleça a confiança no dispositivo vinculado, isto é, o destino dos dados. Deste modo, o usuário é instigado a ter ciência de seus dados em uso bem como o destino destes. Ao final, faz-se a conclusão analisando os objetivos de segurança de outros modelos justificando o parecer contrário ou favorável para aplicação na IoT.

Palavras-chaves: internet das coisas. privacidade. segurança da informação.

Abstract

The concept of Internet of Things (IoT) refers to a network of objects capable of generating, collecting, and exchanging data between them. This interconnection of intelligent objects tends to provide improvements in the well-being of people so that the more "things" acquiring or generating data, the better may be the result propitiated by IoT. On the other side, privacy is best guarded in the face of the minimum supply of data or personal information. They are contrary paths that characterize a paradox. With this, studies are needed that point out possibilities that favor the growth of IoT and at the same time do not let privacy be totally succumbed to technological evolution. The user permeates both factors, being situated in the center. This paradox as well as the lack of documentation and standardization in terms of privacy protection in IoT becomes the research problem. The hypothesis suggests the need for a standard that allows such protection. The scope of standardization of the Internet is very extensive, it is necessary to determine the limits of performance of this thesis. For this, the mapping of the mechanism by which the rules and standards of the Internet are established, as well as defining a standard scenario of IoT applicable in any environment in which it is inserted. Once these parameters were established, it was possible to continue through a critical exploratory analysis of the context that is considered emerging mainly by the lack of documentation regarding the protection of privacy in IoT. As a result, a directing to privacy protection in IoT was systematized. This has as characteristics: to be applicable specifically to the IoT environment; Have as basic principles consider all user data as private as well as adopt a restrictive policy. It is also characterized by a step of human validation, in which it is required that the user allows the sharing of their data, as well as establish the trust to the device to link, that is, the destination of the data. In this way, the user is instigated to have science of their data in question beyond the destination of these. At the end, the conclusion is made by analyzing the security objectives of other models justifying the contrary or favorable opinion for application in IoT.

Key-words: internet of things. privacy. security information.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

5G	*5th Generation Mobile Networks*
ABNT	Associação Brasileira de Normas Técnicas
ARPANET	*Advanced Research Projects Agency Network*
ASO	*Address Supporting Organization*
BNDES	Banco Nacional de Desenvolvimento Econômico e Social
CCOMGEX	Comando de Comunicações e Guerra Eletrônica do Exército
CDMA	*Code Division Multiple Access*
CIA-triad	*Confidentiality, Integrity and Availability triad*
CPS	*Cyber Physical System*
DARPA	*Defense Advanced Research Projects Agency*
DDoS	*Distributed Denial of Service*
DNS	*Domain Name System*
DoS	*Denial of Service*
EDGE	*Enhanced Data Rates for GSM Evolution*
ETSI	*European Telecommunications Standards Institute*
GDPR	*General Data Protection Regulation*
GPS	*Global Positioning System*
GPRS	*General Packet Radio Service*
GSM	*Global System for Mobile Communication*
HTTP	*Hyper Text Transfer Protocol*
HTTPS	*Hyper Text Transfer Protocol Secure*
I2P	*Invisible Internet Project*
IANA	*Internet Assigned Numbers Authority*

IAB	*Internet Architecture Board*
ICANN	*Internet Corporation for Assigned Names and Numbers*
IEC	*International Electrotechnical Commission*
IEEE	*Institute of Electrical and Electronics Engineers*
IESG	*Internet Engineering Steering Group*
IETF	*Internet Engineering Task Force*
IoE	*Internet of everythings*
IoT	*Internet of Things*
INPI	Instituto Nacional da Propriedade Industrial
IP	*Internet Protocol*
IRTF	*Internet Research Task Force*
ISO	*International Organization for Standardization*
ISOC	*Internet Society*
ISP	*Internet Service Provider*
ITAC	*Internet Technical Advisory Committee*
ITU	*International Telecomunications Union*
LAN	*Local Area Network*
LTE	*Long Term Evolution*
LIR	*Local Internet Registry*
MAN	*Metropolitan Area Network*
MIL-STD	*Military Standard*
MCTIC	Ministério da Ciência, Tecnologia, Inovações e Comunicações
NBR	Norma Brasileira
NFC	*Near Field Communication*
NIC.br	Núcleo de Informação e Coordenação do Ponto BR
NIR	*National Internet Registry*

NRO	*Number Resource Organization*
PAN	*Personal Area Network*
PLC	*Power Line Communication*
RAND	*Research and Development*
RFID	*Radio Frequency Identification*
RIR	*Regional Internet Registries*
SCADA	*Supervisory Control And Data Acquisition*
SSL	*Security Sockets Layer*
T2TRG	*Thing-to-Thing Research Group*
TCP	*Transmission Control Protocol*
Tor	*The Onion Routing*
URI	*Uniform Resource Identifiers*
URL	*Uniform Resource Locator*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*
W3C	*World Wide Web Consortium*

Sumário

INTRODUÇÃO

Imagine uma casa que ao amanhecer faça o ajuste da iluminação e da temperatura do ambiente, além de preparar o café com torradas logo que detectado que o indivíduo se levantou da cama; que alerte para medicamentos do dia bem como faça uma análise de exames básicos (como nível de diabetes) e envie esta informação para acompanhamento do médico da família; que defina um repertório musical diferenciado a cada dia com base em preferências do usuário; que seja capaz de facilitar o preparo do almoço providenciando a reposição de produtos que faltem na geladeira, além de "notificar" ao médico da família o tipo de alimentação que normalmente ali existe; uma casa que seja proativa em termos de segurança, detectando vazamento de água ou gás, princípio de incêndio, mal funcionamento da rede elétrica, presença de pessoas diferentes dos moradores habituais acionando profissional ou autoridade pertinente ao caso. Imagine uma casa que promova o bem-estar e proteção da saúde monitorando sinais vitais dos moradores, que realize a detecção de quedas ou indícios de qualquer outro acidente doméstico ou situação que comprometa a integridade das pessoas e que em casos críticos acione serviços de emergência. Imagine uma casa na qual "coisas" sejam capazes de coletar ou fornecer dados e interagir entre si e agentes externos, objetivando ser eficiente em termos de bem-estar aos moradores.

Suponha uma cidade que se auto reorganize em termos de fluxo de trânsito e pessoas, priorizando semáforos, indicando melhores rotas para pessoas e veículos; que permita o agendamento/acompanhamento de serviços de saúde a partir da residência dos moradores, que faça a indicação do melhor local para atendimento em vista de filas de espera; uma cidade em que o sistema de iluminação pública seja ativado somente em locais em que existam pessoas, ou que possa reconhecer por meio de sinais sonoros um acidente ou assalto notificando autoridades; uma cidade que otimize o desperdício de água ou energia elétrica, que permita a reutilização de água da chuva e esgoto, que identifique de forma autônoma a necessidade de redirecionamento de água por entre bairros ou parques ou qualquer outra área da cidade. Imagine uma cidade na qual por meio da monitoração de vídeo seja possível identificar a localização de pesssoas desaparecidas ou procuradas. Imagine uma cidade que seja eficiente em termos de mobilidade, segurança pública e redução de desperdícios, tudo isto por intermédio de "coisas" do ambiente público que sejam capazes de coletar e fornecer dados relativos ao ambiente, interagindo entre si e dando suporte efetivo à administração pública.

Considere um sistema de apoio hospitalar que monitore e controle a aplicação de medicamentos intravenosos, que possa alternar entre medicamentos e alertar ao profissional de saúde quando da ocorrência de problemas ou término da aplicação; um sistema

que monitore sinais vitais do paciente mesmo à distância: batimento cardíaco, respiração, indícios de ataque cardíaco, nível de índices relativos à diabetes, glicose, entre outros. Imagine um ambiente hospitalar que faça a detecção de agentes contagiosos no ar e na água e com isto favoreça a prevenção e controle de situações de contágio, infecções ou epidemias; imagine neste mesmo ambiente a possibilidade de permitir a condução das pessoas para áreas não contaminadas auxiliando na evacuação de locais críticos.

Todos estes cenários são hipotéticos e um pouco do que se espera para o futuro do mundo ao considerar as novas tecnologias, especialmente no que tange à Internet das Coisas (do inglês *Internet of Things* - IoT). A IoT pode promover não só os exemplos descritos, mas viabilizar um mundo com excelência em processos[1] e no uso otimizado de recursos (naturais ou artificiais). Tudo isto por meio do monitoramento e atuação em variáveis do ambiente[2] ao qual a IoT esteja inserida.

Trata-se de uma perspectiva de futuro próximo uma vez que a indústria IoT encontra-se em plena evolução e com produtos atualmente comercializáveis nos mais diversos segmentos. São exemplo: monitoramento e controle de dispositivos residenciais (BOSCH, 2018; PANASONIC, 2018; SAMSUNG, 2018), estacionamentos inteligentes (SMARTPARKING, 2018), veículos agrícolas (FARMOBILE, 2017), detecção e acionamento de socorro em caso de acidentes (DOMALYS, 2018; COROS, 2018) e geladeira (SAMSUNG, 2017) com recursos multimidia.

Dentre os cenários descritos, a Figura 1 exemplifica um contexto sob uma perspectiva mais detalhada. Não se trata de um ambiente real, mas uma proposição de arquitetura IoT na qual há interação entre geladeira, mercado e sistema de saúde, interação está que ocorre por meio de Internet, promovendo maior praticidade no bem-estar do usuário da geladeira. O funcionamento é como se segue.

Inicialmente considera-se que todos os produtos possuam uma forma de armazenamento de dados, por exemplo uma etiqueta com *chip* inserido na revenda ou fábrica. Nesta etiqueta constam todas as informações técnicas do produto como: nome, data de validade e ingredientes de composição. No primeiro momento, a geladeira monitora todos os produtos em seu interior e com isto pode identificar produtos vencidos ou não encontrados (embasando-se em uma lista mantida pelos usuários). Em qualquer uma destas ocorrências, por meio de um *gateway* a geladeira se comunica via Internet com o mercado conveniado e previamente autorizado pelo usuário, então faz a solicitação do produto em questão. Neste momento o sistema do mercado faz os procedimentos necessários à transa-

[1] Conforme Houaiss, Villar e Franco (2009, p. 1.554) **processo** é entendido como uma ação continuada. É a realização contínua de alguma atividade.

[2] As **variáveis do ambiente** são referenciadas nesta tese como os elementos do mundo real com os quais a IoT tenha contato: temperatura, umidade, luz, som, peso, velocidade, ou seja, características de objetos físicos como por exemplo o próprio corpo humano. A expressão também refere-se aos dados e informações fornecidos por outros possíveis *devices* que estejam no mesmo local.

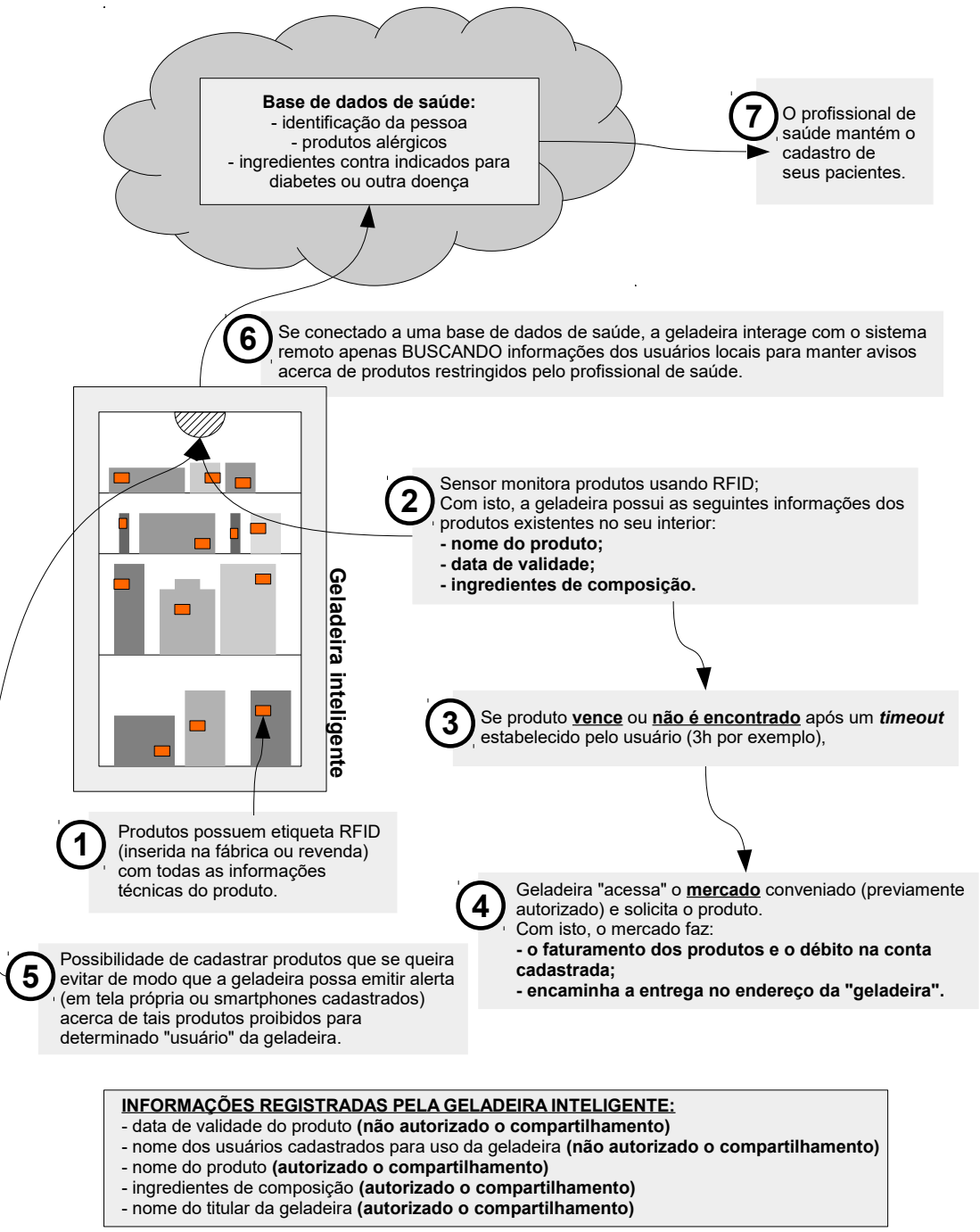


Figura 1: Proposição de arquitetura IoT de uma geladeira inteligente.

ção: faturamento e débito dos produtos na conta do cliente e encaminhamento do produto para o endereço da "geladeira".

Por meio da Internet, a geladeira poderia se conectar aplicação *web* contendo uma base de dados de saúde e com isto, confrontar os ingredientes de composição dos produtos com informações de saúde do usuário, registros estes mantidos pelo profissional de saúde (também por meio da Internet) associado ao usuário.

Um dos requisitos para estas inovações tecnológicas é a conectividade. Quanto mais elevada, maior é a viabilidade para integrar sistemas e coisas. A consolidação desta realidade está cada vez mais próxima. No ano 2000 menos de 7% da população mundial, ou seja, pouco mais de 400 milhões de usuários possuíam acesso à Internet. Em 2016 este valor chegou a mais de 45% da população mundial que equivale a mais de 3,4 bilhões de usuários (STATS, 2016). O surgimento do *smartphone* colaborou com este fenômeno mundial e também permitiu às pessoas se conectarem a partir de mais de um dispositivo de forma simultânea dentro do seu ambiente. Logo, com a IoT, possivelmente a quantidade de conexões tende a se elevar, com maior quantidade de dados adquiridos ou gerados.

Problema e hipótese

No exemplo da geladeira (Figura 1) observa-se que há dois caminhos opostos: de um lado a IoT promove uma melhoria no processo de acompanhamento da saúde por parte do médico. Com tais informações, ele poderia intervir em tempo real, advertindo ou bloqueando o uso da geladeira até que a leitura da advertência seja realizada. Do ponto de vista da saúde, isto seria uma melhoria no bem-estar do indivíduo, conduzindo-o à uma alimentação saudável e adequada às suas condições físicas. Mas por outro lado, há o compartilhamento de conteúdo do interior da casa (existe alguém consumindo tal produto naquele momento), do interior da geladeira (quantidade, tipo e data de compra dos produtos). É necessário compartilhar para se beneficiar da melhoria de processos e consequentemente do bem-estar. Este compartilhamento então realizado por meio dos dispositivos IoT torna os dados e informações disponíveis (em tempo real) para terceiros como o próprio médico, o estabelecimento comercial conveniado à geladeira, bem como o fabricante ou empresa de assistência técnica da geladeira. Esta problemática parte da IoT e toca o contexto da privacidade.

A privacidade é um fator de preocupação histórica da humanidade (COSTA, 2018), (RAMOS, 2008) e diante das novas tecnologias este problema se intensifica. Outro exemplo envolvendo a problemática da privacidade e as novas tecnologias pode ser tomado por meio da captação de imagens. É comum a existência de câmeras de circuito fechado em casas, portarias, bem como sistemas de monitoramento em vias, praças e demais locais públicos. Mesmo diante de avisos de proteção das imagens, estas já foram capturadas sem o consentimento. Esta captura proporciona melhorias no bem-estar no sentido de proteção das próprias pessoas, melhorando o processo de monitoramento que pode ser realizado de forma centralizada ou facilitando a identificação de meliantes por meio de imagens disponíveis. Deste modo, uma vez fora de casa, não há como o usuário prever quando suas imagens serão captadas, não havendo portanto privacidade garantida. Logo, deduz-se que a privacidade seria possível apenas dentro da própria casa, local que o usuário tem o real controle do ambiente. Entretanto, ao introduzir *devices* de segurança (vídeo ou

sensores) para monitoramento por empresa especializada, torna-se disponível também a movimentação no interior da casa, o que reduz drasticamente a garantia da privacidade.

Sob uma perspectiva globalizante, observa-se por meio dos exemplos descritos bem como conforme Kranenburg (2014) que por meio da interconexão de objetos inteligentes a IoT tende a proporcionar melhorias no bem-estar das pessoas de modo que quanto mais coisas adquirindo ou gerando dados, melhor pode ser o resultado propiciado pela IoT. Os dados são um facilitador de novas tecnologias e a IoT é um meio para captação ou geração destes. (LUCERO, 2016)

Por outro lado, quanto mais dados gerados ou adquiridos de um indivíduo, menor é a sua privacidade. Logo, tem-se que a privacidade é melhor resguardada diante do fornecimento mínimo de dados ou informações pessoais (CORCORAN, 2016; PAESANI, 2008; KOCHAVI; JORDAN, 2016). Entretanto, este é o caminho contrário para o funcionamento da IoT. A essência da IoT está na captação/geração de dados para ocasionar uma ação. Se não há dados para captar/gerar, a IoT é nula. Deste modo, ambas: privacidade e IoT constituem um paradoxo[3]. O usuário permeia o centro deste paradoxo (Figura 2) prezando pela maior privacidade ou pelo bem-estar proporcionado pela IoT. Cabe a este usuário controlar quais dados podem ser compartilhados e se possível ter o conhecimento do destino destes.

Figura 2: Representação visual do paradoxo “privacidade e IoT” havendo o usuário como elemento central.

Os problemas envolvendo falta de privacidade na IoT podem estar nos mais diversos segmentos em que esteja inserida: saúde, transporte, proteção e socorro em acidentes, infraestrutura, agricultura, defesa, entre outros; problemas como o uso ilícito de dados privados, roubo de informação industrial, alteração de dados críticos, coação ou assassinato à distância, comprometimento da defesa de uma nação, entre outras possibilidades. Deste modo, são necessários recursos para garantir a segurança das informações privadas.

Em termos de computação, para se garantir a segurança da informação, isto é, para que uma informação seja realmente considerada segura é necessário que a mesma esteja

[3] Conforme Houaiss, Villar e Franco (2009, p.1430) **paradoxo** significa uma contradição, uma aparente falta de nexo ou de lógica, um raciocínio coerente que esconde contradições.

suportada por três pilares (DANTAS, 2011; CHERDANTSEVA; HILTON, 2013; WHITMAN; MATTORD, 2015): a **disponibilidade** que é a informação disponível quando necessário, a **integridade** que é a informação na sua essência, sem modificações e a **confidencialidade** que é a propriedade da informação ser exibida somente ao agente autorizado, seja pessoa ou equipamento. Todos os pilares trabalham em conjunto de forma intrínseca, ou seja, uma forma simbiótica de ser ao passo que não há segurança da informação se qualquer um dos pilares for comprometido. Sendo a IoT um segmento da computação, também estará sujeita aos mesmos princípios de segurança.

Entretanto, quando comparados a um computador tradicional os dispositivos que compõem a IoT são mais vulneráveis em termos de poder de processamento, armazenamento e localização (LEVITT, 2015; SENGUL, 2017). Logo, tais fatores de vulnerabilidade colocam a IoT em situação de maior risco uma vez que podem ser comprometidos com maior facilidade. Como consequência, tais equipamentos podem fornecer dados para uso ilícito, serem induzidos ao fornecimento de dados falsos, ou ainda, simplesmente parar de gerar dados, tudo isto influenciando negativamente no ambiente e desencadeando reações adversas no mundo digital e físico. (LEVITT, 2015)

Uma pesquisa da PwC (PWC, 2018) intitulada *The Global State of Information Security - Survey 2018* foi realizada com base em respostas de 9.500 pessoas em 122 países ligadas ao nível estratégico organizacional de empresas de segmentos como aeroespacial e defesa, educação, energia, finanças, entretenimento, serviços governamentais, indústria da saúde, hospitais, tecnologia, telecomunicações, transporte e logística, entre outros. A pesquisa apontou que deste total de entrevistados 67% possuem estratégia para segurança na IoT ou estão em processo de implementação. Logo, deduz-se que os 33% restantes não possuem recursos de proteção para IoT, o que torna-se algo preocupante considerando que se tratam de indústrias com soluções IoT em linha de produção ou desenvolvimento. Outro fator destacado na pesquisa aponta que dos 67% que possuem estratégia, 36% possuem políticas e padrões uniformes de segurança cibernética para dispositivos IoT. Logo, uma nova dedução aponta que os outros 64% possuem recursos não padronizados de segurança da informação para IoT. Com isto, PwC (2018) evidencia a ausência de uma padronização global para segurança na IoT, bem como a necessidade de uma diretiva que possa ser adotada e aplicada de forma uniforme a qualquer segmento IoT.

Considerando o inevitável paradoxo envolvendo "privacidade" e "Internet das Coisas", bem como a ausência de padronização em termos de proteção da privacidade em IoT, esta tese busca responder as seguintes perguntas:

- Como fazer para que a privacidade não seja invadida e utilizada sem o consentimento do usuário de IoT?
- É possível determinar uma forma que auxilie no controle de confidencialidade de

dados manipulados[4] por dispositivos em ambiente IoT?

- Como viver em um contexto no qual o mundo digital e o mundo real se interconectam levando em consideração o fator privacidade?

A **hipótese** implícita a estes questionamentos sugere a necessidade de um padrão de segurança em IoT que possa suavizar o paradoxo demonstrado na Figura 2.

Objetivo

Esta tese tem como objetivo estabelecer um paradigma para proteção de dados privados manipulados por dispositivos IoT, possibilitando uma maneira de convivência entre "privacidade" e "IoT".

Como objetivos secundários, esta tese acaba por sistematizar a evolução histórica que originou os princípios de segurança da informação, bem como proporcionar uma análise etimológica que permita resgatar o sentido latino das principais palavras envolvidas.

Procedimentos metodológicos

Para esta tese foi utilizado como método de pesquisa a análise exploratória de uma área emergente, realizando uma investigação crítica e uma abordagem qualitativa. A escolha do método teve como motivação a falta de padronização e documentação envolvendo a privacidade na IoT. Este método é descrito como se segue.

A abrangência de padronização da Internet é muito extensa, permeando particularidades em diversos aspectos tais como *hardware*, *software*, governança, entre outras. Em vista disto, com base em ICANN (2013) foi realizado o seccionamento demonstrado na Figura 3 (de modo que cada um dos níveis serão descritos no capítulo 1, subseção 1.1.1 (pág. 31)) com a finalidade de definir os limites de atuação desta tese. Assim, esta se limitou aos aspectos de política e governança. Foi realizado também um levantamento das organizações que produzem os padrões e diretrizes para a Internet e deste modo, pôde-se focar na busca de materiais relativos à padronização em nível de política e governança, em especial ao que diz respeito à privacidade.

A abordagem em um nível mais elevado (política & governança) tem maior aptidão para tal uma vez que pode determinar referências a serem adotadas pelos demais níveis de padronização.

[4] Entende-se pela **manipulação** de dados IoT: a captação de dados por sensores, a manipulação através de processamento bem como a geração através de processamento e atuadores.

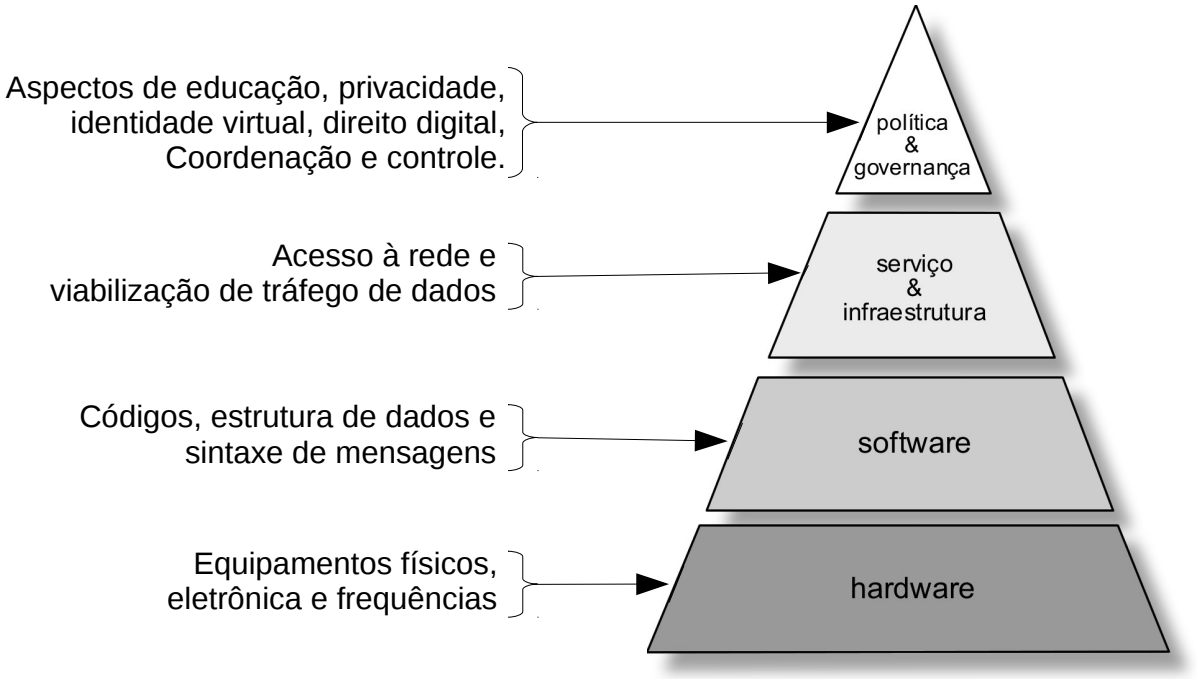


Figura 3: Aspectos de padronização na Internet

Vários modelos de segurança da informação já foram criados e serão discutidos no decorrer desta tese. Entretanto, estes não possuem aplicação específica para IoT e não promovem a resolução do problema.

A base bibliográfica é composta de conteúdos que foram selecionados em documentação de instituições internacionais e nacionais responsáveis pela padronização e gestão da Internet, dentre estes a base de pesquisa IEEE, IETF, W3C, ISOC, simpósios nacionais e internacionais, *whitepapers* de empresas de tecnologia, dicionário de latim, dicionário de lingua portuguesa, legislação brasileira, documentação governamental e militar, livros, documentários, filmes, teses, dissertações, mas não se limitando a estes.

Na própria revisão bibliográfica foram realizadas análises críticas encontrando limites pertinentes à privacidade em face à IoT (estado da arte). Pôde-se apontar a evidente preocupação com a classificação e proteção de dados privados, entretanto, observou-se a falta de um procedimento aplicável em qualquer segmento em que a IoT esteja inserida. A investigação se estendeu à base de marcas e patentes, levantando dados relativos à propriedade intelectual e contabilizando informações de registros relacionados à proteção da privacidade na IoT.

São diversos os cenários IoT possíveis, partindo desde uma rede pessoal (intercomunicação de *devices* pessoais) até uma rede mais ampla (intercomunicação de *devices* geograficamente distantes), havendo também a diversidade de equipamentos para esta tecnologia. Logo, foi necessário definir um cenário padrão de IoT, uma organização sistemática que se adequasse a qualquer segmento ao qual a IoT esteja inserida. Uma vez

definido este cenário, pode-se formular o paradigma objetivo.

Outro ponto de pesquisa concomitante caracteriza-se pela busca de modelos de segurança da informação existentes, analisando seus objetivos quanto à aplicabilidade na IoT. Foi possível rastrear a origem destes modelos, de modo que todos culminam na CIA-triad. Em vista disto, buscou-se compor a evolução histórica, bem como os modelos de expansão criados posteriormente.

No viés da privacidade, foi realizada a análise etimológica dos termos "privacidade" e "confidencialidade", confrontando-os de modo a determinar a correta utilização com base no sentido latino das palavras. Esta tese não adentra às propriedades da ciência do direito, entretanto buscou-se levantar na legislação brasileira Leis pertinentes à privacidade, mais especificamente aos conteúdos tocantes à IoT. A análise possibilitou encontrar possíveis pontos divergentes e que se tornam brechas as quais tornam a garantia da privacidade na Internet algo subjetivo.

Com base na bibliografia analisada, foram identificados os possíveis recursos de proteção à privacidade e que são a confidencialidade e anonimato. Este segundo, também foi submetido a uma análise etimológica e também com base na legislação, foram levantados os meios possíveis para se prover tais recursos na Internet. Isto foi necessário para aplicação ao cenário padrão definido e favorecer a sistematização objetivo da tese. Também foram realizados experimentos em laboratório (registrados nos anexos desta tese) para justificar a aplicabilidade na IoT.

No processo de investigação bibliográfica foram identificados trabalhos relacionados ao tema, partindo das instituições constantes da Figura 5, bem como demais conteúdos pesquisados.

Por fim, realizou-se a sistematização do paradigma ao qual esta tese se propôs. A apresentação é precedida pelo levantamento dos pontos (requisitos e definições) então estabelecidos durante o estudo. Cada elemento que compõe o paradigma foi justificado e explicado por intermédio de um fluxograma funcional demonstrando a sua integração à CIA-triad. O paradigma é tido como um "exemplo de modelo" que pode oportunamente tornar-se referência. Deste modo, fez-se também uma breve exemplificação teórica de aplicação do mesmo.

Por fim, fez-se a conclusão do trabalho justificando o parecer contrário ou favorável em termos de aplicabilidade de objetivos de segurança (de todos os modelos levantados) na IoT.

Organização da tese

O **capítulo 1** compõe uma revisão buscando as origens da Internet, seu ecossistema e mapeamento das instituições que compõem o mecanismos que determina as diretrizes e padrões da Internet. Faz a conceituação de dado *versus* informação com a finalidade do correto uso dos termos na IoT. Em seguida, faz uma abordagem sobre IoT e a evolução da Internet e cenários possíveis. Adentra os conceitos de Indústria 4.0 e *Cyber Physical Systems* confrontando-os e por fim faz um levantamento de possíveis formas de classificação de dispositivos IoT existentes.

No **capítulo 2** é feito um estudo no que diz respeito à origem e evolução da segurança da informação. Neste capítulo descreve-se o tripé da segurança da informação bem como descreve modelos baseados do mesmo, descrevendo os objetivos de segurança de cada um dos modelos levantados.

No **capítulo 3** desenvolve-se a discussão acerca da privacidade na Internet, realizando uma análise etimológica de modo a recuperar o sentido latino dos termos envolvidos e determinar uma utilização sem ambiguidades. Passa-se pela legislação brasileira em termos de privacidade na Internet com atenção especial ao Marco Civil. Ainda neste capítulo faz-se uma descrição dos recursos de confidencialidade e anonimato como alternativas de proteção da privacidade na Internet, fazendo um levantamento dos possíveis recursos de proteção existentes com intuito de justificar a possibilidade ou não de uso na IoT em atenção ao objetivo da tese. O capítulo finaliza realizando um levantamento de trabalhos relacionados, partindo das organizações responsáveis pela padronização na Internet.

O **capítulo 4** faz a apresentação do paradigma para proteção da privacidade no ambiente de IoT. Embasando-se na revisão bibliográfica com análises críticas realizadas, apresenta o resultado por meio da sistematização de um modelo em tese e seu respectivo fluxograma funcional, descrevendo cada um dos componentes integrantes. Em seguida faz-se a aplicação teórica do paradigma a ambientes hipotéticos, demonstrando a forma de adoção/aplicação.

Por fim, faz-se a conclusão do trabalho, resumindo os questionamentos investigados durante o estudo. Em seguida, faz-se uma análise comparativa entre os objetivos de segurança identificados nos modelos existentes, justificando o parecer favorável ou contrário a cada objetivo.

O trabalho inclui por fim as referências e **apêndices** (materiais de autoria do autor, criados especificamente para esta tese).

1 AS ORIGENS DA REDE

O teórico de comunicação Marshall McLuhan[1] propõe em meados da década de sessenta uma discussão acerca dos meios de comunicação como um extensor do homem. Na ocasião o autor falava dos meios de comunicação existentes na época o que não era o caso da Internet. Mesmo antes da concepção da "interligação de redes" que foi comprovada efetivamente[2] em outubro de 1977 conforme Forouzan (2008, p.2), McLuhan previa uma estrutura que poderia viabilizar a unificação do conhecimento, tornando-o acessível de forma global:

> A falta de homogeneidade na velocidade do movimento informacional cria diversidades estruturais na organização. Pode-se prever facilmente que qualquer novo meio de informação altera qualquer estrutura. Se o novo meio é acessível a todos os pontos da estrutura ao mesmo tempo, há a possibilidade de ela mudar sem romper-se. (...) Nossa civilização especializada e fragmentada, baseada na estrutura centro-margem, subitamente está experimentando uma reunificação instantânea de todas as suas partes mecanizadas num todo orgânico. (MCLUHAN, 1964, cap. 10)

A humanidade como um todo e suas comunidades específicas e isoladas, tanto por fatores culturais como em função da localização física (grandes centros urbanos e comunidades do interior) vive esta reunificação. O mundo se adequou à presença da Internet. Deste modo, o conceito de "aldeia global" cunhado por McLuhan acabou culminando no que é a Internet.

Além da unificação do conhecimento, outro ponto destacado por McLuhan refere-se ao interesse do homem por artefatos que poderiam tornar-se extensores do próprio ser, objetos que poderiam potencializar ou melhorar a qualidade de vida: *"(...) os homens logo se tornam fascinados por qualquer extensão de si mesmos em qualquer material que não seja o deles próprios."* (MCLUHAN, 1964, cap.4)

Em razão desta atração por dispositivos "extensores" bem como a acessibilidade do conhecimento de forma global, o autor previa uma tendência que culmina no que a humanidade se depara: a onipresença do máximo de dados possíveis via Internet, seja por meio de computadores, *smartphones* e qualquer outro equipamento conectável à rede de modo que tais dados sejam disponíveis em tempo real. Esta disponibilidade é válida tanto para dados registrados no momento em que acontecem, quanto para dados já armazenados. Este nível de disponibilidade tem relação estrita ao *Big Data*. Conforme Gutierres (2017,

[1] Bibliografia, histórico e curriculum em Gordon (2002)

[2] Através da interligação de três redes distintas: rede da *Advanced Research Projects Agency Network*, conhecida como ARPANET, satélite e rádio de pacotes.

p. 29, 33 e 35) e Kadow (2017, p. 59-65) não existe uma definição rigorosa para esta expressão de modo que os dois somam conjuntamente um levantamento com mais de cinquenta definições de autores diferentes tentando descrever *Big Data*. Entretanto, todas estas convergem para a "quantidade de dados" disponível e a "analítica" destes dados, isto é, a possibilidade de análise profunda, minuciosa pela qual busca-se o aprimoramento de novos serviços e produtos.

Observando por esta perspectiva, a IoT pode ser um novo produto ou serviço que então faz uso dos dados disponíveis, mas também pode ser o agente viabilizador para a aquisição destes.

1.1 O ecossistema da Internet

Faz-se aqui uma análise crítica a respeito do ecossistema afim de identificar e sistematizar seus participantes bem como o mecanismo de desenvolvimento de padrões e políticas aplicáveis à rede.

A Internet é uma rede de redes interligadas, um conjunto de redes independentes e intermediárias que se interconectam de modo que esta junção de redes se torna um subsistema de comunicação global sobre o qual outros sistemas de comunicação possam atuar para transmissão de texto, imagens, audio e vídeo (COULOURIS et al., 2007, p. 76), (WHITE, 2012, p. 246), (STALLINGS, 2009, p. 90). Em vista disto é grande a quantidade de pessoas conectadas à rede, algo estimado em aproximadamente 3,2 bilhões de usuários de acordo com CIA (2017)[3]. No Brasil a quantidade de usuários equivaleu a 66% da população no ano de 2015 conforme CETIC (2015a) e em 2016 este valor chega aos 93% conforme CETIC (2017, p. 354).

Em termos de domicílios com acesso à rede, foram 51% no Brasil conforme (CETIC, 2015b). Em outros países este índice é bem mais elevado conforme a Tabela 1.

Em contrapartida, apesar de não ser o meio de maior existência nos domicílios, mas com uma presença significativa, a Internet é tomada como "*(...) o principal arranjo comunicacional da sociedade (...)*" Silveira (2016, p. 18) *apud* Deleuze (2006), Galloway (2004).

Em razão da sua essência que é a interligação global, a Internet não deve ser dirigida por uma única entidade seja ela uma pessoa, uma organização ou um governo específico, mas deve manter-se uma rede descentralizada administrativamente falando. Este princípio da administração descentralizada é preservado graças ao próprio ecossistema da Internet contextualizado na Figura 4. Conforme ISOC (2014) este ecossistema é dividido em seis segmentos nos quais cada entidade cumpre suas atribuições para o bom

[3] A pesquisa data de 2014 para a maioria dos países, enquanto outros são de anos anteriores.

Tabela 1: Porcentagem de domicílios com acesso à Internet (adaptado de OECD (2015))

País	**% de famílias (domicílios) com acesso à Internet**	**Data da pesquisa**
Alemanha	90,29	2015
Austrália	83	2012
Austria	82,42	2015
Belgica	81,83	2015
Canadá	83,90	2013
Chile	66,5	2014
Dinamarca	91,74	2015
Eslovênia	77,64	2015
Espanha	78,75	2015
Estados Unidos	74,40	2013
Estonia	87,7	2015
Finlandia	89,93	2015
França	82,62	2015
Grécia	68,09	2015
Hungria	75,64	2015
Islândia	96,48	2014
Irlanda	84,86	2015
Israel	70,60	2013
Itália	75,39	2015
Letônia	76	2015
Lituânia	68,26	2015
Luxemburgo	96,78	2015
México	34,4	2014
Nova Zelândia	80	2012
Noruega	96,60	2015
Países Baixos	95,97	2015
Polônia	75,78	2015
Portugal	70,23	2015
Reino Unido	91,3	2015
República Checa	78,98	2015
República Eslovaca	79,48	2015
Suécia	91,03	2015
Suíça	90,63	2014
Turquia	69,54	2015

funcionamento conjunto de todo o ambiente. Estes segmentos são descritos da seguinte forma:

a. **endereçamento e nomeação**: envolve questões relativas ao endereçamento IP, nomes de domínios e números usados em protocolos de Internet. Este segmento é composto pela *Internet Assigned Numbers Authority* (IANA, 2017a), *Internet Corporation for Assigned Names and Numbers* (ICANN, 2017b), *Address Supporting Organization* (ICANN, 2017a), *Number Resource Organization* (NRO, 2017)

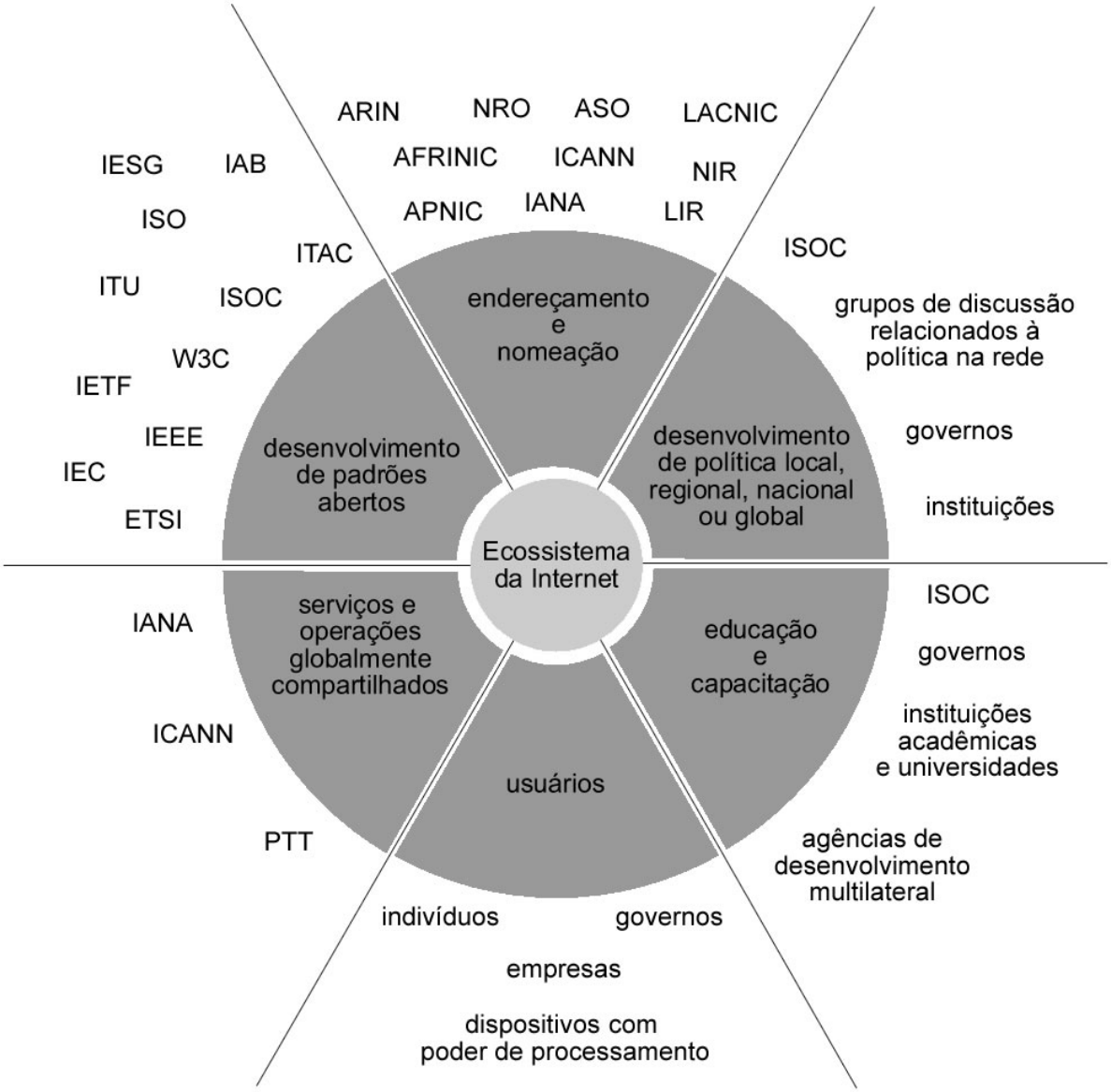


Figura 4: O ecossistema da Internet (adaptado de ISOC (2014))

e seus registros regionais: *The Internet Numbers Registry for Africa* (AFRINIC), *Asia-Pacific Network Information Centre* (APNIC), *American Registry for Internet Numbers* (ARIN), *Registro de Direcciones de Internet de América Latina y Caribe* (LACNIC) e *Ripe Network Coordination Centre* (RIPE NCC) (RIR, 2017), registros nacionais (que no Brasil é o NIC.br (NIC.BR, 2017a)) e provedores de serviço de Internet locais.

b. **serviços e operações globalmente compartilhados**: refere-se a recursos globalmente compartilhados como os *root servers* de *Domain Name System* (DNS) (IANA, 2017b) e domínios de primeiro nível que no Brasil equivale a ".br" (por meio do registro.br). Inclui-se também a distribuição de uso de números IP ao redor do planeta, além ainda dos Pontos de Troca de Tráfego (PTT). (IANA, 2017a),

(ICANN, 2017b), (NIC.BR, 2017d), (NIC.BR, 2017c)

c. **usuários**: segmento composto por quem usa a Internet: indivíduos, governos, negócios, organizações, máquinas/dispositivos com poder de processamento e desenvolvedores de equipamentos e serviços.

d. **educação e capacitação**: seção composta por entidades que trabalham a educação no uso da Internet, bem como a capacitação para lidar com as tecnologias da mesma. São integrantes: governos, ISOC e afiliados, instituições acadêmicas, universidades e agências de desenvolvimento multilateral.

e. **desenvolvimento de política local, nacional, regional ou global**: segmento composto por governos, instituições, ISOC e grupos de discussão relacionados à política na rede. Trata-se de um segmento intimamente ligado à seção de padronização uma vez que diversas organizações que desenvolvem diretrizes e padrões, embasam suas recomendações nos princípios de organizações como a *World Trade Organization* (WTO) e *Organisation for Economic Co-operation and Development* (OECD) então pertencentes a este segmento e descritas mais adiante.

f. **desenvolvimento de padrões abertos**: é o segmento responsável por desenvolver padrões técnicos que possibilitem a interoperabilidade entre dispositivos, serviços e aplicações por meio da Internet, bem como criar normatização de políticas, governança e recomendação de boas práticas para Internet. Participam organizações como: *Internet Engineering Steering Group* (IESG), *Internet Architecture Board* (IAB), *International Organization for Standardization* (ISO), *International Telecomunications Union* ITU, *Internet Technical Advisory Committee*ITAC, *Internet Society* (ISOC), *World Wide Web Consortium* (W3C), *Internet Engineering Task Force* (IETF), *Institute of Electrical and Electronics Engineers* (IEEE), *International Electrotechnical Commission* (IEC), *European Telecommunications Standards Institute* (ETSI).

1.1.1 Determinação das diretrizes e padrões da Internet

O mecanismo pelo qual se definem as diretrizes e padrões da rede é integrado por várias entidades que trabalham em conjunto e os padrões e diretrizes ao serem adotados pela comunidade global, proporcionam a continuidade da administração descentralizada e crescimento saudável da rede (ICANN, 2013). Estas diretrizes apontam tendências, caminhos, instruções que são benéficas para a rede, principalmente considerando a interoperabilidade entre seus participantes. Inclue-se aqui os protocolos, que são o modo pelo qual as regras de negociação entre membros é definida. Por exemplo, o protocolo de comunicação da Internet é o TCP/IP, pelo qual são estabelecidas as regras para endereçamento e troca de mensagens entre membros da rede. (KUROSE; ROSS, 2013)

Este mecanismo se faz por meio de fóruns, publicações e outras possíveis formas de compartilhamento de conhecimento nas quais usuários, empresas, governos, organizações de pesquisa, comunidade acadêmica e técnica, realizam debates abertos com o objetivo de propor diretrizes e padrões para a Internet em todos os seus aspectos de operação. Tais aspectos de padronização foram seccionados e demonstrado na Figura 3 (página 24). A descrição de cada nível é como se segue:

a. **política & governança**: refere-se ao contexto de educação, privacidade, identidade virtual, direito digital, coordenação e controle de serviços compartilhados e demais aspectos de alto nível, isto é, uma abordagem geral que não aprofunda detalhes técnicos e específicos de *hardware* ou *software*, mas sugestiona direções que podem auxiliar na elaboração de padrões dos demais níveis. São exemplos: W3C WoT (RAGGETT; ASHIMURA; CHEN, 2016), IoT Overview ISOC (2015), ABNT NBR ISO/IEC 27002 (ISO, 2013b) e ISO/IEC 30141 (ISO, 2016).

b. **serviço & infraestrutura**: refere-se ao contexto de acesso à rede e viabilização de tráfego de dados, o que pode envolver provedores de acesso, *datacenters*, pontos de troca de tráfego e redes de uma maneira geral no que se refere à estrutura bem como os serviços disponibilizados tais como DNS e *webserver*. Alguns exemplos de documentação neste contexto são: transmissão de pacotes IPv6 em redes elétricas (HOU; HONG; TANG, 2017), IPv6 em Bluetooth (NIEMINEN et al., 2015), recomendação para controle de sensores em ambientes de rede (ITU-T, 2013) e classificação de infraestrutura para *datacenter* – *Tier* – (TURNER et al., 2015), (VERAS, 2015, pos. 1982).

c. ***software***: refere-se ao contexto de códigos, estrutura de dados e sintaxe de mensagens, por exemplo o XML (BRAY; PAOLI; SPERBERG-MCQUEEN, 1998) e CSS (BOS, 2016).

d. ***hardware***: refere-se ao contexto de equipamentos físicos, eletrônica e frequências de transmissão. São exemplos: o Ethernet (IEEE, 2015b), modelos de transmissão digital (ITU-T, 1988) e divisão de frequência para uso em comunicação via rede elétrica (ITU-T, 2014b).

Considerando a descrição de cada um dos níveis identificados, esta tese enquadra-se no âmbito da "política & governança" e como tal se coloca nos limites deste nível sem adentrar questões específicas pertinentes aos demais, mas pondendo servir como base na concepção de padrões e normas para todos os níveis.

Com base no levantamento realizado em Monteiro e Boavida (2011, p. 9), ISOC (2017), ISOC (2014, p. 24), Hoffman (2013), IETF (2017a), W3C (2017b), IEEE (2017c), IAB (2017), IESG (2017), ITU (2017a), OECD (2017a), OECD (2017c), WTO (2017a),

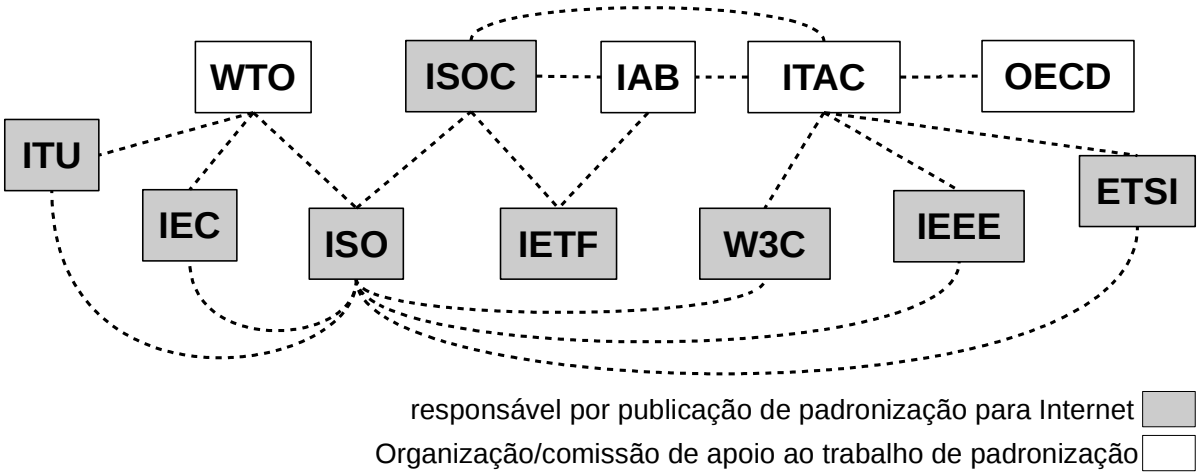


Figura 5: Estrutura que produz os padrões e diretrizes para a Internet

WTO (2017b), ITAC (2017b), ITAC (2017a), ETSI (2017c), IEC (2017a), ISO (2017a) e ISO (2017b), foi mapeada uma estrutura do mecanismo de padronização da Internet conforme apresentado na Figura 5. Esta estrutura é composta por diversas entidades participantes e suas funções a saber:

a ***World Trade Organization*** **(WTO)**: com sede na Suíça, é uma organização mundial que trata de regras do comércio entre nações e seu objetivo é garantir que este flua suave, previsível e livremente o quanto possível (WTO, 2017a). Ainda conforme WTO (2017b) WTO e OECD (descrita em seguida) são organizações distintas mas que trabalham em cooperação.

b ***Organisation for Economic Co-operation and Development*** **(OECD)**: está sediada na França e tem por objetivo ajudar governos a promover a prosperidade e combater a pobreza por meio do crescimento econômico e a estabilidade financeira (OECD, 2017a). A organização trabalha embasada em dados de diversos setores que são coletados ao redor do planeta[4]. Fazendo uma rápida análise da Figura 5 observa-se que a Internet tem como um possível princípio de sua evolução a preocupação com a prosperidade sadia da humanidade. Esta afirmação é fundada pela constatação das instituições apoiadas pela OECD e que são responsáveis por promover a padronização e diretrizes para a Internet.

c ***Internet Technical Advisory Commitee*** **(ITAC)**: este é o conselho técnico da OECD e contribui com trabalhos em política da economia digital, comunicação e serviços de infraestrutura, segurança e privacidade na economia digital (ITAC, 2017b), objetivos estes em consonância com a OECD. Observa-se pela Figura 5

[4] Em OECD (2017b) pode-se analisar o perfil estatístico do Brasil com dados obtidos na base de dados da própria OECD em OECD (2017c).

que esta comissão é um elemento estratégico na concepção de políticas da Internet, motivo pelo qual possui diversos membros (não só de padronização) importantes do ecossistema da Internet. (ITAC, 2017a)

d ***Internet Society* (ISOC)**: é uma organização internacional sem fins lucrativos que busca promover o crescimento da Internet por meio da participação em um grande espectro de questões como política, governança, tecnologia, desenvolvimento de padrõnização, protocolos e infraestrutura técnica, buscando garantir que a Internet cresça saudável e sustentável. Além de coordenar atividades técnicas, funciona como uma fonte oficial de informações sobre a Internet. (MONTEIRO; BOAVIDA, 2011, p. 9), (ISOC, 2017), (ISOC, 2014, p. 24)

e ***Internet Engineering Task Force* (IETF)**: É uma organização que contribue para a engenharia e evolução de padronização, desenvolvendo e mantendo especificações (conhecidas como *Request For Comments* - RFC) para protocolos essenciais da Internet como o IPv4 (DARPA, 1981a), IPv6 (BRADNER; MANKIN, 1995) (DEERING; HINDEN, 1998), HTTP (FIELDING et al., 1999), ICMP (POSTEL, 1981), TCP (DARPA, 1981b), UDP (POSTEL, 1980), definição de métodos[5] para adaptação do IPv6 ao padrão IEEE 802.15.4[6] (IETF, 2014), entre outros. É importante salientar que o IETF tem o respaldo jurídico e financeiro da ISOC, o que o torna um membro intrínseco da mesma. (HOFFMAN, 2013), (IETF, 2017a)

f ***Internet Research Task Force* (IRTF)**: é uma força tarefa que promove pesquisas de longo prazo relativas à evolução da Internet, centrando-se em abordagens que influenciarão o desenvolvimento de novas tecnologias. Com isto, este tipo de pesquisa não produz padrões ou normatizações para uso imediato, mas foca-se no uso futuro da Internet. IRTF (2017), Weinrib e Postel (1996, p.2-3)

g ***World Wide Web Consortium* (W3C)**: é um forum internacional que tem como finalidade propor tecnologias de interoperabilidade para a *World Wide Web*. Esta interoperabilidade é alcançada por meio do desenvolvimento de protocolos, diretrizes, *softwares* e ferramentas que garantam o crescimento a longo prazo da *Web*, isto é, por vários anos. O termo *Web* se refere ao espaço da informação (constituído por identificadores globais chamados *Uniform Resource Identifiers* - URI) como por exemplo o HTML (W3C, 2017b), (ISOC, 2014, p. 25), (W3C, 2017). É importante ressaltar que o W3C trabalha muitas vezes propondo especificações em conjunto com outras organizações como é o caso do HTTP especificado conjuntamente com o IETF. (FIELDING et al., 1999)

[5] Disponível por meio da RFC 4944 e atualizações realizadas por meio das RFCs 6282, 6775, 8025, 8066 (IRTF, 2007).

[6] Padrão IEEE para redes sem fio de baixa frequência, disponível em IEEE (2015a).

h ***Institute of Electrical and Electronic Engineers*** **(IEEE)**: é uma das maiores associações profissionais do mundo nas áreas de engenharia elétrica, eletrônica e informática com mais de 400 mil profissionais participantes ao redor do mundo. Seu objetivo principal é promover a inovação tecnológica em benefício da humanidade. Esta promoção ocorre por meio de publicações, conferências, atividades profissionais e educacionais, atuando no desenvolvimento de padrões (IEEE, 2017c). São exemplos de contribuição do IEEE as especificações tecnológicas de Ethernet (IEEE, 2015b), WiFi (IEEE, 2017a) e Bluetooth (IEEE, 2017b).

i ***Internet Architecture Board*** **(IAB)**: é um comitê que produz RFCs informacionais as quais servem de orientação técnica na definição de padrões e diretrizes no desenvolvimento da Internet como por exemplo a RFC 6973 (COOPER et al., 2013) que trata a consideração da privacidade em protocolos de Internet (IAB, 2017), (ISOC, 2014, p. 24).

j ***Internet Engineering Steering Group*** **(IESG)**: é o comitê responsável pelo gerenciamento técnico das atividades do IETF. Este órgão não produz normas e diretrizes mas é o responsável por aprovar e publicar as novas RFCs do IETF. Em resumo, funciona como um braço administrativo do IETF (ISOC, 2014, p.24), (IESG, 2017).

k ***International Telecommunications Union*** **(ITU)**: é a agência responsável pela coordenação da utilização mudial partilhada de uso do espectro radioelétrico, atribuição de órbita de satélites e demais fatores que envolvam a infraestrutura de telecomunicações. O ITU possui um setor de padronização sendo que as recomendações deste não são exclusivas para a Internet, mas é citado em razão do tráfego da Internet ser realizado em cima destes meios (ISOC, 2014, p.25), (ITU, 2017a). Exemplo: arquitetura de redes de transporte óptico em ITU (2017c).

l ***European Telecommunications Standards Institute*** **(ETSI)**: é uma organização que produz normas aplicáveis em nível mundial para tecnologias de informação e comunicação. É também reconhecida pela União Européia como a organização européia para normatizações (ETSI, 2017a). Produz padrões tecnológicos para comunicação e informação para Internet e rádio e entre suas produções mais conhecidas estão a tecnologia GSM, *Smart Card* e estudos para rede 5G (ETSI, 2017c).

m ***International Electrotechnical Commission*** **(IEC)**: é a organização lider mundial para preparação e publicação de padrões internacionais para todas as tecnologias elétricas, eletrônicas e relacionados. Esta organização fornece plataforma para que empresas, governos e indústria se reunam com finalidade de discutir e desenvolver padrões internacionais neste segmento (IEC, 2017a). Exemplo: requisitos de segurança para sistemas de conversão eletrônica de potência em IEC (2016).

- ***International Organization for Standardization* (ISO)**: é uma organização independente, não governamental composta por 163 países membros, dentre eles o Brasil por intermédio da Associação Brasileira de Normas Técnicas (ABNT)[7]. A ISO tem como objetivo desenvolver padrões internacionais baseado em consenso e relevância para o mercado e que proporcionem soluções para os desafios globais (ISO, 2017a; ISO, 2017b). Esta é considerada mundialmente a organização mais importante em termos de normatização, principalmente o desenvolvimento de normas para facilitar a troca de produtos em nível internacional (MONTEIRO; BOAVIDA, 2011, p. 8). Dentre as organizações constantes na Figura 5 são colaboradores da ISO: ITU, IEC, ISOC, W3C, IEEE e ETSI conforme ISO (2017c). Especificamente na área de redes de computadores a principal contribuição da ISO (juntamento com a IEC), foi o desenvolvimento do modelo *Open Systems Interconnection* (OSI) que visava a interoperabilidade entre equipamentos diversos. Em termos de segurança da informação, é exemplo de contribuição a norma ABNT/ISO IEC 27002 (ISO, 2013b), que propõe diretrizes e requisitos para sistemas de gestão de segurança da informação.

1.2 Revisão dos conceitos "dado" e "informação" para uso na IoT

Dado e informação são conceitos inerentes ao estudo de sistemas de informação, ciência da computação, administração e demais áreas que possam envolver o processo de produção e transmissão do conhecimento. A IoT faz parte do domínio computacional. Deste modo, também faz uso de tais elementos conceituais. Com a finalidade de validar o uso correto destes termos no contexto de IoT, foram levantadas algumas definições em caráter de revisão conforme exposto na Tabela 2.

Tabela 2: Levantamento de definições relacionadas aos conceitos de "dado" e "informação".

Autoria	**Descrição**
O'Brien (2011, p. 12)	*"Dados são fatos crus [...] Mais especificamente, os dados são medidas objetivas dos atributos (as características) de entidades (como pessoas, lugares, coisas e eventos). [...] podemos definir informação como dados que foram convertidos em um contexto significativo e útil para usuários finais específicos."*

– continua

[7] Objetiva prover a sociedade brasileira de conhecimento sistematizado, por meio de documentos normativos (ABNT, 2017)

Tabela 2 – continuação

Autoria	Descrição
Laudon e Laudon (2007, p. 9)	*"Informação quer dizer dados apresentados em uma forma significativa e útil para seres humanos. Dados, ao contrário, são sequências de fatos brutos que representam eventos que ocorrem nas organizações ou no ambiente físico [...]"*
Oliveira (2004, p. 167)	*"Dado é qualquer elemento identificado em sua forma bruta que por si só não conduz a uma compreensão de determinado fato ou situação [...] Informação é o dado trabalhado que permite ao executivo tomar decisões."*
Stair e Reynolds (2000, p. 4)	*"Dados consistem em fatos não trabalhados. [...] Informação é uma coleção de fatos organizados de modo que adquirem um valor adicional além do valor dos próprios fatos."*
Polloni (2000, p. 30)	Descreve que dados são valores, datas, descrições e outros dados que sozinhos não possuem valor significativo. Após serem manipulados por um sistema de processamento, tornam-se informações relevantes.
Bacon e Bull (1973)	Descreve que a semântica afeta como a informação é armazenada ou recuperada mas não o ato de comunicação uma vez que o que pode ser significado para uma pessoa pode ser um ato sem lógica para outro.

Observa-se pela Tabela 2 que as definições são harmoniosas de modo que trata-se de um conceito consolidado: dado é um fato bruto que por si só não é compreensível e informação é o dado processado, tornando-se algo significativo em determinado contexto. Com fundamento nestas definições conclui-se que é correto afirmar que a IoT trabalha exclusivamente com dados para gerar informações ou novos dados.

1.3 Internet das Coisas

Internet of Things - IoT é um termo que se refere a uma rede composta por objetos (também chamados de "coisas") e que incorporados com eletrônica, *software*, sensores e atuadores, podem fazer a interação entre o mundo físico e o mundo digital, sendo capazes

de gerar ou receber dados entre estes. (STOUT; URIAS, 2016), (BALDINI et al., 2016), (JOHNSTON; SCOTT; COX, 2016)

Tais objetos são aqueles que não são encontrados tradicionalmente na Internet como por exemplo: geladeiras, carros, lâmpadas, eletrodomésticos, canetas, braceletes, jaquetas, equipamentos militares, válvulas de abastecimento, circuitos de fornecimento de eletricidade, equipamentos médicos e de apoio à vida. A IoT pode atuar em diversas atividades humanas sendo possível aplicá-la nos mais variados segmentos: automação residencial (SOUMYA et al., 2016), (ANJANA et al., 2015), cuidados com a saúde (ANGELES et al., 2017), (RAJPUT; GOUR, 2016), (ISLAM et al., 2015), (NAWIR et al., 2016), suporte à vida (SILVA; SARINHO, 2016), (CHANDRAN; CHANDRASEKAR; ELIZABETH, 2016), (ABAWAJY; HASSAN, 2017), agricultura (AGRAWAL; CHITRANSHI, 2016), prevenção ou socorro em acidentes (GAO, 2016), (CHANDRAN; CHANDRASEKAR; ELIZABETH, 2016), transporte (SEHGAL; MEHROTRA; MARWAH, 2016), infraestrutura (HALIM; YAAKOB; ISA, 2016), (WEBER et al., 2016), entre outras possibilidades inerentes à viabilização de cidades inteligentes. (GOTOVTSEV; DYAKOV, 2016), (LEE; JEONG; PARK, 2016), (AKKERMANS et al., 2016), (HOU et al., 2016), (HU et al., 2017)

Conforme Kranenburg (2014, p. 38):

> Uma IoT bem-sucedida significa o melhor feedback possível sobre nossa saúde física e mental, os melhores negócios possíveis com base em monitoramento em tempo real para alocação de recursos, a melhor tomada de decisões baseada em dados em tempo real e informações de fontes abertas, os melhores alinhamentos dos meus fornecedores locais com potencial global de comunidades mais amplas.

Imaginando um cenário futuro no qual todos os objetos do cotidiano estejam conectados, seria possível mapear e identificar em tempo real situações que não fossem favoráveis para a comunidade e com isto promover melhorias para as pessoas. Exemplos de situações são: reorganização de trânsito; identificação de vazamentos em sistemas de abastecimento; identificação de acidentes de trânsito ou doméstico bem como o acionamento da emergência; redefinição de rotas de transporte de mercadorias com base em pedidos realizados em tempo real; identificação de óbitos por morte natural ou não natural (acidente ou assassinato), localização de pessoas desaparecidas, monitoramento e identificação de sinais vitais em pacientes (mesmo à distância) e indícios de risco de vida. Estes são alguns domínios que a IoT pode assessorar quando inserida. Logo, observa-se que esta citação de Kranenburg (2014) sugere a promoção do bem-estar das pessoas em decorrência da IoT.

A IoT também pode ser compreendida por meio da analogia proposta em Lucero (2016, p.4): no século XIX e início do século XX a humanidade passou pelo que o autor

denomina "*electrification*", época em que lares e indústrias passaram por uma grande transformação, de modo que hoje em dia a eletricidade se tornou algo essencial e também um facilitador para novas tecnologias que funcionam à base deste tipo de energia. Para o século atual, Lucero (2016) denomina a era "*datafication*" com impacto similar junto à humanidade. Inicialmente pela Internet e agora por meio da IoT a "*datafication*" é um requisito que se torna essencial para as pessoas e também um facilitador (no sentido de possibilitar monitoramento e fornecimento de grande quantidade de dados em tempo real) para o desenvolvimento de novas soluções aplicáveis nos mais diversos setores (Figura 6).

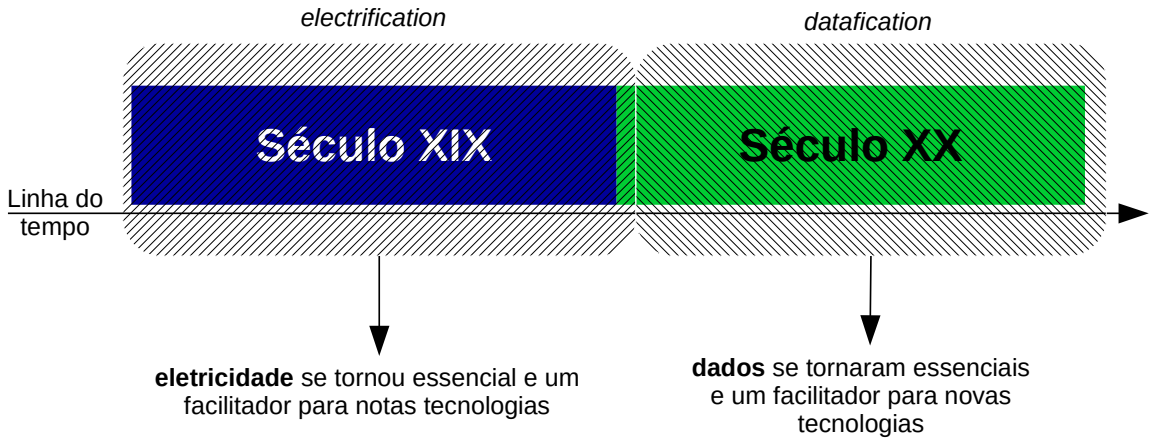


Figura 6: representação visual situando a *electrificaton* e *datafication*

Embasando-se nos exemplos de aplicabilidade, diversidade de segmentos aplicáveis, bem como pela própria definição de IoT, é válido considerar que esta tem como objetivo final proporcionar melhorias no bem-estar das pessoas. Como consequência, viabiliza o uso otimizado de recursos naturais ou artificiais, identificando desperdícios, mal uso, redistribuição, entre outros problemas e possibilidades.

Tudo isto é possível por meio do monitoramento e atuação em variáveis do ambiente ao qual a IoT esteja inserida. Isto se dá por intermédio da coleta ou geração de dados de forma autônoma, isto é, execução de ações com base em instruções pré-programadas, trocando dados entre si sem a interferência humana, agindo e reagindo de acordo com eventos no ambiente em que estejam inseridos (CERVANTES et al., 2014). Porém, o excesso de poder nas "mãos" das máquinas resulta nas seguintes situações:

a. levanta questionamentos em razão da privacidade que é o que se discute nesta tese;

b. instiga problemas com o livre arbítrio em um futuro próximo;

c. tendência ao paradoxo da automação que conforme Hollnagel e Woods (2005) diz: quanto maior for a complexidade ou quantidade de coisas interconectadas no ambiente, maior será a escala de possíveis problemas. Isto inclui o vazamento ou roubo

> de dados privados, distorção de decisões humanas, ausência ou insuficiência de dados bem como o armazenamento errôneo, refletindo diretamente no ambiente e às pessoas nele inseridas. (LEVITT, 2015)

Tais argumentos reforçam a necessidade de uma abordagem por meio da qual se possa sistematizar um direcionamento em nível de "política & governança" (Figura 3, página 24) que auxilie no tratamento de questões relativas à privacidade em face à autonomia de dispositivos.

Em termos financeiros esta é uma tecnologia emergente com previsões que alcançam valores bem elevados para o ano de 2020 a saber: 200 bilhões conforme IDC, Intel e Nations (2014), 24 bilhões conforme Intelligence (2016), 40 bilhões conforme ABI (2014) e 28 bilhões conforme Jankowski et al. (2014).

Conforme reportado em Columbus (2016) *apud* ETCIO (2016), em 2016 foram gastos com IoT o total de 120 bilhões de dólares, sendo 54 bilhões de dólares em produtos e tecnologia tais como sensores, atuadores, chips, armazenamento, plataforma IoT, entre outros; e 66 bilhões de dólares em serviços para IoT tais como gerenciamento, consultoria, entre outros. A previsão de crescimento para 2021 é estimada em 253 bilhões de dólares a serem gastos com IoT. Considerando este mercado em evidente crescimento, grandes corporações como Google, Microsoft, Cisco, Apple, tornaram-se ativas no segmento no que diz respeito à promoção da pesquisa na área (LEXINNOVA, 2014). No Brasil há em andamento o estudo "Internet das Coisas: um plano de ação para o Brasil" (BNDES, 2017). Conforme o documento, estima-se para o país um impacto econômico anual entre 50 e 200 bilhões de dólares em 2025, havendo como foco os segmentos de cidades, saúde, rural e indústrias.

Sobretudo, observa-se que este é um mercado em plena ascenção com tendência de cada vez mais se tornar algo tão comum quanto a própria energia elétrica que chega onde as pessoas se encontram.

1.3.1 Cenário IoT

O cenário IoT parte desde uma rede pessoal (também conhecida como *Personal Area Network* - PAN) até uma rede mais ampla (também conhecida como *Wide Area Network* - WAN). Há diversos protocolos de comunicação com particularidades em termos de alcance ou taxa de dados, podendo ser aplicados a situações específicas. A Figura 7 apresenta um comparativo de protocolos de comunicação demonstrando visualmente a diferença entre eles em termos de alcance máximo e taxa de dados (bits por segundo) (ALSEN; PATEL; SHANGKUAN, 2017; BAUER et al., 2015; ALLIANCE, 2017; COMPONENTS, 2017).

Observa-se que existem variedades de protocolos que podem ser aplicados aos mais diversos segmentos com base em suas necessidades. Alguns tendem à taxa de dados mais elevada ao passo que outros prezam pelo maior alcance.

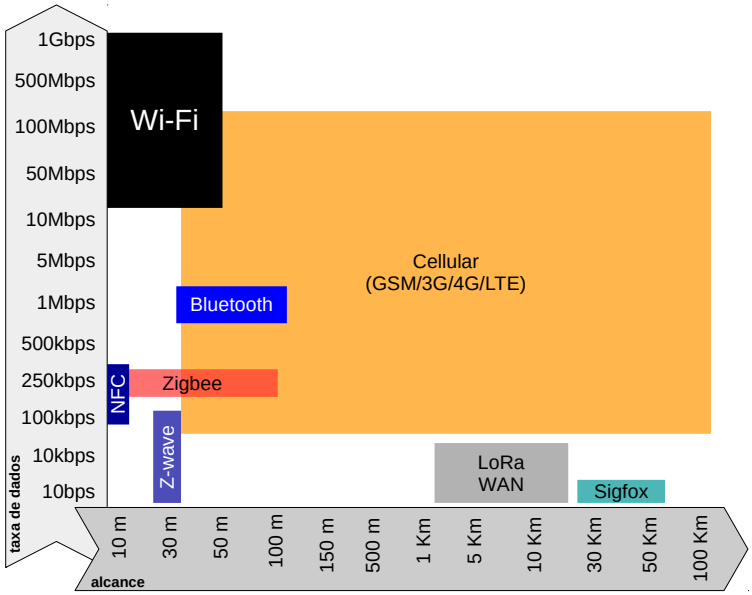


Figura 7: Protocolos de comunicação para IoT (adaptado de Alsen, Patel e Shangkuan (2017)).

Conforme Bauer et al. (2015) estes protocolos possuem como características:

- **Wi-Fi**: é largamente utilizado em residências e comércios, tornando-o um facilitador para inclusão de dispositivos IoT no ambiente, principalmente em vista da grande capacidade de taxa de dados.
- **Bluetooth**: é um protocolo intermediário entre os demais citados, sendo também comum a sua utilização para interligação de redes pessoas: periféricos de áudio, *smartphones*, dispositivos de monitoramento de saúde, *wearables*, etc. Assim como o Wi-Fi, também é um protocolo largamente utilizado pelas pessoas.
- **NFC**: é um protocolo com baixa taxa de transferência bem com baixo alcance. É indicado para aplicações de curto alcance e que não precisem de grande fluxo de dados.
- **Zigbee**: Comparando-se ao *Bluetooth*, possui uma menor capacidade de transmissão, sendo mais comum sua utilização na industria.
- **Z-wave**: A tecnologia deste protocolo reside no baixo consumo de energia. Dentre os protocolos apontados nesta tese, é um dos que possui menor taxa de transferência e alcance, o que torna-o aplicável em redes pessoais e que não precisem de tantas informações: lâmpadas, sensores, entre outros dispositivos com poucos dados.

- **LoRa Wan**: Trata-se de um dos protocolos com a menor capacidade de taxa de transferência de dados, mas destaca-se pelo longo alcance. Deste modo, torna-se uma solução útil para instalação em localidades remotas de difícil acesso e com quantidade de dados baixa, tais aplicações de monitoramento rural, medicação de índices atmosféricos, entre outros.

- **Sigfox**: Foi criado com o propósito de uso para comunicação entre máquinas, direcionado a aplicações com baixo nível de transferência de dados e baixo consumo de energia, aplicável nos mesmos ambientes sugeridos para o LoRa Wan.

- **Cellular**: Assim como o Wi-Fi, os protocolos utilizados na telefonia celular são largamente utilizados, tornando-se também um facilitador para inclusão de soluções IoT em ambiente que seja coberto por tal tecnologia. Possui alta taxa de transferência e alcance o que o torna uma das melhores formas de interligação de dispositivos IoT.

A RFC 7452 (TSCHOFENIG et al., 2015) sugere quatro modelos de padrão de conectividade para a IoT (Figura 8). No modelo (a) é considerada a comunicação de dispositivo para dispositivo, comunicação esta que faz uso de uma rede sem fio e protocolos próprios para IoT (ex.: protocolos da Figura 7). No modelo (b) considera-se a comunicação entre dispositivos IoT diretamente com um provedor de serviço remoto via Internet utilizando protocolos tradicionais da Internet (ex.: HTTP). No modelo (c) tem-se a mesma situação do modelo (b) havendo como diferencial a presença de um *gateway* local que será responsável pela comunicação com a Internet, podendo este equipamento ser o mesmo utilizado pelas pessoas para obter acesso à Internet. Por fim o modelo (d) demonstra um compartilhamento de dados obtidos pelo dispositivo IoT podendo estes dados serem acessados por terceiros autorizados.

Os quatro modelos da Figura 8 podem ser transmutados para a Figura 9 (página 43) conforme equivalência demonstrada na Figura 10 (página 44). Na primeira equivalência há apenas a comunicação direta entre dispositivos IoT por intermédio de uma rede sem fio. Neste caso, considera-se que o próprio dispositivo assuma a função de *gateway*. As equivalências dois e três demonstram que os demais modelos de comunicação culminam em uma mesma disposição que refere-se à comunicação iniciada no dispositivo IoT e se estende até o destino vinculado, comunicação esta que pode ser direta ou por intermédio de um *gateway*. A equivalência do quarto modelo limita-se até o primeiro provedor destino, pois, a partir deste trata-se de um ambiente de Internet tradicional.

Diante destas considerações, elege-se o cenário estruturado na Figura 9 para utilização nesta abordagem. Este cenário é composto pelos seguintes elementos:

- **Ambiente**: refere-se ao “alvo” de atuação. Pode ser o espaço físico, objetos do

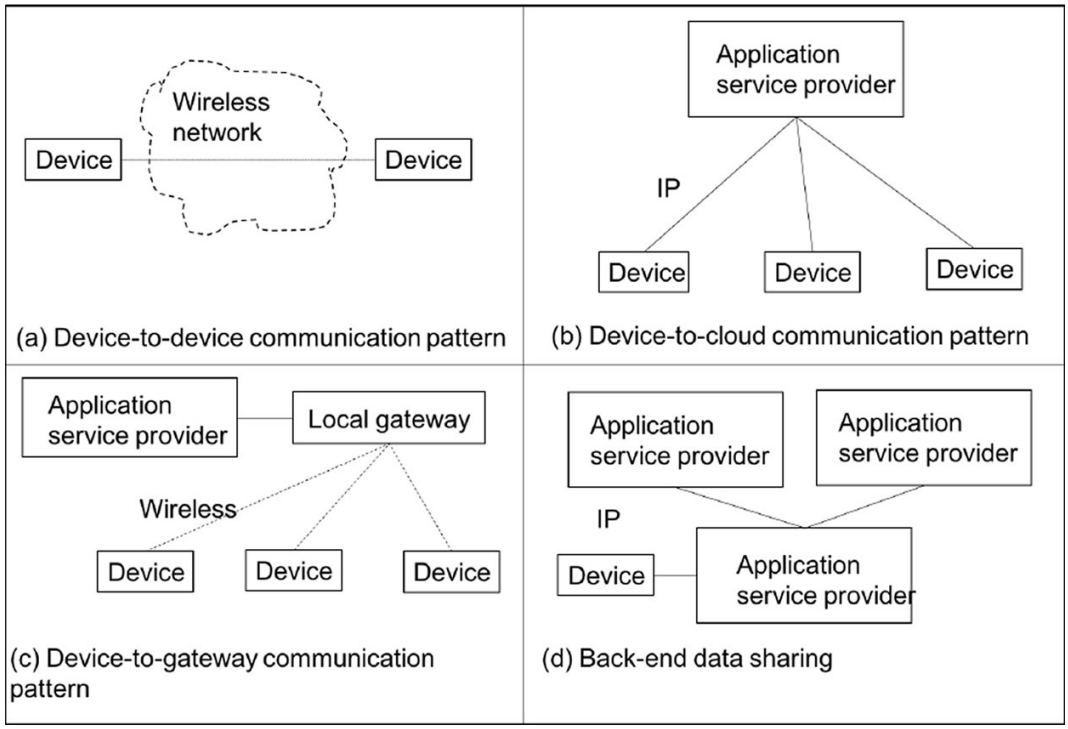


Figura 8: Padrões de comunicação para dispositivos IoT (SENGUL, 2017)

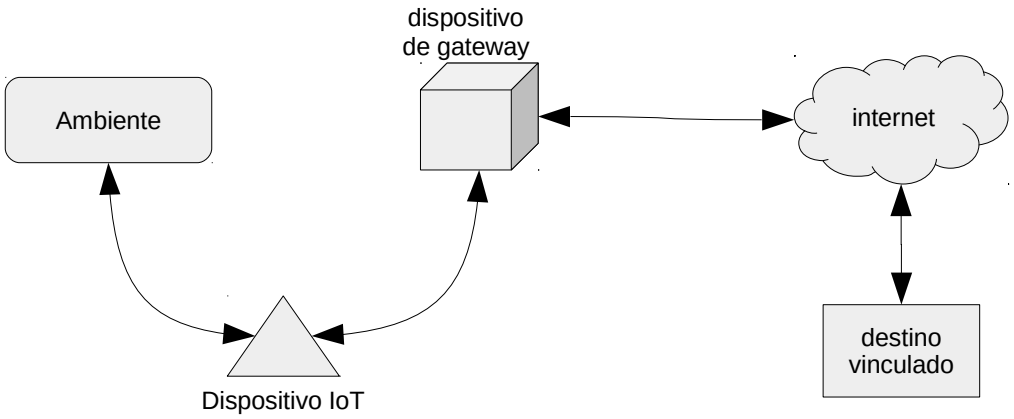


Figura 9: Composição do cenário padrão de Internet das Coisas.

cotidiano, elementos naturais, corpo humano ou qualquer outra entidade passível de atuação.

- **Dispositivo IoT**: equipamento responsável pela atuação ou coleta/geração de dados.

- **Dispositivo de *gateway***: equipamento que funciona como um portal de saída para a Internet. É por meio dele que os dispositivos IoT irão se comunicar com a Internet. Pode inclusive ser designado de forma concomitante para a função de *firewall*, tornando-se um ponto de controle entre a rede IoT (rede interna) e o mundo externo (a Internet), definindo o que pode e o que não pode passar de uma rede

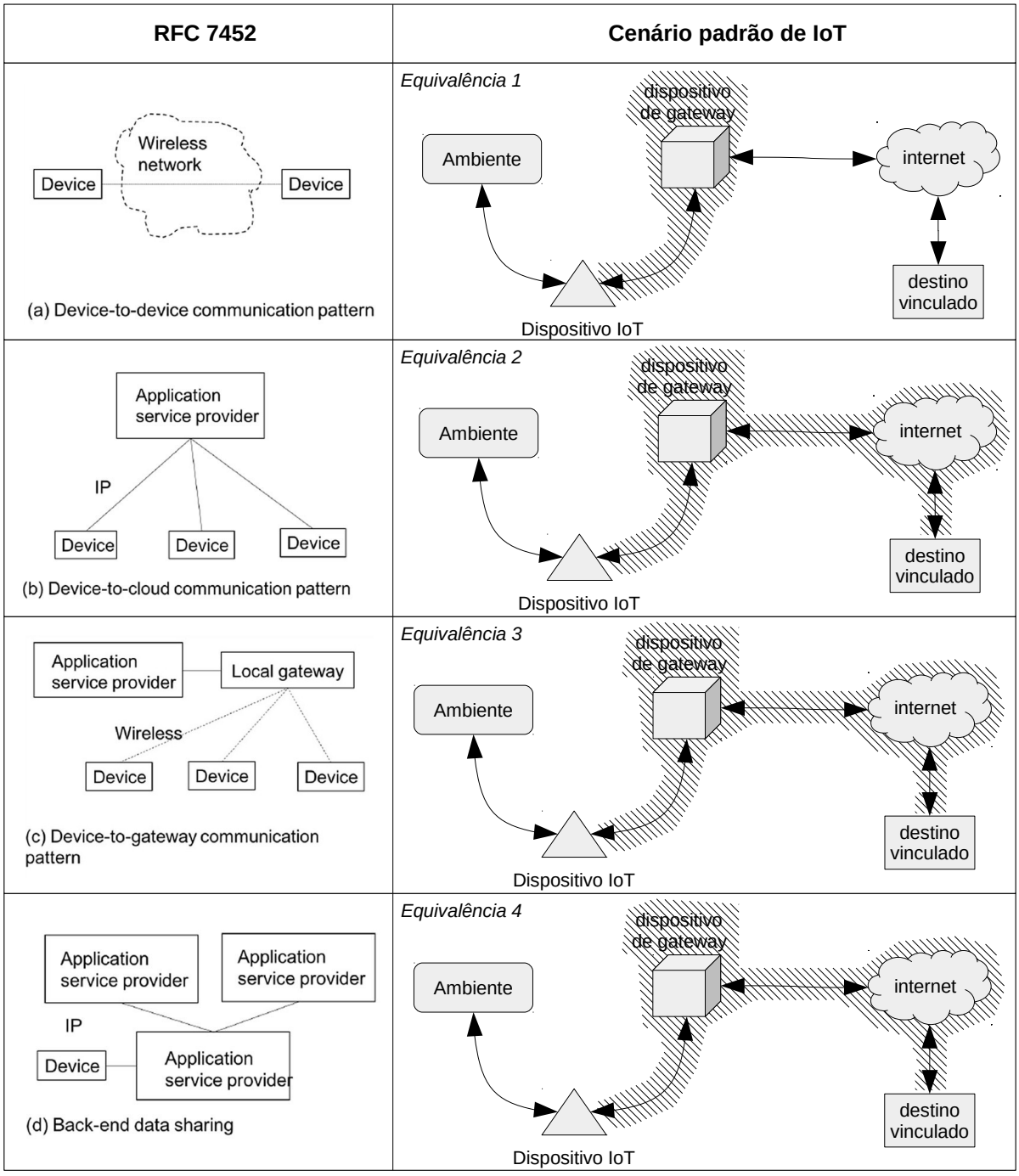


Figura 10: Equivalência entre modelos de comunicação da RFC 7452 e o modelo de cenário ora proposto

para a outra (MACHADO JR, 2015). Conforme Sengul (2017) há situações em que o próprio dispositivo IoT faz a função de *gateway*.

- **Internet**: meio usado para transmissão de dados.
- **Destino vinculado**: é o local de desígnio para os dados capturados ou gerados pelos dispositivos IoT. Pode ser um outro dispositivo IoT ou uma aplicação que fornecerá dados e informações para outros dispositivos, sistemas ou pessoas. (ISO, 2016, p. 26)

Nesta concepção (Figura 9) o dispositivo IoT recebe ou gera dados do ambiente e através do *gateway* os envia por Internet para agentes externos, os quais podem ser outros dispositivos IoT ou um serviço de processamento/armazenamento de dados em nuvem (GUBBI et al., 2013). Conforme descrito, no caso de vários dispositivos IoT atuantes no mesmo ambiente, todos eles podem fazer uso de um mesmo *gateway*. Um exemplo de funcionamento neste tipo de situação equivale a um sistema de auxílio à vida composto por diversos sensores (de batimento cardíaco, pressão, temperatura, entre outros) para um mesmo ambiente que no caso é o paciente; todos os dispositivos IoT farão uso do mesmo *gateway* para enviar os dados a um serviço remoto de armazenamento/processamento de modo a proporcionar o monitoramento à distância por parte de médicos, profissionais de enfermagem, familiares ou acompanhantes.

1.3.2 A IoT na evolução da Internet

Segundo Krumm (2010, p. 2) a evolução da computação moderna divide-se em três eras com base na proporção de computadores por pessoa (Figura 11). A primeira era é caracterizada pelo uso de computadores de grande porte (*mainframes*) em um cenário em que um único computador era utilizado por muitas pessoas em uma organização. A segunda era tem como característica o surgimento do computador pessoal, sendo possível a aquisição e uso do computador por uma única pessoa de forma dedicada. A terceira era tem como característica o aumento exponencial do uso de computadores portáteis em rede de modo que o cenário passa a ser composto de vários dispositivos computacionais por pessoa facilitando a onipresença da Internet. Por este motivo, este cenário é também conhecido por computação ubíqua.

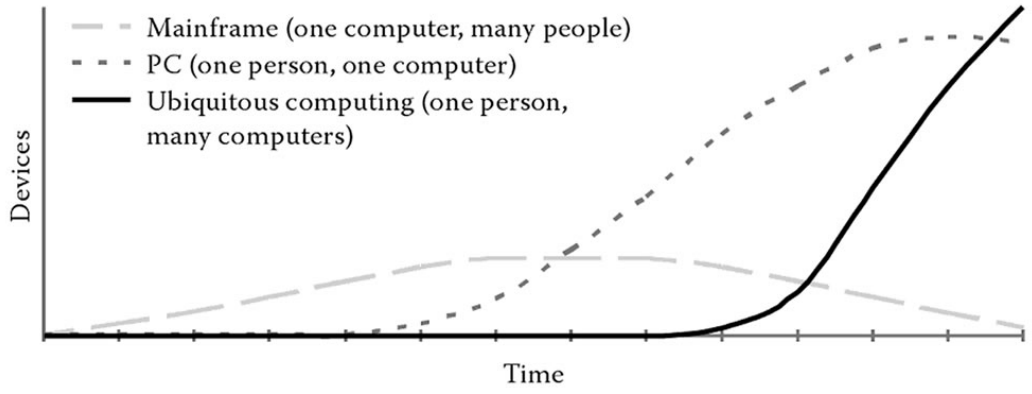


Figura 11: Representação das três eras da computação moderna (KRUMM, 2010, p.2)

Segundo Gubbi et al. (2013) a evolução da Internet também faz uma divisão em três momentos chamados de ondas: a primeira onda (denominada “www”) diz respeito às páginas *web* estáticas; a segunda onda (denominada “web2”) refere-se à *web* de rede social; e, a terceira onda (denominada “web3”) refere-se à *web* de computação ubíqua.

Esta última onda alinha-se com a pesquisa realizada por Jankowski et al. (2014) no qual tem a IoT como a terceira onda.

De fato há consonância entre Krumm (2010), Gubbi et al. (2013), Jankowski et al. (2014), Lucero (2016) e McLuhan (1964) pois todos apontam para um momento na evolução da humanidade que trás (direta ou indiretamente) a onipresença de dados em tempo real, o que é viabilizado por intermédio da IoT. Neste momento em que a humanidade adentra a porta da era da "*datafication*", tornar-se-á gradativamente mais comum o surgimento de objetos conectáveis que possibilitarão o monitoramento cada vez mais extremo de pessoas.

Considerando a criticidade da tarefa dos dispositivos IoT, bem como a quantidade deles previsto a compor a Internet nos próximos anos, tem-se um enorme campo de exploração de vulnerabilidades em termos de privacidade dentro do ciberespaço. Mesmo diante do constante avanço tecnológico, os dispositivos de IoT de uma forma geral possuem recursos muito limitados no que tange a poder de processamento, energia e armazenamento (LEVITT, 2015; SENGUL, 2017). Diante destas limitações, fatores importantes como a privacidade ficam relativamente mais vulneráveis do que em um computador ou *smartphone* tradicionalmente encontrados na Internet.

Deste modo, juntamente com a evolução tecnológica e quantidade de dados presente na rede, também é necessária a evolução da segurança da informação. Isto deve ocorrer em termos de política, governança e tecnologias, no sentido de atualização de regras, procedimentos e ferramentas a serem adotados em face à nova realidade principalmente em vista da privacidade das pessoas.

1.3.3 Indústria 4.0 e *Cyber Physical Systems*

Conforme Hermann, Pentek e Otto (2016) a expressão "indústria 4.0" surgiu em 2011 quando o governo alemão anunciou-o como uma das iniciativas chave de sua estratégia de alta tecnologia chamada *High-Tech Strategy 2020 for Germany*. Ainda conforme Hermann, Pentek e Otto (2016, p.2) e Ferber (2012) o termo foi concebido por líderes da indústria alemã, pesquisadores, associações industriais e sindicatos para descrever como a IoT poderá melhorar de forma drástica os processos de engenharia, produção, logística e gerenciamento de ciclo de vida da indústria.

Tal nomenclatura refere-se à uma quarta revolução industrial na história da humanidade, então precedida pela primeira revolução (caracterizada pela mecanização dos processos); segunda revolução (caracterizada pela inserção do uso de energia elétrica para produção em massa) e terceira revolução (digitalização ou "revolução digital", quando computadores e eletrônica proporcionaram o desenvolvimento dos processos de produção de forma automatizada) (LASI et al., 2014), (JAZDI, 2014, p.1), (DRATH; HORCH,

2014), (HERMANN; PENTEK; OTTO, 2016). A "quarta revolução" refere-se à interconexão entre o mundo real e digital, criando um novo paradigma no qual objetos do mundo real e processos virtuais estão interligados (Figura 12, página 47).

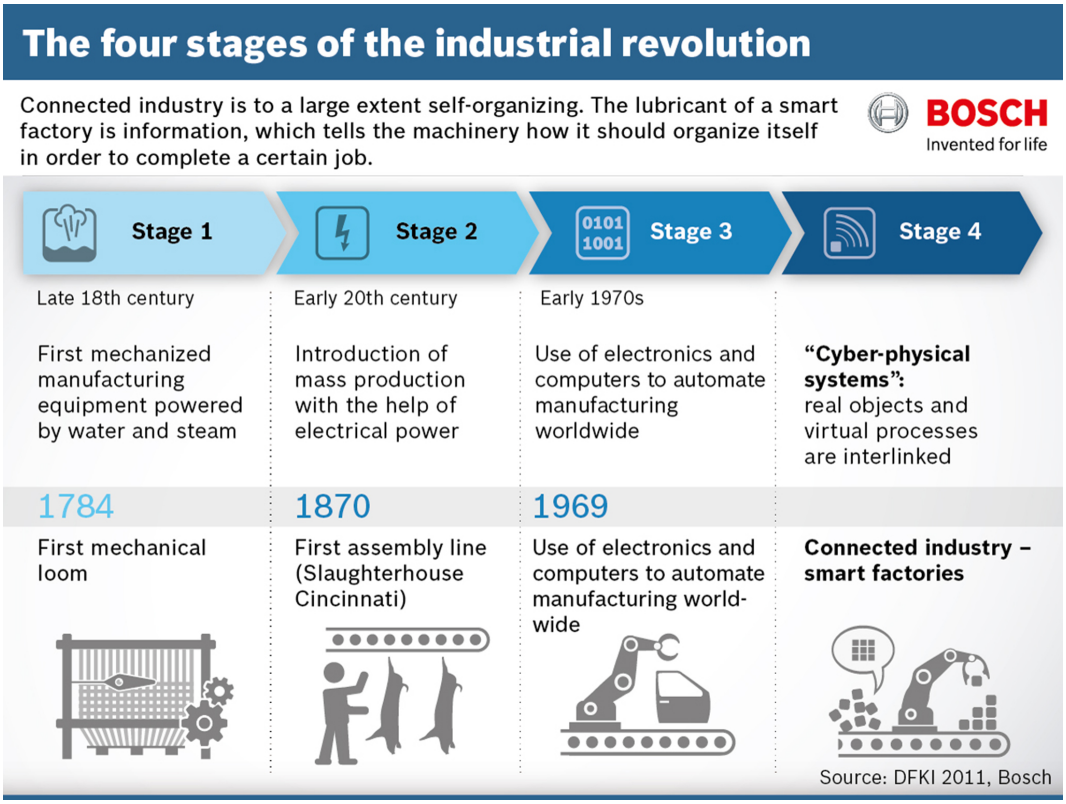


Figura 12: Os estágios da revolução industrial (BOSCH, 2016a)

Por intermédio de *softwares* instalados em objetos físicos, estes utilizam-se de sensores que captam dados do mundo real e os processa localmente ou em nuvem. Com base nos dados adquiridos o sistema no mundo digital executa ações no mundo real por meio de atuadores. Um exemplo deste tipo de tecnologia é o projeto *Romulus* (EDACENTRUM, 2016) que tem por objetivo reduzir custos de desenvolvimento e fabricação. Trata-se de um sistema multi sensor que grava, processa e transmite parâmetros de medida tais como pressão, aceleração, temperatura, entre outros, de modo que os produtos possam fornecer o seu modelo e o status de sua fabricação o que possibilita o monitoramento, suporte e definições de produção mesmo à distância (Figura 13).

Hermann, Pentek e Otto (2016) define três componentes chaves da indústria 4.0:

- ***Smart Factories***: ideia da *Internet of Everythings* (IoE) na qual pessoas, coisas e dados se conectam possibilitando novas direções para organizar e conduzir processos industriais.
- **IoT**: responsável por habilitar objetos de modo que estes possam interagir entre si e "cooperar" com seu vizinho *smart* do ambiente industrial.

Figura 13: Sistema inteligente de sensores para indústria 4.0 (BOSCH, 2016b)

- ***Cyber Physical Systems***: fusão do mundo digital e físico, integração de computação e processos físicos.

O primeiro componente descreve uma nova forma de se pensar indústria, na qual são possíveis novos modelos de negócio; integração com clientes por meio da produção customizada de cada produto; flexibilidade e mobilidade, características estas que permitem o uso de dispositivos móveis no ambiente de produção para controlar ações em qualquer espaço físico, criando uma nova dimensão de diagnóstico, manutenção e operação destes sistemas.

Os próximos componentes, isto é, IoT e *Cyber Physical Systems* (CPS) são tidos no contexto da indústria 4.0 como conceitos separados (HERMANN; PENTEK; OTTO, 2016). A IoT é responsável pela habilitação de objetos para interação ao mesmo tempo que o CPS refere-se à integração entre o mundo real e digital. Entretanto, esta conceituação não é universal e às vezes estes são referenciados como sinônimos a exemplo de Jazdi (2014), Ning et al. (2016, p.2) e Stankovic et al. (2016).

"*Cyber Physical Systems*" é uma nova área de estudos e tem como objetivo pesquisas que envolvam a comunicação entre o mundo real e digital (STANKOVIC et al., 2016). Esta interação entre ambos os mundos, então tida como o cerne da indústria 4.0 é representada visualmente na Figura 14. Observa-se por esta Figura que a linha tangente entre os dois mundos tem a IoT como mediadora. A IoT não só permite a comunicação entre objetos sem a interação humana, mas também faz a tradução entre o mundo físico e digital.

Esta emergente área de estudo trás consigo especulações acerca da segurança e

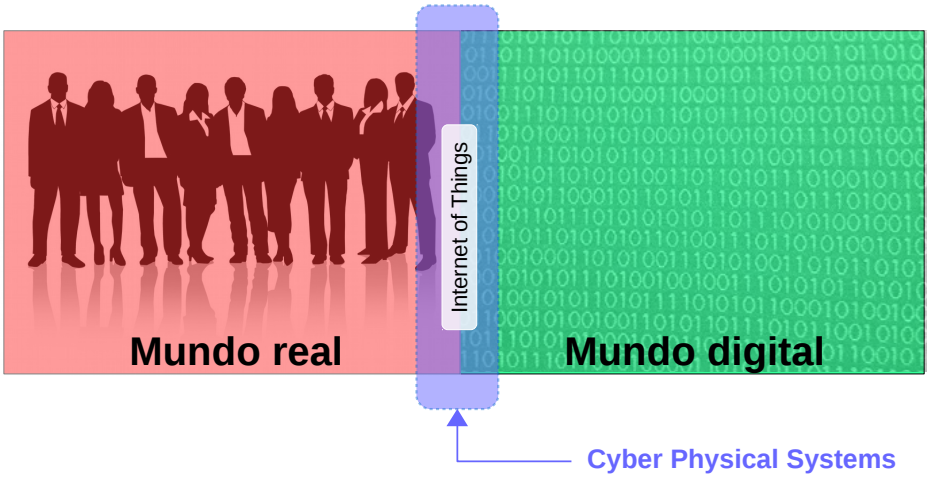


Figura 14: Representação visual do conceito de *Cyber Physical Systems*

privacidade (NING; LIU, 2012):

- Como propor uma estrutura de segurança apropriada para aplicações inteligentes das coisas?
- Como a humanidade pode participar seguramente no mundo físico e digital considerando a interconexão entre ambos?

Para responder a estas questões bem como promover a pesquisa e o desenvolvimento do tema, a Academia Nacional de Ciências, Engenharia e Medicina dos Estados Unidos[8] produziu o documento "*A 21st Century Cyber-Physical Systems Education*" (STANKOVIC et al., 2016). A primeira informação a destacar no documento é a proposta de criação de novas cátedras inerentes à CPS: inclusão de CPS em introdução à engenharia, ciência da computação e cursos afins; criação do bacharelado em Engenharia de *Cyber Physical Systems*; criação do mestrado em *Cyber Physical Systems*; e criação do programa de Ph.D em *Cyber Physical Systems*.

Stankovic et al. (2016) também propõe os princípios da integração entre o físico e o digital descrevendo-os como áreas de conhecimento nas quais estudantes precisam ter conhecimento: comunicação e rede, tempo real (sincronização de processos), sistemas distribuídos, sistemas embarcados, propriedades físicas e interação humana. Todos estes princípios são necessários para conhecer e saber trabalhar na fronteira entre o físico e o digital.

[8] originalmente fundada pelo presidente Lincoln em 1863 para ser um conselho independente em questões científicas, posteriormente incluindo os institutos de engenharia e medicina. (MEDICINE, 2017)

O documento propõe ainda como características essenciais de sistema: segurança e privacidade, interoperabilidade, confiabilidade, gerenciamento de energia, estabilidade e performance e fatores humanos e usabilidade.

O documento faz repetidos alertas às questões de segurança e privacidade de modo a tornar evidente a preocupação no tema. Isto torna esta tese alinhada aos objetivos propostos em Stankovic et al. (2016) no contexto de *Cyber Physical Systems* e indústria 4.0 ao buscar um meio para aprimorar a segurança na IoT em relação à proteção da privacidade.

1.3.4 Classificação para a IoT

Não foi identificado padrão de classificação oficial, seja do ponto de vista de tamanho do dispositivo (físico ou capacidade de processamento e/ou armazenamento), grau de risco quanto à privacidade, contexto em que seja inserido ou qualquer outro tipo de leitura. Mas algumas iniciativas tendem em favorecer algum tipo de classificação. Em Santos et al. (2015) os autores alegam que a indústria é quem deve ditar o rumo da IoT. Esta afirmação pode ser corroborada pelo fato de que diversos comitês da Figura 5 possuem como membros empresas da indústria tecnológica. A propriedade intelectual de patentes é fator determinante para evolução de novas tecnologias bem como para a alcançar uma escala de produção comercial aceitável por investidores/desenvolvedores.

A classificação internacional de patentes foi estabelecida em 1971 e é adotada por mais de 100 países, incluindo o Brasil e coordenada pela Organização Mundial de Propriedade Intelectual (WIPO, do inglês *World Intellectual Property Organization*) sediada na Suiça[9]. Tal classificação tem como índice códigos específicos para cada segmento conforme demonstrado na Tabela 3. Estas podem ser chamadas de grandes áreas, havendo subdivisões em cada uma delas. (INPI, 2015)

Tabela 3: Classificação internacional de patentes (adaptado de INPI (2015)).

Seção	**Classificação**
A	Necessidades Humanas
B	Operações de processamento; Transporte
C	Química; Metalurgia
D	Têxteis; Papel
E	Construções Fixas
F	Engenharia Mecânica, Iluminação, Aquecimento, Armas, Explosão
G	Física
H	Eletricidade

[9] Existem bases de dados nacionais em cada país, bem como a base internacional. É possivel solicitar a patente nacional ou internacionalmente. No Brasil o registro (nacional ou internacional) de marcas e patentes é realizado por meio do INPI.

Conforme constatado por meio da Tabela 3 bem como por JPO (2017) e Santos et al. (2015), não foi identificada uma classificação para IoT em termos de registro de propriedade intelectual. Deste modo, como método de levantamento quantitativo dos pedidos de registro envolvendo IoT, foram utilizados termos específicos de busca (Tabela 4) junto à base de dados da WIPO denominada PATENTSCOPE (WIPO, 2017). Nesta Tabela 4 a coluna "total" apresenta a quantidade total de registros retornados; a coluna "campo" refere-se a qual campo foi utilizado; a coluna "critérios de busca" refere-se aos textos buscados nos campos indicados e a coluna "datas" apresenta o período cronológico entre o primeiro e último registro encontrados.

Tabela 4: Buscas de pedidos de registro de propriedade intelectual armazenados na base PATENTSCOPE (WIPO)

total	**campo**	**critérios de busca**	**datas**
0	título	"internet of things" e "privacy"	
0	resumo	"internet of things" e "privacy"	
0	titulo	"internet of things" e "security"	
0	resumo	"internet of things" e "security"	
2.306	título ou resumo	"iot"	1869 à 2017
5.332	título ou resumo	"internet of things"	2008 à 2017

Fazendo uma análise da Tabela 4, observa-se que não foi identificado nenhum registro que envolva os termos "*internet of things*" e "*privacy*" conjuntamente, situação esta que leva à conclusão de que não foram submetidos internacionalmente a este órgão, pedidos de propriedade intelectual que tratem de qualquer procedimento acerca de privacidade em IoT. O mesmo foi realizado com os termos "*internet of things*" e "*security*" não havendo qualquer resultado também para esta combinação. Ainda na mesma Tabela, a busca pelo termo "iot" no título ou resumo resultou em 2.306 registros. Entretanto este resultado não foi levado em consideração em vista de ambiguidades no resultado pois outras tecnologias também utilizam tal sigla, inclusive observa-se que o período retornado começa em 1869, época que não se tinha Internet ou IoT. Contudo é importante observar que quando o autor utiliza o termo "iot" com intuito de referenciar *internet of things*, a expressão por extenso também é incluída, então desta forma o critério de busca somente pela sigla foi eliminado da pesquisa.

Por fim, na última linha da Tabela 4 na qual foi utilizado como critério o termo "*internet of things*" no título ou no resumo, obteve-se um total de 5.332 registros sendo este critério utilizado para continuação da pesquisa.

Por meio de uma análise também gerada por WIPO (2017) e demonstrada na Figura 15, observa-se que a China é o país com maior manifestação de registros em nível internacional junto a este órgão. Entretanto, o Japão é o país que se tornou o pioneiro na preocupação com a forma de registro de patentes. Conforme JPO (2017) o Japan Patent Office definiu e começou a utilizar (desde novembro de 2016) uma nova classificação de

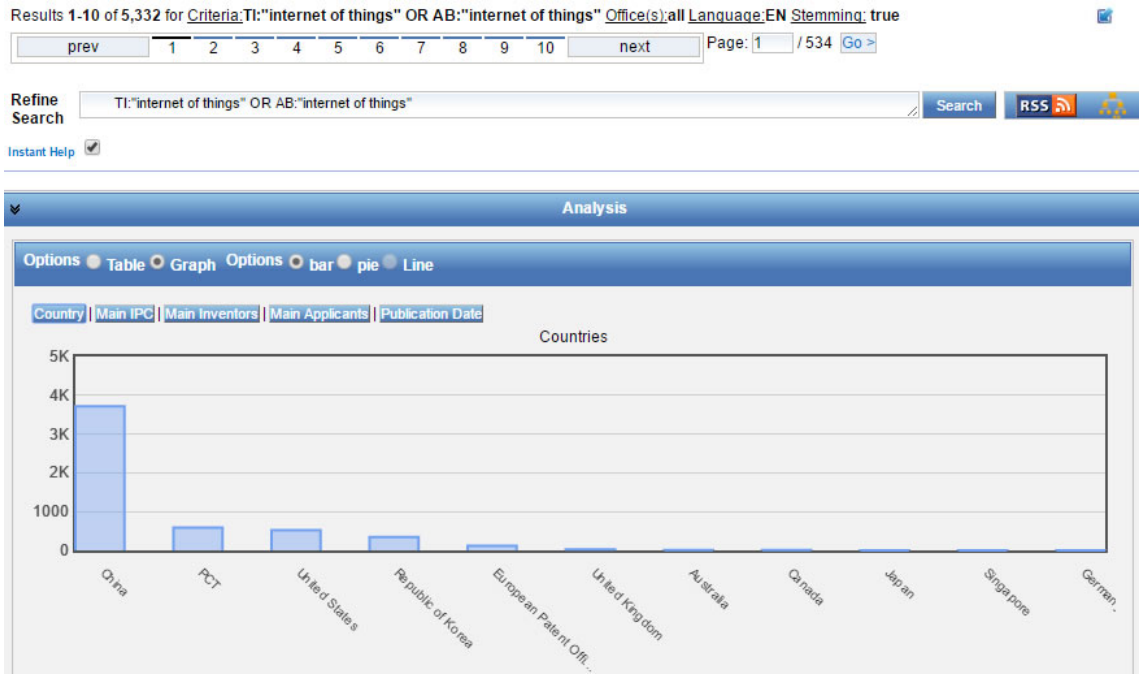


Figura 15: Quantidade de patentes registradas em WIPO (2017) conforme critérios da última linha da tabela 4

patente para uso exclusivo naquele país. Em fevereiro de 2017 esta proposta passou para a fase de revisão para que em janeiro de 2019 este seja utilizado em nível internacional.

Fazendo uma busca junto a este órgão utilizando o método descrito em JPO (2017), foram encontrados 445 registros de pedido classificados como IoT. Porém não foi possível identificar separadamente o tipo de contexto no qual cada pedido de registro se enquadra, mas tal informação foi disponibilizada em JPO (2017) conforme observa-se pela Figura 16. Esta Figura apresenta a distribuição de uso específico de documentos alocados na nova classificação de patentes e evidencia-se a categoria de *health care* e afins como a mais frequente em pedidos de registro, seguida pela categoria de transporte, diversão/esporte/games, serviços e por fim as demais categorias.

LexInnova (2016) é um *whitepaper* que faz uma análise perspectiva acerca de patentes de IoT no ano de 2016. Tal empresa utilizando-se de sua ferramenta proprietária[10], apresenta uma taxonomia (Figura 17) na qual são elencados os registros de patente de acordo com os tipos de aplicação/uso envolvidos. Dentre os 5.009[11] registros encontrados, nos quais em ordem de maior frequência são as patentes que envolvem protocolos de comunicação, serviços especialmente adaptados/dispositivos, segurança de dados, recuperação da informação e demais.

[10] LexScore é uma ferramenta proprietária da LexInnova para levantamento de informações sobre propriedade intelectual (LEXINNOVA, 2014, p. 11). Faz uso um algoritmo proposto em Allison et al. (2003). Apesar de requisitado não foi concedido acesso à ferramenta nem geração de outros possíveis relatórios.

[11] O documento data de 2016, sendo que em 2017 conforme a tabela 15 o total de registros é de 5.332, diferença esta justificada pelas datas de busca (uma em cada ano).

Category of specific use
for health care, e.g. hospitals, medical treatments or diagnosis; for social work
for transportation
for amusements; for sports; for games
for service
for communication
for manufacturing
for home and buidling; for home electric appliances
for agriculture; for fishing; for mining
for supplying electricity, gas or water
for finance
for construction
for logistics, e.g. warehousing, loading, distribution or shipping
others

Figura 16: Distribuição de uso específico de documentos alocados na classificação IoT (JPO, 2017)

Level 1	Level 2	Level 3	Patent Applications
Networking	Wired	Communication Protocols	5,009
		Resource Management	1,746
		Light Guides/Optical Elements	66
		Multiplexing Methods	419
		Topology Management	677
	Wireless	Resource Management	1,501
		Specially adapted services/devices	3,747
		Traffic Management	2,815
		Access/Authentication	3,035
		Connection Management	2,598
		Topology Management	1,538
		Communication Protocols	714
		Multiplexing Methods	2,357
		EMW/ Radio Waves	1,706
		Baseband Processing	406
	Area Based Networks (LAN/WAN)		1,198
	Switching Systems		1,778
	Measurement/Testing		928
Computing	Algorithm	Routing Algorithms	696
		Image Processing	2,777
		Character Recognition	170
		Others	1,295
	Encryption	Error Correction	921
		Data Security	3,198
		Data Encryption	2,110
	Memory Management	Information Retrieval	3,179
Infrastructure	Control Systems		2,359
	Power Supply/ Management		1,440
	Hardware	Circuits	1,852
		Waveguides	116
		Acoustics	46
		Sensors	756
Miscellaneous Patents	Applications	Transportation	2,020
		E-commerce	2,939
		Entertainment	391
	Others		219

Figura 17: Taxonomia de patentes de IoT proposta em LexInnova (2016, p.8)

Confrontando estas análises (Figura 15 e Figura 16), deduz-se que as aplicações IoT para *health care* e afins envolvem com frequência questões relativas à comunicação de dados, criação ou adaptação de dispositivos existentes, segurança dos dados envolvidos bem como a recuperação correta de informações. Ou seja, a preocupação com a precisão

dos dados, seja na sua recuperação ou transmissão, bem como a segurança destes é fator essencial nos pedidos de registro de propriedade intelectual para IoT.

2 SEGURANÇA DA INFORMAÇÃO: EVOLUÇÃO E MODELOS

Há uma grande abundância de informação disponível e que pode ser consumida por todos que estão na Internet através de seus dispositivos tecnológicos espalhados pelo globo e estações espaciais através da *Crew Support LAN* [1]. Visualizando este emaranhado de corporações interligadas e em alguns casos, extremamente competitivas, o valor da informação cresce exponencialmente, transformando em um fator essencial para a criação e mantença dos mais diversos róis de negócios e devido a isto, sua proteção se torna primordial. O valor destas informações se torna exponencialmente maior no contexto de uma ataque cibernético, o que torna a IoT um potencial meio de aquisição de informações confidenciais. O foco da segurança da informação se faz na conscientização das pessoas que utilizam o sistema em ações contínuas seguras. Entretanto, há uma busca na garantia absoluta na segurança, que se frustra quando o sistema permite acesso ilegítimo.

Para atingir o seu objetivo fim, a segurança da informação é um somatório de ações, políticas, regras e controles rígidos. Tem como característica sua interdependência e total compromisso dos níveis hierárquicos corporativista, clareza e objetividade em seus princípios de segurança, reflexo do negócio da corporação em suas políticas de segurança e orientação direcionada nas ocorrências de incidências de acessos ilegítimos, quando ocorrer.

A preocupação com o fator segurança da informação sempre esteve presente na humanidade principalmente no contexto militar e industrial. Entretanto, antes da era da computação não era algo que requereu tanta preocupação. Com a introdução dos equipamentos informáticos no segmento de forças armadas e governos, tal preocupação passou a ser melhor considerada e precisava de documentação que oficializasse procedimentos em relação às novas possíveis ameaças. Este documento é a política de segurança. Nele deve constar toda o embasamento para questões relacionadas à segurança da informação. Conforme Nakamura e Geus (2007, p. 188) a política de segurança é um documento unanime em recomendações provenientes de três meios: o meio militar, o meio técnico/acadêmico e o meio empresarial. Os militares foram os primeiros a produzir documentos relativos à segurança, seguidos pelo meio acadêmico e mais recentemente pelo meio empresarial como exposto em seguida.

[1] Sistema que permite aos astronautas acessarem a Internet a partir da Estação Espacial Internacional. (YEMBRICK, 2010)

2.1 CIA-triad: o tripé da segurança da informação

Conforme Dantas (2011), Cherdantseva e Hilton (2013), ISO (2013b), Whitman e Mattord (2015), e Defesa (2012) a pesquisa acadêmica bem como os modelos de segurança da informação corporativos e militares possuem como princípios fundamentais a tríade **confidencialidade, integridade** e **disponibilidade**. Este conjunto é conhecido como o tripé da segurança da informação, internacionamente denominado "*CIA-triad*" em referência aos termos *Confidentiality, Integrity* e *Availability*.

Existem outros objetivos de segurança como o não repúdio, a autenticidade, a utilidade, etc. Estes não são objetivos básicos mas foram sugeridos através de modelos posteriores os quais também serão abordados neste capítulo.

A Figura 18 (pág. 57) expõe a linha de tempo com referência às publicações que moldaram o estudo de gestão e política de segurança da informação. Os eventos pertinentes à esta evolução são descritos como se segue.

A origem da CIA-triad remonta às décadas de 1960 e 1970 (Figura 18). A pedido de uma força tarefa especial do Departamento de Defesa dos Estados Unidos da América, um estudo iniciado em 1967 pela RAND[2] resultou em uma publicação técnica em fevereiro de 1970. Este documento é conhecido como *RAND Report R-609*[3] (intitulado *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security*). Conforme Samonas e Coss (2014, p. 23) e Whitman e Mattord (2015, p. 5) esta é considerada a publicação que deu início ao estudo em gestão e política de segurança. Seu conteúdo ainda não caracteriza a tríade, mas ele compõe a base para que esta venha a ser cunhada em trabalhos futuros.

O RAND Report R-609 (também conhecido como "*The Ware Report*" em referência ao nome do autor) descreve os seguintes tipos de vulnerabilidades contra as quais um sistema de segurança deve prover proteção:

a. **divulgação acidental**: uma falha de *hardware*, *software* ou subsistemas que resulte na exposição de informação ou violação do sistema.

b. **penetração deliberada**: uma falha na qual uma invasão possibilite o comprometimento do sistema tornando-o não confiável.

c. **infiltração ativa**: método no qual um usuário legítmo passa a ter acesso a subsistemas ou áreas aos quais ele não tenha autorização.

[2] *RAND Corporation* é uma organização fundada em 14 de maio de 1948 (após a segunda guerra mundial) sem fins lucrativos e que promove pesquisa e análises com finalidade de melhoria na política e tomada de decisões (RAND, 2016).

[3] Em `http://www.rand.org/pubs/reports/R609-1/index2.html` é possível acessar o *RAND Report R-609-1*, que é uma reedição realizada em 1979 pelo próprio autor, Willis H. Ware, substituindo o documento original com algumas melhorias (não especificadas no *site*).

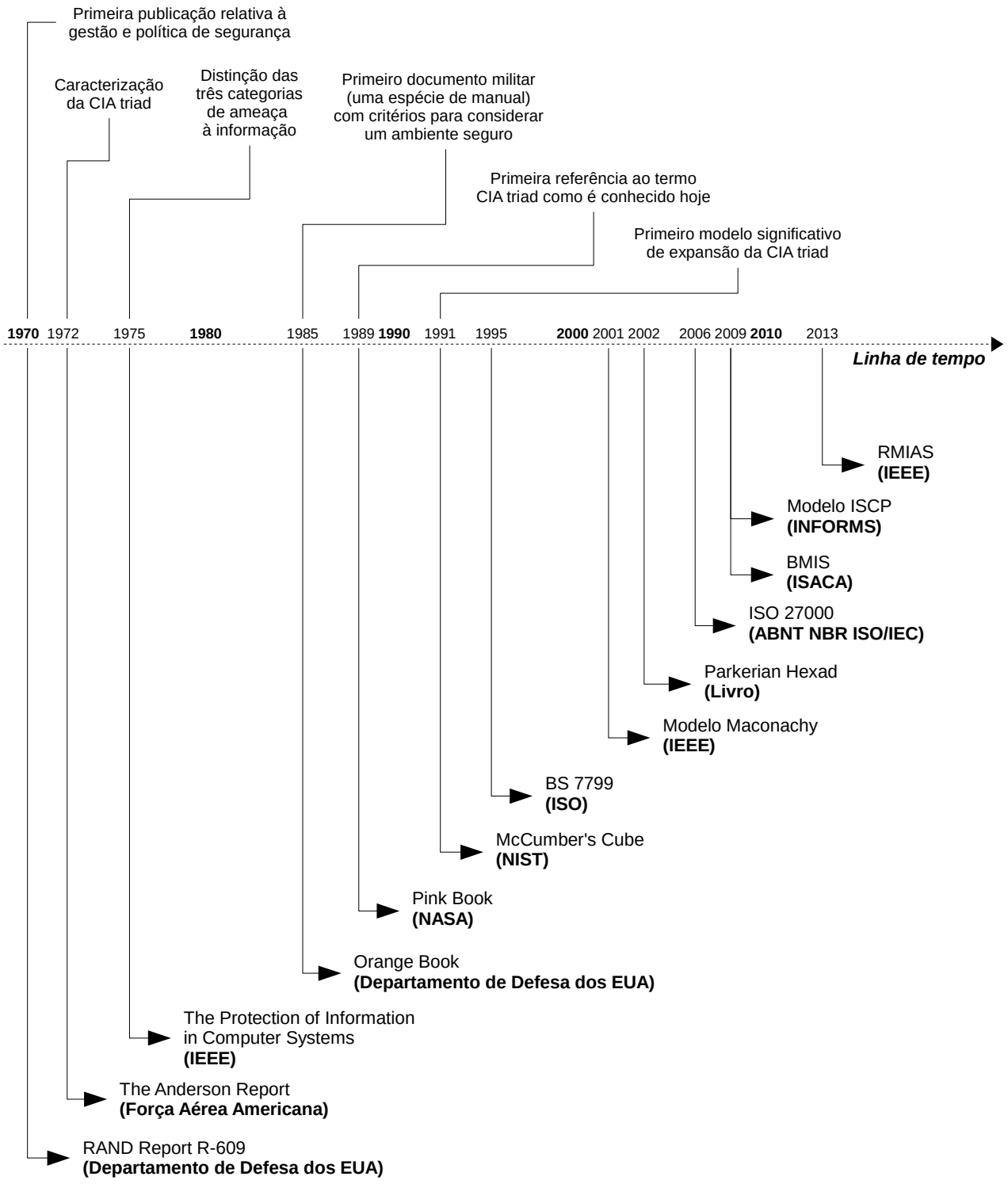


Figura 18: Histórico de evolução da CIA-triad e modelos de expansão.

d. **subversão passiva**: utilização de meios para monitorar informações residentes no sistema ou transmitidas de/para o mesmo.

e. **ataque físico**: refere-se à possibilidade de um ataque físico ao ambiente em que o sistema esteja localizado.

Considerando tais vulnerabilidades o RAND Report R-609 definiu três princípios fundamentais de segurança os quais podem ser considerados predecessores da CIA-triad e que seriam suficientes para o combate às possíveis ameaças (WARE, 1979):

i os sistemas deverão acomodar sem excessão, a responsabilidade individual e assegurar que informações que afetem a defesa nacional estejam protegidas da divulgação não autorizada.

ii o sistema informático deverá conceder acesso à informação classificada somente a pessoas com autorização para tal.

iii os meios para atingir os objetivos de segurança devem basear-se em uma combinação de *hardware*, *software* e medidas processuais suficientes para assegurar a proteção adequada para todas as categorias de informação protegidas.

Observa-se pelos princípios "i" e "ii" a preocupação quanto ao acesso de informações somente a quem seja autorizado, o que caracteriza o cuidado implícito com a privacidade, uma vez que refere-se às informações classificadas[4].

Continuando a linha temporal proposta na Figura 18, em outubro de 1972 ocorre a publicação de outro documento técnico intitulado *Computer Security Technology Planning Study* (ANDERSON, 1972) (também conhecido como "*The Anderson Report*" em referência ao nome do autor), trabalho este desenvolvido para a Força Aérea dos Estados Unidos da América. Conforme Samonas e Coss (2014) o *Anderson Report* identificou três categorias de potenciais riscos à segurança os quais se tornaram a CIA-triad:

i **liberação de informação não autorizada**: uma pessoa não autorizada consegue obter informações armazenadas no computador. Esta categoria pode se estender à análise de tráfego, na qual o atacante pode observar todo o tráfego de dados de/para o computador alvo, equivalendo-se ao princípio da confidencialidade.

ii **modificação de informação não autorizada**: uma pessoa não autorizada é capaz de alterar informações armazenadas, o que equivale ao princípio da integridade.

iii **negação não autorizada de uso**: um atacante poderia privar um usuário autorizado a usar o sistema, equivalendo-se ao princípio da disponibilidade.

[4] Algo que será discutido em capítulo posterior no que diz respeito à etimologia do termo "privacidade".

Na sequência cronológica, em setembro de 1975 o artigo intitulado *The Protection of Information in Computer Systems* foi a primeira publicação de cunho acadêmico relativo à gestão e política de segurança da informação (SALTZER; SCHROEDER, 1975). Dentre os princípios básicos de proteção da informação descritos no documento, estão a confidencialidade, a integridade e a disponibilidade, inclusive utilizando como referência o *Anderson Report*. Conforme Samonas e Coss (2014), neste documento distingue-se as três categorias de ameaça à informação e que são equivalentes aos do *Anderson Report*:

i *unauthorised information release* (equivale à confidencialidade);

ii *unauthorised information modification* (equivale à integridade);

iii *unauthorised denial of use* (equivale à disponibilidade).

Dez anos depois (em dezembro de 1985) foi publicado Latham (1985), que foi o primeiro documento militar (um manual) com critérios para que um ambiente fosse considerado seguro. O documento intitulado *Department of Defense Trusted Computer System Evaluation Criteria* também conhecido como *Orange Book* em referência à capa do documento é um manual norte americano aplicável ao gabinete do Secretário de Defesa, departamentos militares, comandos especiais e organização de chefes de estado maior daquele país. O *Orange Book* estabeleceu seis requisitos fundamentais para a segurança computacional (LATHAM, 1985):

i ***security police***: deve haver uma política de segurança explícita e bem aplicada. Deve haver um conjunto de regras usadas pelo sistema para determinar se um usuário pode ter determinado acesso. A política de segurança deve ser obrigatória de forma que a implementação de regras de acesso seja eficaz.

ii ***marking***: rótulos de controle de acesso devem ser associadas aos objetos. Para controlar o acesso às informações armazenadas no computador, de acordo com a política de segurança cada objeto deve ser marcado com um rótulo que identifique de forma confiável o nível de sensibilidade da informação.

iii ***identification***: todos os indivíduos devem ser identificados. Cada acesso à informação deve ser mediado com base em "quem" está acessando e quais classes de informação o usuário está autorizado.

iv ***accountability***: informações de auditoria devem ser mantidas e protegidas de forma que ações que afetem a segurança sejam rastreadas até o responsável (responsabilização de pessoas).

v ***assurance***: o sistema computacional deve ter mecanismos de *software* e *hardware* que possam independentemente garantir que o sistema aplique os requisitos "i" ao "iv".

vi ***continuous protection***: os mecanismos que impõem estes requisitos básicos devem ser continuamente protegidos contra adulteração e/ou alterações não autorizadas.

É possível identificar as características da CIA-triad nos seguintes requisitos sob os quais o documento se embasa:

a. A **confidencialidade** equivale aos requisitos *marking, identification, accountability* uma vez que a rotulação, identificação e informações de auditoria, estão diretamente ligados à questão da confidencialidade.

b. A **integridade** equivale ao requisito *assurance* uma vez que este diz respeito aos mecanismos para que todos os critérios funcionem, inclusive verificação de integridade do sistema conforme Latham (1985, p. 15).

c. A **disponibilidade** equivale também ao requisito *assurance* uma vez que a verificação de integridade do próprio sistema é o que permitirá a garantia deste pilar da segurança.

Por fim, conforme Cherdantseva e Hilton (2013, p.2-3) o termo CIA-triad apareceu em 1989 em um documento da *National Aeronautics and Space Administration* conhecido como *The Pink Book* [5]. A partir deste ponto na linha de tempo, os termos confidencialidade, integridade e disponibilidade se consolidaram como a CIA-triad e servindo como pilares de sustentação para a segurança da informação. Considerando o período entre o estudo iniciado em 1967 pela RAND e esta citação de 1989, tem-se que foram praticamente mais de vinte anos de estudos para que a tríade confidencialidade-integridade-disponibilidade fosse consolidada. A Figura 19 (pág. 61) demonstra visualmente a evolução da CIA-triad através da correlação entre os documentos citados.

2.1.1 Confidencialidade

O aspecto da confidencialidade é o primeiro a ser lembrando quando se fala em segurança da informação. Ele diz respeito à ameaça de liberação não autorizada de informações. Este requisito busca garantir o acesso somente com autorização, ou seja, para que uma informação seja considerada segura é essencial que haja uma forma de garantir esta seja disponibilizada somente mediante autorização. Deve haver um mecanismo de

[5] Mission Operations Directorate Automated Information Systems Security Manual, JSC 23982 (COYNE, 1995) *apud* (NASA, 1990).

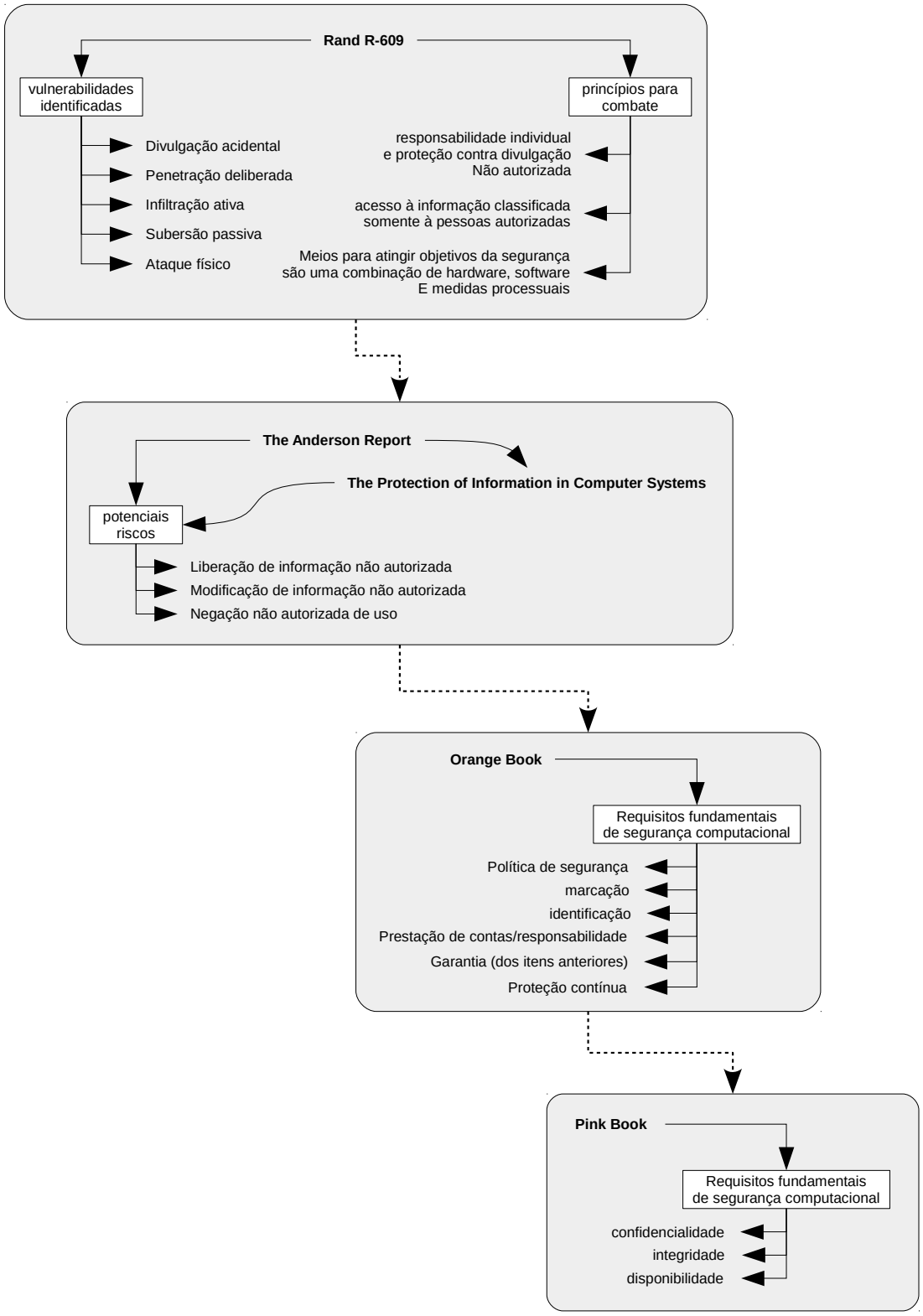


Figura 19: Evolução das características de segurança CIA-triad através da correlação de documentos levantados.

barreira que impeça o acesso direto. São exemplos de uso da confidencialidade qualquer ambiente controlado que seja acessível apenas mediante uso de chave de acesso: servidor

de banco de dados, conta de e-mail, sala cofre, área específica de uma empresa, entre outras possibilidades. (DANTAS, 2011; CHERDANTSEVA; HILTON, 2013; WHITMAN; MATTORD, 2015)

O mecanismo de barreira pode ser aprimorado através de recursos de criptografia para ofuscar os dados protegidos diante de terceiros (STALLINGS, 2008, p. 17-33). Podem ser utilizadas técnicas clássicas de criptografia por meio de cifra simétrica (mesma chave para encriptar e decriptar os dados) ou assimétrica (chaves diferentes para encriptar e descriptar dados). Os modelos de segurança em nível de política & governança não enfatizam em detalhes a melhor técnica criptográfica, cabendo esta definição ao nível operacional de *software*.

2.1.2 Integridade

O aspecto da integridade diz respeito à ameaça da modificação não autorizada de informações. Este requisito busca garantir que a informação não sofra alterações indevidas. Espera-se que a informação seja disponibilizada de forma completa e sem qualquer tipo de modificação (DANTAS, 2011; CHERDANTSEVA; HILTON, 2013; WHITMAN; MATTORD, 2015). A quebra da integridade é fator crítico e pode ter consequências catastróficas. São exemplos de uso da integridade qualquer ambiente controlado em que o sucesso das operações depende da qualidade íntegra dos dados fornecidos. O monitoramento de sensores ou radares no contexto militar é essencial para a defesa de um país. De nada adianta sistemas de radar ou sensores que não forneçam dados reais, isto é, adulterados de alguma forma, dando a falsa impressão de segurança ao não registrar objetos ou fenômenos no céu, terra ou mar; no contexto civil, o uso de sistema GPS com a integridade comprometida pode induzir a locomoção a um local propício para sequestro ou roubo; no contexto de saúde, a integridade é crucial, principalmente pelos sistemas que integram uma unidade de tratamento intensivo (UTI). Equipamentos não podem fornecer dados errôneos em relação à saúde do paciente.

Contudo, um último fator de grande importância em relação à integridade diz respeito à necessidade do melhor conhecimento possível (por parte do operador) do ambiente onde as operações ocorrerão. Este conhecimento é fator chave na interpretação dos dados críticos e viabilizam a identificação mais rápida de possível quebra de integridade.

2.1.3 Disponibilidade

Por fim tem-se o aspecto da disponibilidade, o qual faz referência à ameaça de negação não autorizada de uso. O objetivo deste pilar é garantir a propriedade da informação estar disponível quando solicitada. (DANTAS, 2011; CHERDANTSEVA; HILTON, 2013; WHITMAN; MATTORD, 2015)

Este talvez seja o primeiro pilar a sofrer ataques cibernéticos, pois a indisponibilidade de sistema pode ocasionar vantagens diante do ambiente que dependa deste. É o que se busca um ataque do tipo *distributed denial of service* [6] (DDoS). Um ataque deste tipo pode retardar ações militares (indisponibilizar sistema de defesa, sistema de *login*, etc.), comprometer tomadas de decisão no ambiente empresarial (indisponibilidade de dados ou informações comerciais em tempo real, etc.) ou até mesmo levar a óbito um paciente por falta da informação que deveria estar disponível para a equipe médica.

Em termos computacionais a disponibilidade pode ser mantida através do armazenamento em nuvem. Os recursos atuais permitem comprovadamente[7] que os dados e informações possam ficar online 99,995% do tempo o que equivale a um período de *downtime* de 0.4 horas/ano, ou seja, a indisponibilidade dos dados pode ocorrer por menos de uma hora durante um ano inteiro. (VERAS, 2015, Tab. 5-3 e Fig. 5-7)

Fazendo uma breve análise, pode-se concluir previamente que entre os três pilares, a quebra da disponibilidade seria a forma mais eficiente de se iniciar um ataque. Uma vez quebrada a disponibilidade, na sequência poderia-se comprometer a integridade através da adulteração ou substituição de dados (ação realizada enquanto os dados não estão disponíveis ao usuário legítmo) e por fim comprometendo o sistema alvo talvez mesmo sem mitigar o aspecto da confidencialidade. Deste modo, ao implementar um plano de segurança da informação, convém que todos os pilares (Figura 20) em igual nível de relevância sejam atendidos.

Em 1999 ocorreu a publicação da primeira versão da norma ISO/IEC 15.408, conhecida como *Common Criteria* (ISO/IEC, 1999). Este documento não propõe evolução à CIA-triad, mas descreve métodos para avaliação de atributos de segurança em TI. (ALMEIDA, 2007)

2.2 Modelos baseados na CIA-triad

Em nível de política & governança diversos autores propuseram modelos de referência para segurança da informação. Cada um deles com uma proposta de incremento à CIA-triad. Em todos eles é possível identificar a CIA-triad ou a essência de seus elementos.

A linha temporal da Figura 18 (pág. 57) também apresenta o surgimento de novos modelos propostos. Em 1991 McCumber (1991, p. 328-337) propõe um modelo de referência conhecido como *McCumber's Cube* (Figura 21). Este modelo é representado por um

[6] Método usado para negar a usuários legítimos o acesso a determinado computador. Basicamente caracteriza-se pelo envio de muitas requisições a um servidor de forma que ele seja inundado e não consiga responder a todas, tornando-se assim inutilizável. (SYMANTEC, 2016)

[7] A norma TIA-942 é uma certificação específica para datacenters que faz a definição e a classificação em quatro níveis ou camadas (*tiers*) com base em: arquitetura e estrutura, telecomunicações, aspectos elétricos e mecânicos. Estes quatro *tiers* são índices, sendo que o de valor mais alto corresponde aos dados aqui fornecidos conforme Veras (2015, cap. 5).

Figura 20: CIA-triad: o tripé da segurança da informação

cubo tridimensional. A primeira dimensão é composta pela CIA-triad, isto é, os aspectos de integridade, disponibilidade e confidencialidade ao qual os autores chamam de características de informações críticas. Na segunda dimensão estão os possíveis estados em que a informação pode estar, isto é, armazenamento, processamento e transmissão. Por fim, na terceira dimensão encontram-se as medidas de segurança, ou seja, mecanismos necessários para atender às caracterísitcas críticas nos possíveis estados em que a informação estiver. Estas medidas são a "tecnologia" (técnica implementada em *hardware*, *software* ou *firmware* como por exemplo: dispositivo biométrico, módulo criptográfico ou sistema operacional), a "política e prática" (é o reconhecimento do fato de que o sistema de informações seguras não é um produto que venha a ser disponibilizado futuramente) e por fim a "educação, treinamento e consciência" (considerado pelos autores como a medida proeminente do modelo, pois a compreensão das ameaças e vulnerabilidades associados ao sistema em questão, permite lidar efetivamente com as medidas de controle).

Conforme Tong e Wong (2008, p. 5-6) foi por volta desta mesma época que ocorreu o nascimento da norma ISO 27000, atualmente adotada no meio corporativo e passível de certificação no Brasil através da ABNT/NBC ISO 27000[8]. Seu ponto de origem foi em 1989 quando o UK *Department of Trade and Industry's* (DTI)[9] *Comercial Computer Security Centre* (CCSC) publicou um documento chamado *Users Code of Practice* que posteriormente veio a ser publicado como *British Standard* BS 7799:1995. Esta norma britânica era um código de prática para gerenciamento de segurança da informação e serviu como base para a criação das normas ABNT/NBR ISO IEC 17799-1 (requisitos

[8] Série de certificações criadas pela *International Organization Standardization* relacionadas à segurança da informação: código de práticas para segurança, contingência, segurança em nuvem, entre outros. `http://www.iso.org/`

[9] `https://www.gov.uk/government/organisations/department-of-trade-and-industry`

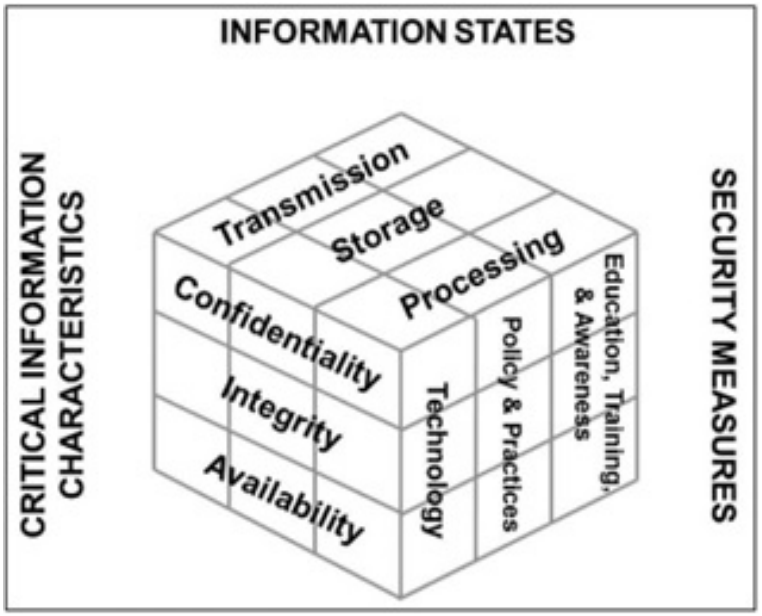


Figura 21: McCumber's Cube (MCCUMBER, 1991)

para sistema de gestão de segurança da informação) e 17799-2 (código de prática para a gestão de segurança da informação) que a partir de 2006 foram publicadas como série 27000 por questões de padronização, passando então a serem nomeados 27001 e 27002 respectivamente. A norma ABNT NBR ISO/IEC 27001 (ISO, 2013a) atua como uma lista de requisitos de sistema gerenciador de segurança da informação, requisitos estes a serem cumpridos através das demais normas da série, como a ABNT NBR ISO/IEC 27002 (Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação) (ISO, 2013b, p.2). Esta série ISO 27000 define o objetivo da política de segurança da informação da seguinte forma: "*Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes*". Para alcançar este objetivo, a norma orienta (ISO, 2013a, p. 6) que os controles sejam realizados com observância ao modelo *Plan-Do-Check-Act* ou PDCA (Figura 22):

- *Plan*: estabelecer a política e seus objetivos, processos e procedimentos.
- *Do*: executar o que foi planejado.
- *Check*: checar, avaliar criticamente a execução.
- *Act*: executar ações corretivas e preventivas com base na análise realizada.

Nesta norma não há a explícita descrição da CIA-triad, mas observando o documento como um todo, é evidente que os requisitos são dispostos de forma a atender os três pilares da segurança da informação.

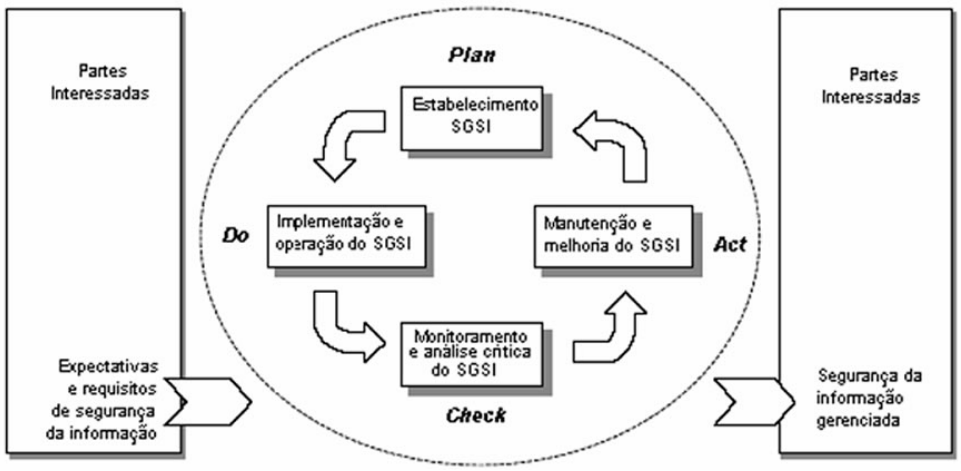


Figura 22: Modelo PDCA (ISO, 2006)

Contudo, conforme Dantas (2011, p. 14) a ABNT NBR/ISO IEC 27002 ressalta outras quatro propriedades: a autenticidade, a responsabilidade, o não repúdio e a confiabilidade. Tais atributos são possíveis atualmente através do uso de certificação digital. Uma mensagem assinada eletronicamente através de certificado digital, possui consigo a garantia de autenticidade, a identificação do responsável pelo envio, a garantia de que quem envio não pode negar que o tenha feito e por final é confiável.

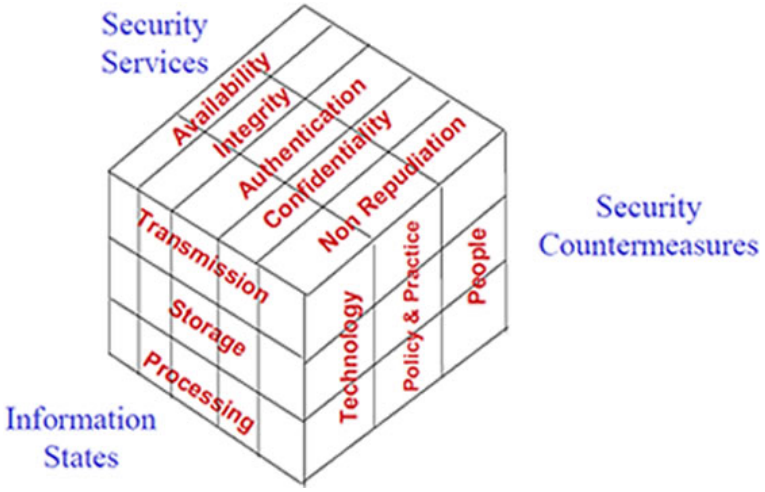


Figura 23: Modelo Maconachy (MACONACHY et al., 2001).

Continuando a sequência cronológica, Maconachy et al. (2001) faz uma discussão acerca da evolução da "garantia da informação" e como resultado apresenta um modelo (Figura 23) embasado no *McCumber's Cube* ao qual faz duas mudanças. Na primeira, substitui-se o termo "educação, treinamento e consciência" por "pessoas" assumindo a necessidade de um estudo contínuo (educação, treinamento e a compreensão das ameaças). Na segunda e mais significativa mudança, os autores incluem dois novos aspectos à dimensão de características da informação segura (agora denominada "serviços de segurança"): a "autenticação"(objetivo de estabelecer a validade da transmissão, mensagem

ou origem da mesma, ou ainda um meio de verificar autorização individual para receber categorias de informação específicas) e o "não repúdio"(garantia de que os dados do remetente serão fornecidos ao destinatário como prova de que o remetente é quem diz sê-lo).

Figura 24: Modelo Parkerian Hexad (PARKER, 1998).

Em 2002, Donn B. Parker[10] propôs uma expansão à CIA-triad adicionando à esta três novos elementos: a autenticidade, a utilidade e a propriedade (BOSWORTH; KABAY, 2002, cap. 5). Este modelo é resultado de pesquisas e publicações do autor a partir de seu livro Parker (1998). A adição destes novos elementos ocorreu em vista da complexidade de tecnologias emergentes, mas sem despresar os pilares clássicos. De acordo com a proposta de Parker, seu modelo então denominado Parkerian Hexad (Figura 24) possui os seguintes atributos de segurança da informação:

a. **confidencialidade** refere-se à propriedade da informação não ser disponibilizada a pessoas não autorizadas.

b. **integridade** refere-se à propriedade da informação não ser alterada sem autorização.

c. **disponibilidade** refere-se à propriedade do recurso (informação) estar disponível quando necessário.

[10] Pioneiro em computação, escritor, professor e pesquisador, é um promotor de medidas de segurança contra cyber crimes e renomado especialista em abusos e intrusões informáticos. `http://history.computer.org/pioneers/parker-db.html`

d. **autenticidade** este atributo funciona como uma prova de identidade. Refere-se à garantia da origem da mensagem (dado ou informação). A ideia é fornecer junto com a própria mensagem uma garantia de que quem a originou é quem diz sê-lo. Este inclusive é um atributo garantido pelo uso de Certificados Digitais para realização de assinatura eletrônica.

e. **utilidade** refere-se ao nível de utilidade que a informação possui. Se ela não é útil para determinado usuário, não precisa ser disponibilizada. Este atributo é também conhecido como o "princípio do menor privilégio" (SALTZER; SCHROEDER, 1975).

f. **possessão**: refere-se à propriedade de se ter algo possuído ou controlado, ao estado de ter/tomar o real controle físico.

Em 2009, a ISACA[11] propõe o *Business Model for Information Systems* (BMIS) (Figura 25) o qual tem como pontos chave os elementos "organização", "pessoas", "tecnologias" e "processo" ao centro. Todos estes interligados através de cultura, governança, arquitetura, emergência, suporte & habilitação e fatores humanos (ISACA, 2009). Não é um modelo especificamente relacionado à segurança da informação, mas como modelo de negócio, possui a essência da CIA-triad. O elemento "processos" deve ser cerceado pelos requisitos de integridade, disponibilidade e confidencialidade quando associado aos demais elementos (ISACA, 2009, p.15).

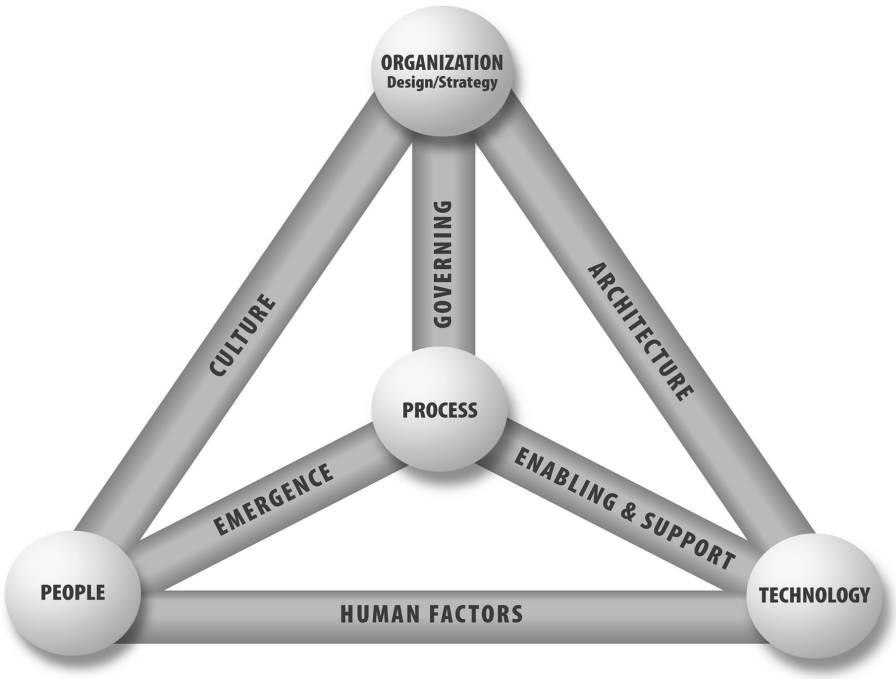
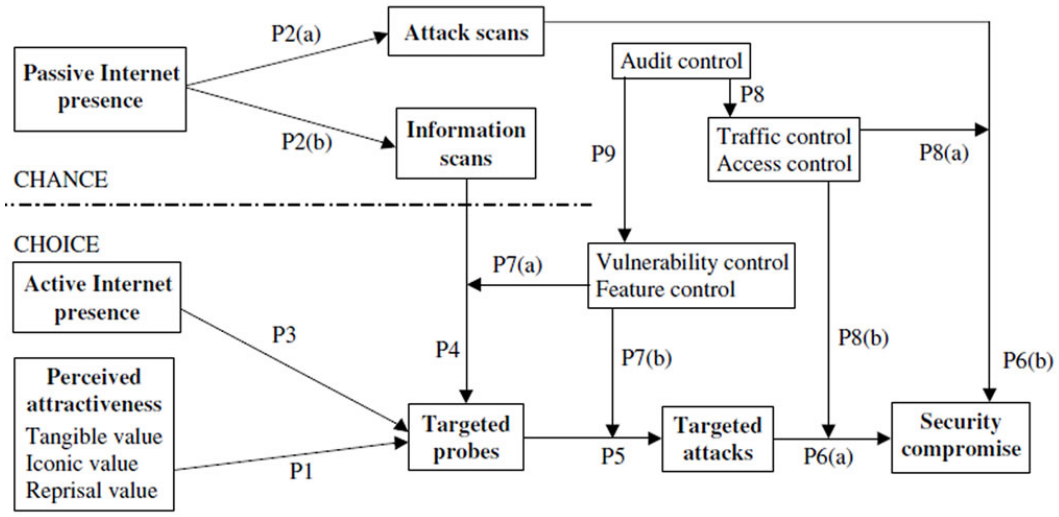


Figura 25: ISACA BMIS (ISACA, 2009)

[11] Associação independente e sem fins lucrativos que pesquisa o desenvolvimento de práticas em sistemas de informação. `www.isaca.org`

Em março de 2009 Ransbotham e Mitra (2009) apresenta o *Information Security Compromise Process* (ISCP) (Figura 26). Este modelo baseia-se no tipo de ataque considerando duas possibilidades para tal: ataque passivo e ataque ativo. O ataque passivo é ocasionado pelo escaneamento não direcionado de informações para uso futuro ou em tempo real. Em um ataque ativo, considera-se um alvo direcionado para realização do ataque. No contexto geral deste modelo, a CIA-triad pode partir de um controle de auditoria que por si atesta o controle de tráfego ou acesso a dados, bem como um controle de vulnerabilidades que está diretamente ligado ao escaneamento não direcionado de informações ou mesmo um ataque com alvo identificado. Uma vez que tais ataques consigam vencer estes dois controles, a tentativa de comprometer o sistema será bem sucedida.



Information scans	Nontargeted attempts to gather information about systems that can be used later for security compromise
Attack scans	Nontargeted attempts to compromise systems
Targeted probes	Targeted attempts to gather information about a specific system that can be used later for security compromise
Targeted attacks	Targeted attempts to compromise systems
Security compromise	Successful attempt to compromise the information security of a firm

Figura 26: Modelo ISCP (RANSBOTHAM; MITRA, 2009)

Quatro anos após, Cherdantseva e Hilton (2013) faz referência aos modelos anteriormente descritos em McCumber (1991), Maconachy et al. (2001), Ransbotham e Mitra (2009) e propõe o *Reference Model of Information Assurance & Security* (RMIAS) (Figura 27, pág. 71). Este modelo é dividido em quatro dimensões:

a. **Ciclo de vida da segurança do sistema de informação**: refere-se ao ambiente de desenvolvimento do sistema, ilustrando a progressão da segurança do sistema de informação do decorrer de seu desenvolvimento.

b. **informações de taxonomia**: descreve a natureza da informação a ser protegida.

c. **contramedidas de segurança**: categorizar contramedidas disponíveis para proteção da informação;

d. **metas de segurança**: são os objetivos de segurança que o modelo propõe. Nesta dimensão, além da CIA-triad, mantém-se o requisito de autenticidade proposto por Parker (1998), agora nomeado como "autenticidade e confiabilidade"e adiciona mais três requisitos:

   - **privacidade**: um sistema deve obedecer à legislação (em termos de privacidade) e deve permitir aos indivíduos controlar, sempre que possível, as suas informações pessoais.
   - **não repúdio**: capacidade do sistema para provar legalmente uma ocorrência/não ocorrência de um evento ou participação/não participação do mesmo.
   - **auditabilidade**: capacidade de conduzir monitoramento persistente de todas ações realizadas por seres humanos e máquinas no ambiente.

É importante ressaltar que dentre os modelos de segurança levantados, o RMIAS foi o único a definir de forma clara a participação conjunta da confidencialidade e a privacidade como parte dos objetivos do modelo, caracterizando-os separadamente. O objetivo da confiabilidade refere-se à necessidade de autorização para que determinada informação ou dado seja disponibilizado e a privacidade refere-se à possibilidade de controle das informações ou dados por parte do próprio usuário.

Observa-se visualmente pela Figura 18 (pág. 57) que a CIA-triad levou praticamente vinte anos para ser cunhada (considerando o período entre o início do estudo em 1967 e o Pink Book) e os modelos a partir de então parecem tender a uma complexidade cada vez maior ao longo dos anos, mas em todos eles mantém-se a CIA-triad. A Figura 28 faz uma representação visual sintetizando a correlação entre os modelos destacando a evolução de objetivos de segurança propostos.

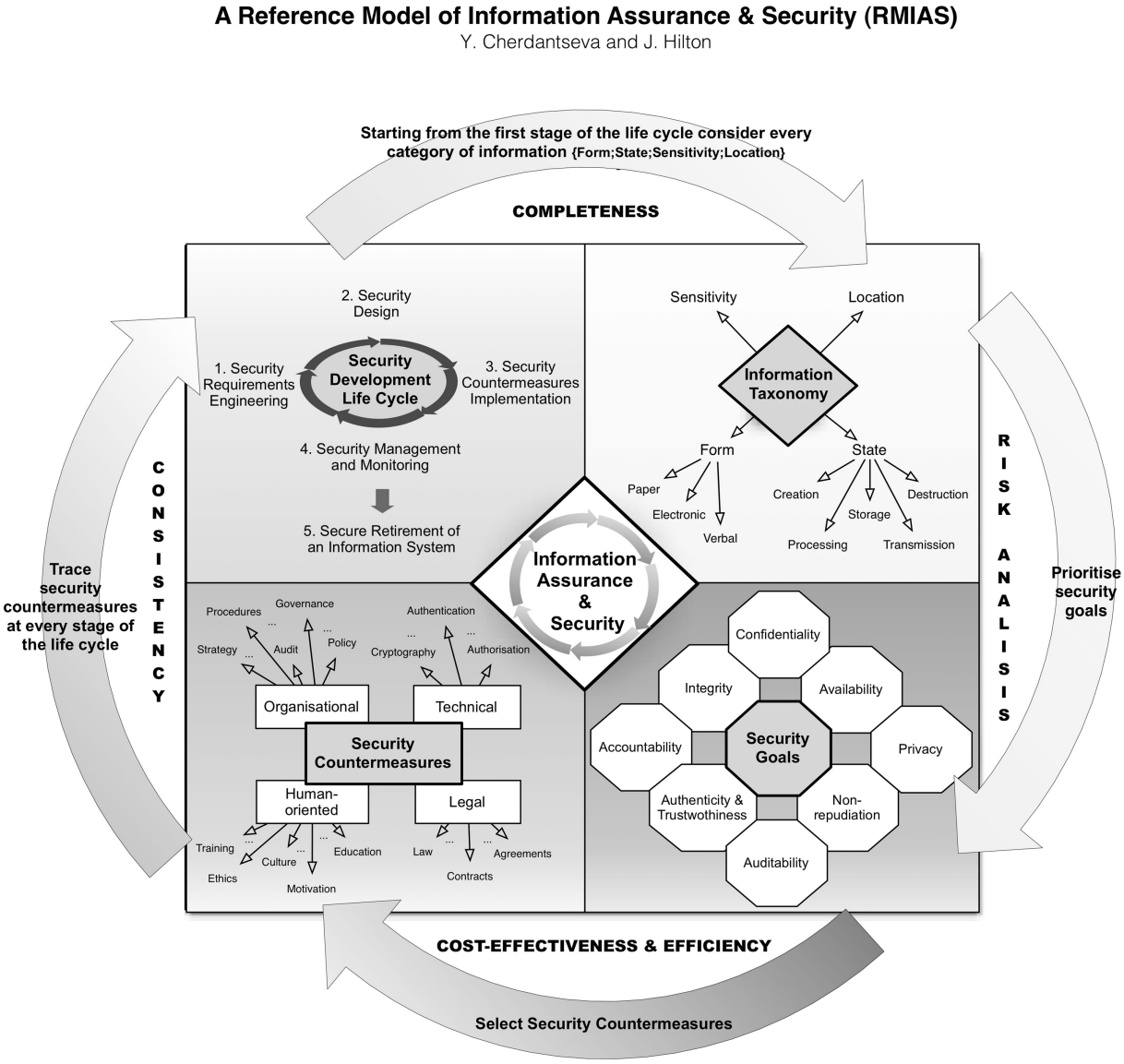


Figura 27: Modelo RMIAS (CHERDANTSEVA; HILTON, 2013)

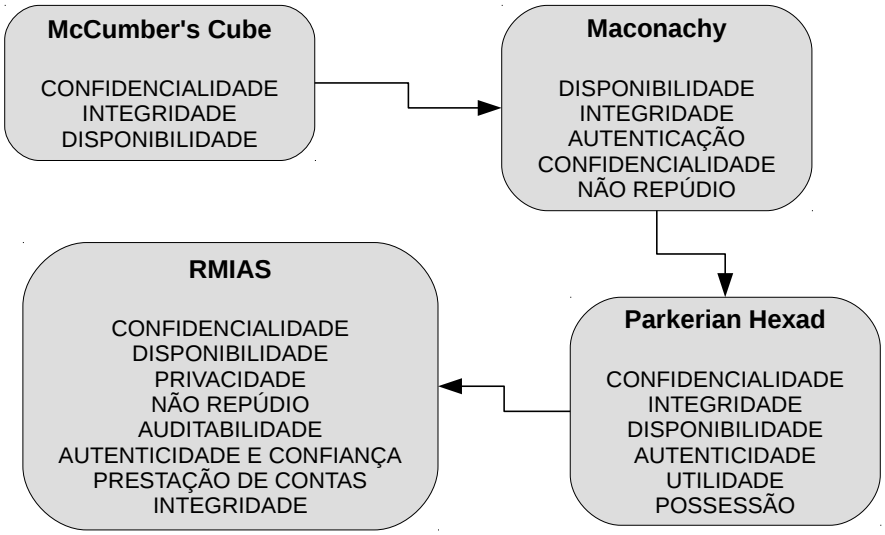


Figura 28: Correlação evolutiva dos modelos de melhoria à CIA-triad.

3 PRIVACIDADE NA INTERNET

A relevância na discussão da privacidade é cada vez maior considerando a expansão das novas tecnologias de comunicação e a preocupação com a vida privada diante da Internet. Esta relevância é ainda mais notória em vista da possibilidade de exposição de dados em tempo integral proporcionado pela IoT. São situações exploradas no cinema e séries de TV através de documentários com casos reais: *Dark Net* (KOCHAVI; JORDAN, 2016); e obras de ficção com proposições lógicas que mostram o extremo da exposição da vida privada: *The Circle* (BREGMAN et al., 2017).

Conforme Corcoran (2016) a exposição pode ser relacionada à pessoa física (dados fisiológicos e comportamento), ações, comunicações pessoais, imagens, localização e espaço, associação de grupo e experiência pessoal. Tal exibição coloca em crise a vida particular, a intimidade e exige uma interpretação mais apurada diante das novas tecnologias e formas de uso (PAESANI, 2008). Em Kochavi e Jordan (2016) a frase "*Cada informação sobre você vale algo para alguém.*" descreve o cerne do problema relativo à privacidade. Por mais insignificante que seja determinado dado, este pode ser aplicado por alguém para fins ocultos ao seu proprietário. Deste modo, deve haver um mecanismo que assegure a confidencialidade de dados privados.

Tais mecanismos de proteção à privacidade bem como o uso dos dados de usuário devem ser descritos na política de privacidade a qual deve explicar de forma explícita o que é coletado e como estes dados são utilizados. Para se ter um real exemplo deste fator, foram analisadas criticamente as políticas de privacidade de dois serviços utilizados no Brasil, escolhidos aleatoriamente: política do Google (GOOGLE, 2017b) (na versão de 18 de dezembro de 2017) e do Facebook (FACEBOOK, 2017) (na versão de 29 de setembro de 2016). Como resultado, destacam-se os seguintes pontos descritos nos documentos:

- **Política do Facebook**:
  - coleta os tipos de conteúdos visualizados.
  - coleta contatos que se tem maior envolvimento.
  - coleta grupos que mais gosta de compartilhar.
  - duração de atividades do usuário.

  A coleta destes tipos de dados é justificada na política como necessária para melhorar cada vez mais os serviços, oferecendo conteúdos mais personalizados. Entretanto esta prática acaba por coletar dados referente à privacidade do usuário no que diz respeito às suas preferências pessoais. O documento não cita o direito e opções da não coleta de dados caso o usuário queira utilizar o sistema desta forma.

- **Política do Google**:
  - armazena pessoas que são mais importantes para o usuário.
  - armazena consultas de pesquisa.
  - armazena o conteúdo do usuário, incluindo e-mails.
  - controle de atividades: o usuário pode "decidir"quais informações deseja que sejam salvas na conta.

  Esta política tem algumas particularidades também interessantes e uma característica que merece destaque é a total transparência. Observa-se que na política é explícito que dentre os dados armazenados e analisados, está o conteúdo de e-mails. Também é explícito que o usuário pode "decidir" quais informações deseja que sejam salvas na conta. Ao mesmo tempo que há este nível de transparência, o usuário não possui o real poder para esta decisão. A Figura 29 (pág. 74) é composta de recortes de tela do controle de atividades que definido em Google (2017a). Observa-se que atividades na *web* e aplicativos, atividades de voz e áudio, informações do dispositivo e histórico de localização, todos podem ser coletados mesmo que o usuário assinale o não desejo para tal. Esta ação está em destaque em cada recorte.

As duas políticas analisadas fornecem pontos interessantes a serem observados em uma abordagem de proteção à privacidade. O processo deve ser o mais transparente possível e dar opções reais ao usuário para compartilhar ou não seus dados. No caso da IoT, haverá situações em que a decisão de não compartilhamento poderá inutilizar sua finalidade, deste modo deve ser descrito de forma clara.

3.1 Análise etimológica dos termos "privacidade" e "confidencialidade"

Os termos privacidade e confidencialidade se esbarram de alguma forma em suas definições de modo que estas se unem e ao mesmo tempo sejam separadas. O tratamento de ambos como sinônimos ocorre pelo fato de que a significação institucional/empresarial atravessou a significação etimológica. Contudo, busca-se a diferenciação e recuperação do sentido latino das palavras, desgeneralizando-as e definindo a aplicação prática de cada uma.

Privacidade na Internet difere-se de confidencialidade na Internet. A privacidade não é uma técnica de proteção, mas é algo a ser protegido. É uma classificação de dado ou informação. Mesmo que se queira manter a privacidade de determinados dados, estes podem ser expostos independente da vontade (CERT.BR, 2012, p. 85). Uma navegação privada não é necessariamente uma navegação confidencial, mas uma navegação na qual

Figura 29: Descrição das opções de pausa no armazenamento de conteúdos na conta do usuário Google.

dados de identificação pessoal não devem ser fornecidos para outros *sites* ou armazenados no dispositivo. É possível tornar a privacidade da navegação também confidencial ao aplicar recursos de segurança à privacidade, algo comum nos navegadores de Internet.

Conforme Houaiss, Villar e Franco (2009, p. 1553) **privacidade** é um substantivo que refere-se à vida privada, particular, íntima e de acordo com Vieira e Micales (2016, p. 332) o termo é originado do latim ***privus*** que significa particular. Deste modo, o dado privado é considerado particular, próprio, que não diz respeito a terceiros. Ressalta-se em tempo que pela etimologia e significados levantados não há referência a mecanismos para limitação de acesso.

Confidencialidade é a qualidade de ser confidencial. Conforme Houaiss, Villar e Franco (2009, p. 519) o termo é um adjetivo que caracteriza algo não divulgável, que deve manter-se escondido. Conforme Vieira e Micales (2016, p. 88) trata-se de um substantivo originado do latim ***confidentia*** que significa segurança e ***confinium*** que significa limite, fronteira, confinamento. Deste modo, a definição de confidencialidade envolve o sigilo bem como a proteção do que se esconde. Um dado confidencial é aquele que é cerceado, fronteirizado, limitado de modo a manter-se seguro, escondido e não divulgável. Para se ter acesso ao dado é necessário um mecanismo que permita atravessar a fronteira imposta.

As duas noções se tocam no que tange ao isolamento do dado, mas se distanciam no que tange à maneira de fazê-lo. Seja um dado privado ou um dado confidencial, ambos são isolados; mas a maneira de prover este isolamento é que os diferencia. **Privacidade é uma classificação ao passo que a confidencialidade sugere a existência de mecanismo de proteção**.

A Figura 30 (pág. 76) exemplifica visualmente a diferenciação entre um dado privado e um dado confidencial através da aplicação prática de tais termos. Na ilustração desta Figura a foto é o dado em questão. Mesmo sendo classificado como privado, não significa que ele seja algo confidencial, protegido contra acesso de terceiros.

Esta abordagem sugere que no contexto de IoT a privacidade deva ser assumida como um princípio básico, ou seja, qualquer dado seja considerado privado. Definindo tal premissa, a aplicação de um modelo de segurança poderá determinar a fronteirização do dado privado e com isto instituir uma forma controlada de divulgação, permitindo definir quem pode ter acesso.

A diferenciação entre privacidade e confidencialidade é necessária em vista da diversidade e quantidade de dados passíveis de captação da IoT. É difícil estabelecer de forma incontestável que tipo de dados podem ser considerados privados. O nome de uma pessoa pode ser considerado privado? A localização geográfica de uma pessoa pode ser considerada privada? O nome de um medicamento utilizado por um indivíduo pode ser considerado privado? A rota de um veículo pode ser considerada privada? Todas as questões podem ser respondidas como positivo ou negativo, mas depende do contexto, do ponto de vista. Sobretudo, considerados privados ou não, tais dados serão administrados por equipamentos computacionais com instruções pré-programadas para processamento/armazenamento, criando oportunidades de exploração por terceiros.

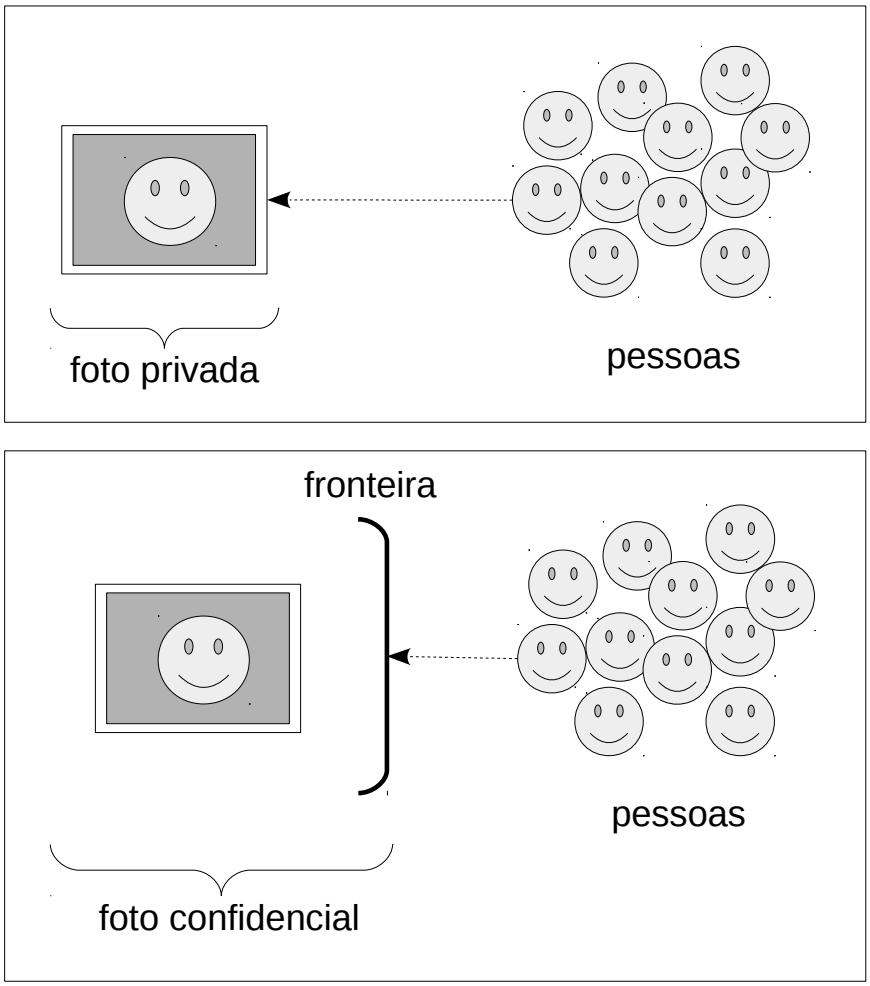


Figura 30: Exemplo de aplicação prática dos termos “privado” e “confidencial”.

Em Lee e Kobsa (2016) é feito um estudo para buscar entender a noção das pessoas em relação à privacidade em IoT. Para a pesquisa foram recrutados 200 participantes educados sobre a IoT, questionando a estes acerca de 14 cenários combinados aleatoriamente com base nos parâmetros “onde” (local particular, espaço público, etc.), “o que” (telefone, localização, voz, foto, vídeo, sexo, olhar, etc.), “quem” (desconhecido, amigo, governo, outro dispositivo, etc.), “razão” (segurança, comercial, social, saúde, etc.) e “persistência” (uma vez ou continuamente). Considerando que foram criados cenários únicos para cada participante ao combinar estas variáveis, no total foram criados 2.800 cenários. A Tabela 5 (pág. 77) apresenta a quantidade de respostas em termos de aceitação da IoT na “administração” de dados privados. Observa-se que 352 pessoas (equivalente a pouco mais de 12%) consideraram aceitáveis os cenários propostos, ou seja, mesmo educados em relação ao tema, trata-se de uma minoria de pessoas ao passo que os demais consideraram de alguma forma como inaceitável a IoT para a administração de dados privados.

Diante desta análise etimológica em face da IoT como tecnologia emergente, a conscientização da proteção da privacidade deve ser tomada como algo intrínseco. O real

Tabela 5: Nível de aceitação de dados privados na IoT

Rótulo	**Quantidade de opiniões**
Aceitável	352/2800
Algo inaceitável	466/2800
Inaceitável	840/2800
Muito inaceitável	1142/2800

valor de dados próprios das pessoas, bem como o questionamento da real necessidade de compartilhamento dos mesmos deve estar em evidência.

3.2 Privacidade e Internet na legislação brasileira

A privacidade é um fator de preocupação histórica (COSTA, 2018), (RAMOS, 2008). Nos primórdios das culturas hebraica, grega e da China, a preocupação com a privacidade era algo consistente, focado na maioria das vezes no "direito a estar só". No Brasil a referência expressa à intimidade e à vida privada foram sancionados através da Constituição de 1988, mais especificamente o inciso X do Art.5 (BRASIL, 1988) que diz: *"são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação"*. O direito de proteção é amparado também pelo Art. 21 da Lei 10.406/2002 (BRASIL, 2002) que transcreve de forma clara a inviolabilidade da vida privada. Em termos de privacidade na Internet são pertinentes as seguintes Leis:

- **Lei de Acesso à Informação (Lei 12.527/2011)**: dispõe sobre a regulamentação do acesso à informação[1], sendo um documento direcionado especificamente ao contexto da administração pública: órgãos públicos da União[2], estados[3] e municípios. O documento descreve sobre o acesso e divulgação de informações, procedimentos de acesso, restrições, proteção e controle de informações sigilosas, entre outros. Ressalta-se que o documento menciona a necessidade de cumprimento da Lei respeitando a vida privada, entretanto o documento não define explicitamente os termos privacidade ou confidencialidade. (BRASIL, 2011)

- **Lei de Crimes Cibernéticos (Lei 12.737/2012)**: dispõe sobre a tipificação criminal de delitos informáticos. Ressalta-se que não faz nenhuma definição dos termos privacidade e confidencialidade, mas apenas descreve o que passa a ser considerado por Lei um crime cibernético. (BRASIL, 2012)

- **Marco Civil da Internet (Lei 12.965/2014)**: é o documento que estabelece os princípios, direitos e deveres para o uso da Internet no Brasil. Este documento

[1] Publicação da classificação de documentos secretos: Nacional (2012, p. 2) por força desta Lei.
[2] Portal de transparência do Governo Federal: Brasil (2017)
[3] Portal de transparência do estado de MG em MG (2017) e do estado de SP em SP (2017)

contém termos importantes em relação à privacidade da Internet (BRASIL, 2014). Em vista disto, convém uma análise em maiores detalhes a ser realizada em seguida.

- **Código Penal (Decreto-Lei 2.848/1940)**: dispõe sobre penalidades em vista da violão de privacidade. Destaca-se os Art. 153 e 154 que tipificam como crime a divulgação de segredos que causem dano a outrem, bem como a violão de segredo profissional, o que inclui a invasão de dispositivo informático.

São pertinentes ainda os seguintes Projetos de Lei que tramitam na Câmara dos Deputados:

- **Projeto de Lei 5276/2016** que dispõe sobre o tratamento de dados pessoais trazendo uma contribuição interessante ao propor a definição: "*dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa*" (EXECUTIVO, 2016b, Art. 5º, Inciso I). A legislação brasileira carece de definições melhor adequadas como esta. Entretanto o projeto encontra-se parado desde 2016 conforme Executivo (2016a).
- **Projeto de Lei 6291/2016** o qual propõe a alteração do Marco Civil no sentido de proibir o compartilhamento de dados pessoais dos assinantes de aplicações de Internet. Este é um ponto importante a ser observado pois não se refere ao conteúdo da comunicação e sim ao autor da comunicação, ou seja, dados pessoais, particulares dos usuários de Internet. Entretanto o projeto encontra-se parado desde 2016 conforme Derly (2016).

3.3 Marco Civil da Internet

A Lei 12.965 de 23 de abril de 2014 conhecida como o Marco Civil da Internet (BRASIL, 2014) é a primeira Lei nacional (regulamentada através do Decreto 8.771/2016 (BRASIL, 2016)) com aplicabilidade específica ao uso de Internet no Brasil, dispondo princípios, garantias, direitos e deveres em relação ao uso da rede no Brasil. Portanto, em termos de Internet, esta é a Lei máxima no Brasil, sendo a legislação de referência para assuntos relacionados ao tema.

No primeiro capítulo a Lei define os princípios do uso da Internet no Brasil, dentre os quais destacam-se a proteção à privacidade e proteção dos dados pessoais. Isto quer dizer que toda a esfera pessoal, a vida familiar, o convívio com pessoas próximas, tudo isto tem o direito de não ser exposto publicamente através da Internet. Entretanto, a conscientização da maioria das pessoas quanto à privacidade é o principal inimigo da Lei e das próprias pessoas.

Uma vez que o indivíduo por vontade própria faz a divulgação de registros fotográficos, localização física ou círculo de amigos, ele próprio está expondo a sua privacidade o que muitas vezes pode ser o fator inicial que desencadeará um problema futuro que envolva questões de privacidade. A divulgação de dados próprios é algo que deve ser realizado com muita cautela, principalmente quando não há consciência do poder que um dado pode propiciar em mãos erradas.

Na sequência, o Art. 7 dispõe sobre as garantias que por direito são asseguradas ao usuário de Internet, uma vez que trata-se de um exercício essencial de cidadania. São citados como direito assegurado (BRASIL, 2014, Art. 7, Incisos II e III):

- "*II - A inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;*", e
- "*III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;*".

Entende-se por fluxo de comunicação o conteúdo de uma comunicação que flui entre origem e destino, tal como o acesso a um *website*, acesso a uma máquina remota, ou qualquer outro tipo serviço remoto acessível pela Internet. Com isto, é assegurado o direito de se realizar uma comunicação pela Internet sem que seu fluxo seja violado ou tenha o sigilo comprometido.

Entretanto, observa-se que havendo ordem judicial a violação é permitida na forma da Lei. Não se objetiva aqui discutir pontos da ciência do direito, entretanto é observado que a privacidade na sua plenitude não pode ser garantida por Lei. Esta afirmação é embasada no inciso III o qual faz menção às "*comunicações privadas armazenadas*", ou seja, indiretamente é permitido que se armazene comunicações privadas e em uma possível ordem judicial, esta seja revelada.

No Art. 14, lê-se que: "*Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet*" Brasil (2014, Art. 14). Através deste artigo fica explícito que não é permitido guardar os registros de acesso a aplicações, e que são "*o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internete a partir de um determinado endereço IP*" (BRASIL, 2014, Art. 6, Inciso VIII).

Com isto, o Marco Civil não permite a violação do sigilo da comunicação e veda o armazenamento de informações de acesso (data, hora e IP), mas por outro lado permite armazenar a comunicação, mesmo privada, uma vez que não se fala o contrário no documento. Este é um ponto crucial o qual merece discussão mais aprofundada em trabalhos futuros.

Diante do exposto, a IoT como integrante da Internet provavelmente também pode ter o seu conteúdo de fluxo armazenado, o que não é algo interessante e reforça a necessidade de proteção a qualquer conteúdo de comunicação em IoT. Em relação ao registro de data, hora e IP de acessos, estes podem ser utilizados para determinar padrões de comportamento de pessoas e ambientes, mas esta situação é até de certo modo aceitável considerando o fato de que a revelação seja feita apenas mediante ordem judicial.

Por fim, ressalta-se que o Marco Civil não é um documento a ser menosprezado, mas precisa ser melhor revisto em termos técnicos uma vez que permite brechas passíveis de exploração.

3.4 Confidencialidade e anonimato como recursos de proteção da privacidade na Internet

As redes sociais em conjunto com os *smartphones* são recursos que atualmente oferecem muita praticidade para que o usuário torne toda a sua vida disponível e acessível facilitando o monitoramento por terceiros. Esta prática é facilitada e sugestionada uma vez que por padrão as pessoas estão em tempo integral com seus dispositivos móveis de comunicação. Ao adotar tal prática o próprio indivíduo se auto expõe de uma maneira em que não é preciso recursos avançados para a aquisição de dados e informações por parte de terceiros, dados estes que podem ocasionar riscos à segurança do próprio indivíduo. Algumas pessoas praticamente fazem da rede social um diário em tempo real com informações de localização, alimentação, costumes e preferências, seja através de texto, fotos ou vídeos. Conforme Assumpção, Santana e Santos (2015, p. 33) mesmo fotos e vídeos podem ter dados extraídos e correlacionados ao usuário, permitindo assim descobrir informações pessoais mesmo que o usuário não as tenha escrito, baseando-se no comportamento e imagens por ele produzido ou visualizado.

Esta é uma questão de cultura do usuário que precisa ser "corrigida" pois é um comportamento que anula todo e qualquer recurso que busque resguardar a privacidade, dentre estes o anonimato. Anonimato é uma expressão que pode ser utilizada de forma confusa em face à confidencialidade e privacidade, deste modo convém evidenciar sua etimologia. A diferenciação entre anonimato e privacidade na Internet se dá em relação à forma de tratamento dos dados e informações que possam de algum modo revelar a identificação ou localização física do usuário.

Anonimato é um atributo do que é anônimo. Conforme Houaiss, Villar e Franco (2009, p. 140) este termo origina-se do latim ***anonumos*** e significa aquilo que não tem o nome ou assinatura do criador, não tem autoria. O anonimato na Internet caracteriza-se pelo desconhecimento da origem da mensagem, mas permite conhecer o conteúdo e o destino. Deste modo, uma mensagem com a qualidade de anônima pode ser interpretada

e ter o seu destino identificado e apenas o emissor permanece obscuro.

Em contrapartida, a privacidade caracteriza-se pela classificação de dados e informações particulares que identifiquem o usuário ou sua localização física. Considerando a possibilidade de divulgação destes dados mesmo sem o consentimento do usuário, deve ser aplicado um mecanismo de anonimato e/ou confidencialidade para garantir o resguardo dos conteúdos.

Por fim, a confidencialidade na Internet caracteriza-se pela proteção do conteúdo da mensagem. Assim uma mensagem confidencial não é publicamente acessível, mas permite-se identificar a sua origem, isto é, quem é o emissor. Também é possível a aplicação de confidencialidade ao destino da mensagem de modo que este não seja identificável em caso de interceptação do fluxo de dados.

A Tabela 6 apresenta o resumo de diferenças entre privacidade, anonimato e confidencialidade no uso da Internet. Observa-se que a privacidade em si não protege dados, não se trata de uma técnica de proteção.

Tabela 6: Resumo de diferenças entre privacidade, anonimato e confidencialidade na Internet.

Alvo	**Privacidade**	**Anonimato**	**Confidencialidade**
origem da mensagem	conhecido	não conhecido	conhecido
destino da mensagem	conhecido	conhecido	conhecido/não conhecido
conteúdo da mensagem	conhecido	conhecido	não conhecido

A proteção à privacidade no âmbito da Internet pode ser conseguida através da confidencialidade e/ou do anonimato e estes são proporcionados através do uso de recursos como o protocolo https, redes virtuais privadas como Tor, I2P ou um túnel próprio, tecnologias estas descritas em seguida.

3.4.1 HTTPS

O *Transmission Control Protocol* (TCP) é um protocolo[4] para gerir a transmissão de dados entre computadores. É através dele que as mensagens que viajam entre as milhares de rotas da Internet conseguem chegar a seus respectivos destinos. Entretanto tais mensagens podem ser interceptadas e consequentemente ter o seu conteúdo e integridade comprometidos. Em vista disto, conforme Kurose e Ross (2013, p. 711) o TCP possui uma versão conhecida como *Secure Sockets Layer* (SSL) a qual é um protocolo que provê confidencialidade e integridade na comunicação entre dois pontos de rede. Com isto tem-se a garantia da confidencialidade e integridade do conteúdo da mensagem. A identificação do uso de SSL é possível em navegações *web* quando o endereço começa com a expressão "https" que significa *Hyper Text Transfer Protocol Secure*. Trata-se do protocolo http[5]

[4] procedimento em comum adotado entre dois agentes envolvidos.
[5] *Hyper Text Transfer Protocol* é o protocolo padrão para acesso à páginas *web*.

com uma camada de segurança. Este é um protocolo utilizado por *browsers* para ter a garantia de sigilo do conteúdo da mensagem entre origem e destino. O funcionamento é basicamente da seguinte forma: a mensagem é criptografada na máquina de origem, faz o percurso de viagem e por fim chegando ao destino ela é descriptografada. Deste modo durante o percurso de viagem a mensagem pode ser interceptada mas o seu conteúdo não será legível.

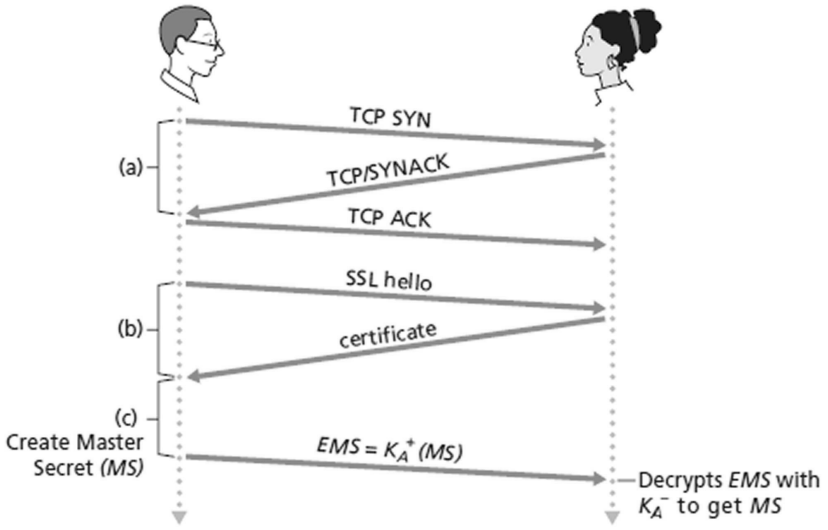


Figura 31: *Handshake* inicial para estabelecer uma conexão SSL (KUROSE; ROSS, 2013, p. 713)

O processo de criptografia é garantido mediante uma negociação prévia entre as máquinas envolvidas, sendo assim, é um recurso ineficiente quando a origem ou destino estiverem previamente comprometidos, isto é, de alguma forma observados. O *handshake* inicial entre os dois computadores para que se tenha a criptografia ocorre em três etapas como representado na Figura 31:

(a) **Bob precisa estabelecer uma conexão com Alice**: Bob envia uma requisição para verificar se Alice está *online*; Alice envia uma mensagem com resposta de confirmação da sua existência; Em seguida Bob envia uma resposta dizendo que recebeu a confirmação de Alice (esta mensagem é uma confirmação de que Bob está *online* também).

(b) **Bob verifica se Alice é realmente Alice**: Bob envia uma mensagem SSL Hello (uma apresentação dizendo que vai usar SSL) de agora em diante; Alice envia como resposta um certificado (uma identificação contendo a chave pública) através da qual Bob pode gerar mensagens de forma que só Alice possa descriptografar. Isto será necessário para a próxima mensagem a qual só poderá ser descriptografada por Alice.

(c) **Bob envia a *Master Secret* (MS) para Alice**: Bob gera uma chave MS (que será utilizada somente nesta sessão SSL), encripta-a utilizando-se da chave pública de Alice e envia a *Encrypted Master Secret* (EMS). Alice decripta a EMS utilizando-se de sua pória chave privada e a partir de então somente Bob e Alice conhecem a chave *Master Secret* para troca de mensagens deste fluxo de conexão.

O uso do https, isto é, o protocolo ssl em conexões padrões de Internet é praticamente unanime em ambientes de *login* e como acaba por tornar-se um padrão para *sites* em geral. Existem também recursos como o Https Everywhere[6] que força o uso de https em 100% das conexões realizadas, obrigando o uso do protocolo mesmo que o usuário não queira.

3.4.2 Túnel VPN

Virtual Private Network ou VPN é um circuito virtual (que não existe fisicamente) criado em cima da estrutura da Internet. Este circuito é como um túnel exclusivo de transferência de dados e toda a comunicação é encriptada de forma que agentes externos não consigam enxergar o conteúdo das mensagens que trafegam no mesmo (KUROSE; ROSS, 2013, p. 718). É um recurso de baixo custo pois pode aproveitar a estrutura física já existente da Internet tornando uma opção adotada em grande escala por organizações e governos. A VPN pode prover os requisitos da CIA-triad, isto é, a integridade, a disponibilidade e a confidencialidade, entretanto não garante o anonimato até pelo fato de que não é criada com este fim. Alguns serviços de VPN (pagos ou gratuitos) prometem a não divulgação dos dados de acesso de usuários, mas apenas o fato da existência do cadastro é um ponto negativo na questão do anonimato. Este banco de dados está sujeito à invasão, fornecimento de informações por força de Lei, entre outras possibilidades.

Para o funcionamento da VPN é necessário o estabelecimento prévio do circuito, isto é, a concepção do caminho entre a máquina local e o *host* de saída da VPN, isto é, o local a partir de onde a conexão será originada do ponto de vista da Internet. Este procedimento é relativamente simples e pode ser feito utilizando aplicativos específicos (fornecido por empresas especializadas) ou utilizando-se de recursos disponíveis no sistema operacional como por exemplo o *Secure Shell* (SSH) através do código proposto no Apêndice A.

Para exemplificar a dinâmica de funcionamento, foi realizado um experimento comparativo de acesso sem VPN e com VPN[7] ao destino `www.pucsp.br` (localizado no Brasil). Para a comprovação da rota até o destino pode ser utilizado qualquer ferramenta de *traceroute* (disponível para a maioria dos sistemas operacionais ou disponibilizados em

[6] Disponível em `https://www.eff.org/https-everywhere`

[7] utilizando o Windscribe, disponível em `https://windscribe.com/`

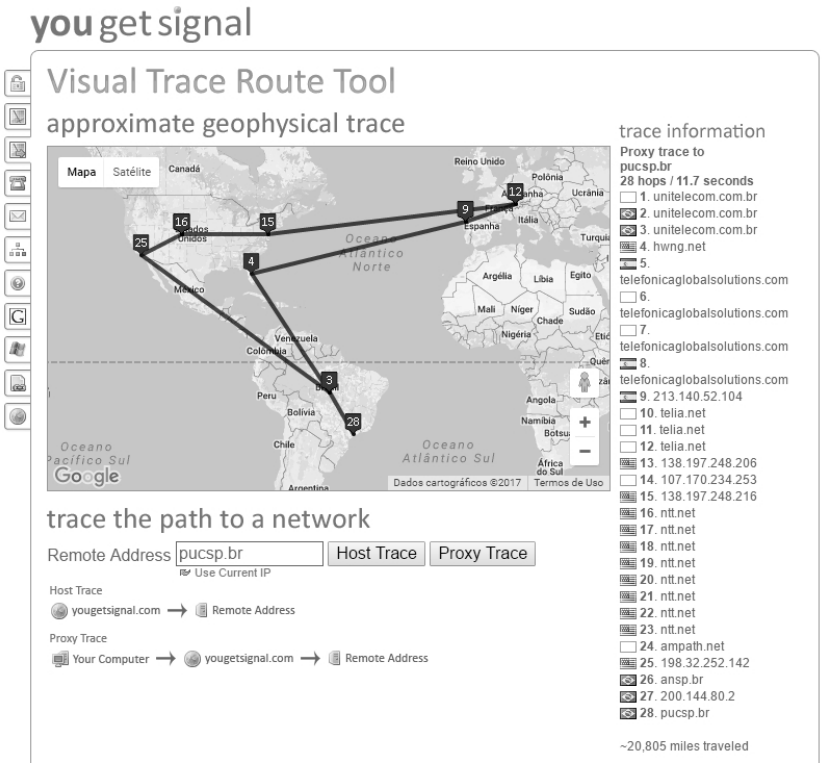


Figura 32: Traçado da rota sem a utilização de VPN.

sites). Dentre tais opções foi escolhida uma ferramenta com resultado visual através do mapa mundi[8] que permite um melhor entendimento do caminho desenhando-o de forma intuitiva.

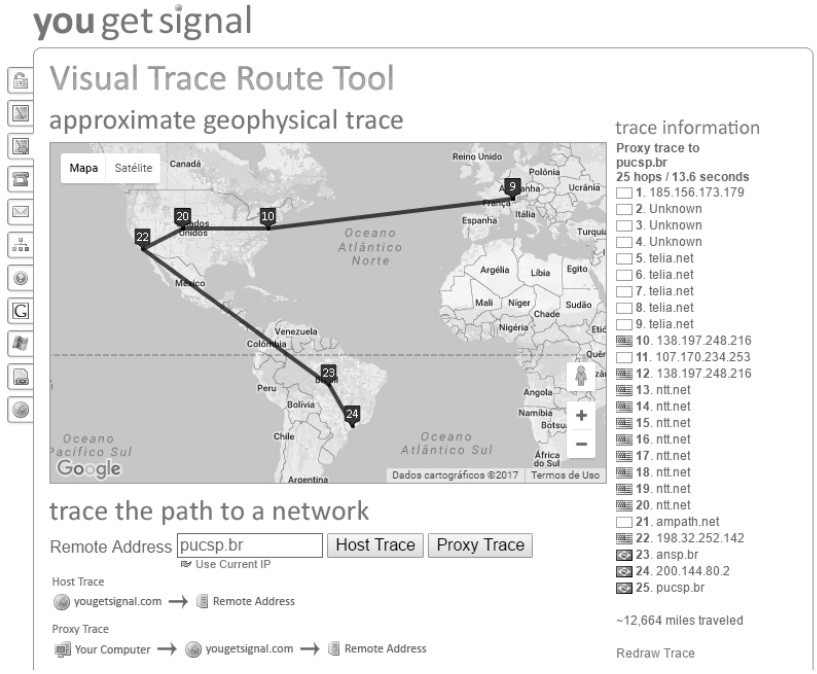


Figura 33: Traçado da rota com a utilização de VPN.

[8] Disponível em `https://www.yougetsignal.com/tools/visual-tracert/`

O primeiro acesso foi realizado sem o uso de VPN e conforme observa-se na Figura 32, do ponto de vista da Internet a conexão foi originada no Brasil, passando por diversos roteadores ao redor do mundo e chegando ao destino, também no Brasil.

O segundo acesso (Figura 33) foi realizado com o uso de VPN e do ponto de vista da Internet a conexão foi originada na França. O caminho entre a máquina local e a França, ou seja, o túnel, este não é percebido.

Utilizando a VPN desta forma, tudo o que for realizado a partir da máquina local, é como se ela fosse o *host* de saída da VPN, ocultando assim a verdadeira origem da conexão. Mas conforme comentado anteriormente, a empresa que provê o serviço de VPN conhece seus clientes, ou seja, quem utiliza VPN. Isto é um ponto crítico a considerar quando se quer anonimato total.

Outra forma de uso é quando se cria uma VPN por conta própria, isto é, sem a interferência de terceiros. Uma vez estabelecido o circuito, os computadores geograficamente distantes se comunicarão como se estivessem na mesma rede local. A Figura 34 é a representação visual de uma VPN estabelecida na qual faz-se a interligação de duas redes geograficamente distantes utilizando-se da estrutura da Internet. O túnel é a camada de encriptação a qual protege a conexão VPN de interceptação externa, ou seja, todo o tráfego passa por dentro deste de forma que somente as redes A e B se "enxerguem" como se fosse uma única rede local. O equipamento cliente é o responsável por requisitar o estabelecimento do circuito e o servidor é quem responde à requisição. No Apêndice A é sugerido um *script* para estabelecimento deste tipo de circuito de uma forma simples, na qual um aplicativo qualquer (banco de dados, intranet, aplicação proprietária, entre outros) pode fazer uso.

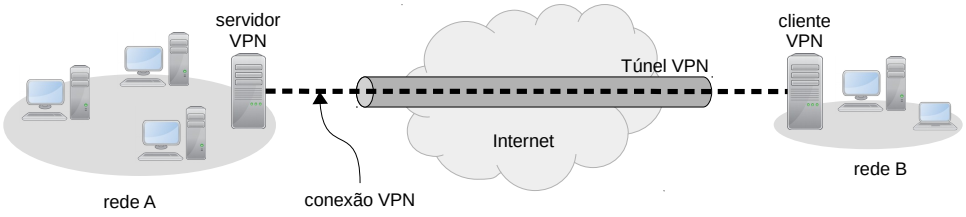


Figura 34: Tunel VPN estabelecido entre duas redes geograficamentes distintas.

Um último fator a considerar em relação ao uso de VPN é a latência. Em vista dos procedimentos de encriptação tem-se uma camada extra de processamento o que por definição torna a VPN mais lenta comparando-se a um acesso sem uso da mesma. Para comprovação desta afirmação foi realizado um experimento conforme disposto no Apêndice E. Através do experimento observou-se que a conexão sem VPN tem um *time to live* bem mais baixo comparando-se à conexão com VPN o que realmente comprova que este é um fator a ser levado em consideração.

A latência é um fator importante a ser levado em consideração pois para cada tipo de uso da IoT existe um nível de tolerância. A Tabela 7 (pág. 86) é uma adaptação de Hou et al. (2016) na qual foram destacadas apenas as colunas referente à latência e nível de segurança & privacidade em cenários com casos típicos de uso da IoT. As situações com baixa tolerância à latência são: *residential monitoring*, *driving assistance* e *vital signal alert*. Estes são casos em que a latência pode comprometer o objetivo fim do sistema pois trabalham com informações vitais. Estes casos típicos também requerem um alto nível de segurança e privacidade em vista da criticidade dos dados. Deste modo, mesmo que a tolerância à latência seja baixa, deve haver ao menos uma camada de segurança no ambiente, camada esta a ser minuciosamente implementada para uso de forma a causar o mínimo impacto possível de latência e com isto não comprometer o objetivo do sistema como um todo. Na mesma Tabela 7 observa-se outros casos de uso em que a tolerância à latência é maior. São situações em que o atraso (em termos de milissegundos) não compromete o funcionamento tais como *water metering*, *home automation*, *smart meeting*, *traffic monitoring* e *patient monitoring*.

Por fim, ainda há a questão do uso pois quanto maior é a segurança aplicada, menor é a usabilidade. Não há tanta complexidade ao fazer uso de um tunel VPN mas de qualquer forma é um procedimento extra a ser considerado. Esta é uma equação que deve ser muito bem configurada ao definir as prioridades e alcançar o equilíbrio desejado.

Tabela 7: Latência tolerável (adaptado de Hou et al. (2016)).

Scenario	***Typical use case***	***Tolerable latency***	***Security & privacy***
Smart building	*water metering*	*high*	*low*
Smart building	*residential monitoring*	*low*	*high*
Smart home	*home automation*	*high*	*high*
Smart home	*smart meeting*	*medium*	*high*
Intelligent transportation	*traffic monitoring*	*high*	*low*
Intelligent transportation	*driving assistance*	*low*	*high*
Smart healthcare	*patient monitoring*	*medium*	*high*
Smart healthcare	*vital signal alert*	*low*	*high*

3.4.3 Rede TOR

A rede Tor (acrônimo de *The Onion Routing*) também conhecida como *Deep Web* é uma rede sobreposta à Internet, ou seja, ela não possui estrutura própria e depende da primeira rede para funcionar. Esta nomenclatura se deve à sua forma de funcionamento que dispõe encriptação em camadas (como uma cebola). Conforme Jha et al. (2016, p. 2) é uma rede iniciada em 1994 quando era conhecida como *Hidden Web* e posteriormente em 2001 renomeada para *Deep Web*. A primeira denominação ocorreu em razão do sistema ser uma forma de ocultar páginas *web* dos meios tradicionais de busca. A nomenclatura

atual faz uma analogia ao ambiente oceânico de modo que o que está na *Deep Web* seria o equivalente a estar no oceano profundo ao passo que os conteúdos tradicionais e acessíveis por buscadores estão na área "superficial" do oceano.

Conforme Levitt (2015) é um dos recursos de maior nível em proteção à privacidade. A rede Tor é um tipo de VPN, entretanto o diferencial comparando-se à uma VPN tradicional é que a rede Tor é composta por um grupo de servidores operados por voluntários adeptos à causa da privacidade na Internet (TOR, 2017). Estes servidores disponibilizam listas de Tor *nodes* ativos, isto é, disponibilizam em tempo real os nós ativos para entrada na rede Tor. Obviamente tais servidores não são máquinas comprometidas (observadas), do contrário, invalidaria o objetivo do projeto como um todo. Entretanto, em vista da falta de confiança somada à própria proposta do projeto Tor, trata-se de um ambiente indicado para navegação anônima.

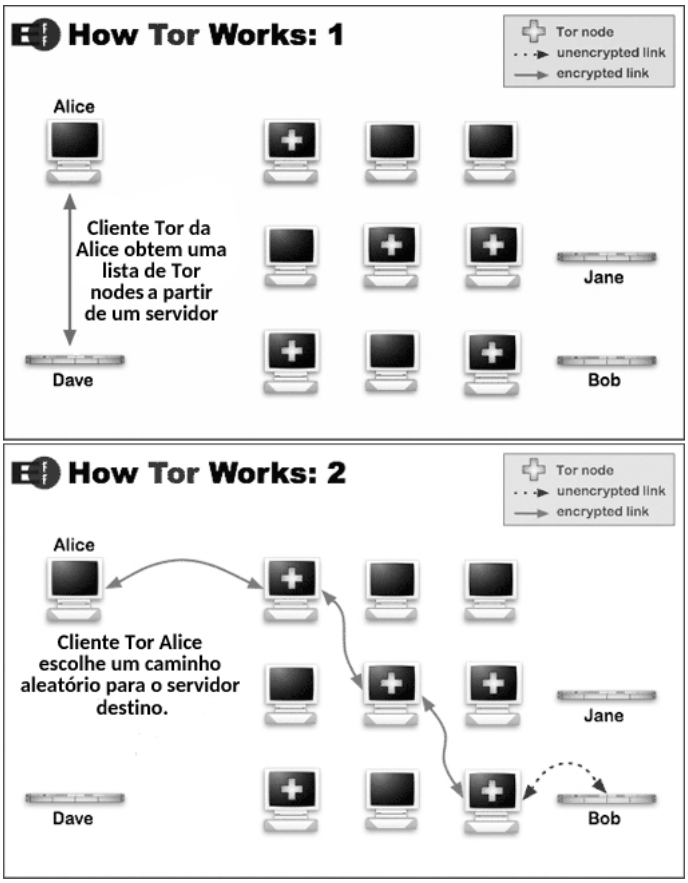


Figura 35: Como funciona a rede Tor (TOR, 2017, tradução livre)

Uma conexão na rede Tor é composta por vários túneis virtuais (entre pares de nós disponíveis) ao invés de uma conexão direta entre a origem e o destino. A primeira etapa para estabelecer a comunicação é utilizar um cliente Tor[9] com o qual obtem-se a lista de Tor *nodes* para entrada na rede Tor, também chamados de *Guard Relay*. Conforme a Figura 35, na primeira etapa (*How Tor Works*: 1) Alice (cliente) obtem a lista de Tor

[9] *Download* do cliente Tor: `https://www.torproject.org/download/download-easy.html.en`

nodes de Dave (servidor). Ressalta-se que esta primeira conexão para busca da lista é por https, logo é encriptada. De posse da lista, na segunda etapa da mesma Figura 35 (*How Tor Works*: 2) Alice escolhe um caminho aleatório para chegar ao destino. O último servidor do circuito Tor passa a ser a origem dos pacotes de dados sob o ponto de vista da Internet tradicional, ou seja, se houver algum tipo de monitoramento por pessoas ou máquinas, é como se a conexão de Alice estivesse partindo deste último *node* da rede Tor. Tal situação é demonstrada na Figura 36 quando foi estabelecida a conexão a partir do Brasil. Na ocasião foi acessado um *site* com recursos para rastreamento de IP[10]. Observa-se pela figura que o local originário da conexão é reconhecido como França, ou seja, é como se o usuário estivesse a uma considerável distância do seu local real de acesso. Na mesma tela, observa-se outros números de IPs, os quais são alguns dos *nodes* por onde o circuito Tor estava passando no momento. É importante ressaltar que a máquina que originou a conexão (no exemplo Alice) tem a informação do circuito como um todo.

Outra prova de conceito em relação a este último IP do circuito (ou qualquer outro *node*) pode ser obtida submetendo tais endereços IPs a alguma ferramenta de *nslookup* como IP-Lookup[11] ou IP Tracker[12]. Este tipo de ferramenta tem por finalidade recuperar informações técnicas sobre determinado IP, dentre elas a localização física do mesmo.

O circuito Tor por completo pode ser dividido em três tipos de *relay*[13], cada um com a sua própria camada de encriptação (WRIGHT, 2015):

- ***Guard Relay*** é a entrada para a rede Tor. Este possui a informação de que Alice (IP origem) usou a rede Tor mas não sabe para qual finalidade e localidade.
- ***Middle Relay*** é composto pelos *nodes* utilizados para a transmissão de dados entre o *Guard Relay* e o *Exit Relay*, garantindo que um não conheça o outro. Neste *relay* não se sabe o conteúdo, a origem e o destino da mensagem.
- ***Exit Relay*** é a saída da rede Tor, tratando-se do último *node* utilizado e o qual envia o tráfego para a Internet tradicional. Este possui apenas a informação do destino da mensagem.

Com isto, tem-se três encriptações de forma que nenhum *node* do circuito Tor tenha condições de conhecer a rota completa do fluxo de dados, com excessão de quem originou a conexão.

A Figura 37 (pág. 90) apresenta uma estatística gerada pelo Tor Project (TORMETRICS, 2017). Através desta, observa-se que ano de 2008 existiam um pouco mais

[10] Disponível em `http://en.dnstools.ch/show-my-ip.html`
[11] Disponível em `http://ip-lookup.net/`
[12] Disponível em `http://www.ip-tracker.org/`
[13] Link de retransmissão de dados

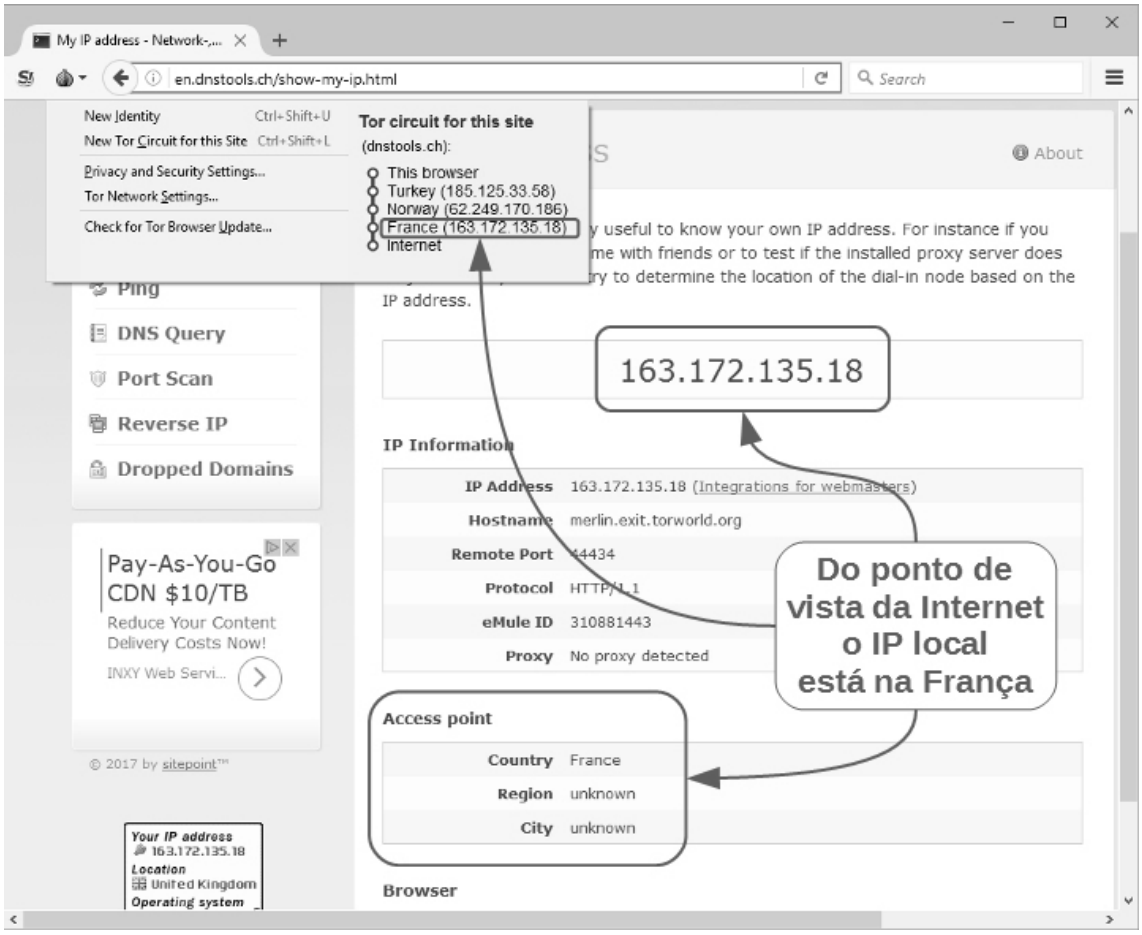


Figura 36: Uso do cliente Tor para acessar um site de rastreamento de IP

de 1.000 *relays* funcionando e quase dez anos depois, em 2017, existem aproximadamente 7.000 *relays* de roteamento em funcionamento na rede Tor distribuídos ao redor do mundo. É uma aumento exponencial não tão rápido quanto à Internet tradicional, mas demonstra o crescimento existente e real da rede Tor. Dentre estes *relays* em funcionamento aproximadamente 2.500 são de entrada (*guard*) e quase 1.000 de saída. É apresentado também uma média de *relays* estáveis, isto é, conectados a longo prazo bem como os de maior largura de banda (acima de 100Mbits/seg.), ambos os casos girando em torno de 6.000 *relays*. O projeto TorFlow apresenta uma proposta que permite visualizar o movimento de fluxo de dados entre estes *relays* através do uso de milhares de particulas para simulação de fluxo (UNCHARTED, 2016). É importante ressaltar que não se trata do fluxo real de dados da rede Tor, mas sim o fluxo gerado pelo TorFlow e que permite uma impressão visual de extensão da rede.

3.4.4 Rede I2P

A rede I2P (acrônimo de *Invisible Internet Project*) é outra rede sobreposta à Internet, ou seja, assim como a rede Tor, não possui estrutura própria e depende da rede tradicional para funcionar. Foi criada em 2003 (mais de uma década após a rede Tor)

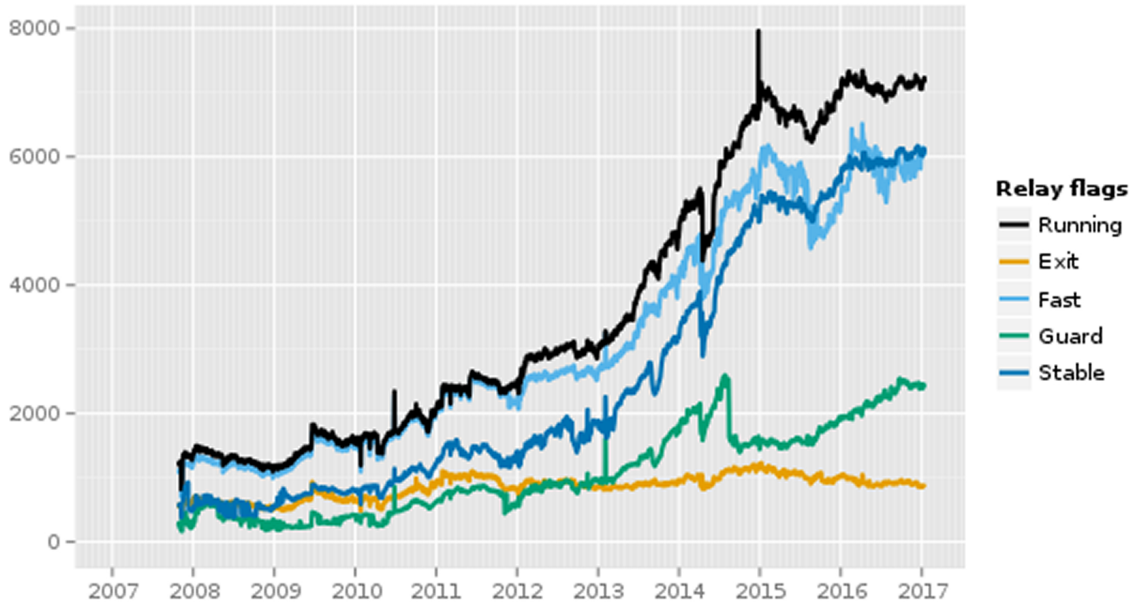


Figura 37: Levantamento de quantidade e tipos de *Relays* da rede Tor (TORMETRICS, 2017)

e tem como objetivo ser uma rede de anonimato. A diferença entre Tor e I2P é que a rede Tor permite que usuários acessem a Internet tradicional de forma anônima (protege a privacidade da origem da mensagem) e a rede I2P cria uma rede própria, de forma que sejam acessíveis apenas endereços específicos desta rede (protege a privacidade dos dois lados da conexão, isto é, a origem e o destino). São serviços diferentes e não concorrentes (DAVID, 2017; I2P, 2017a).

Assim como na rede Tor, a rede I2P possue uma especificação de URL (ex. `http://echelon.i2p`) que só é visível utilizando um *client* I2P[14], ou seja, tais *websites* são inacessíveis para a Internet tradicional. A rede I2P também é uma VPN e para que a comunicação entre dois clientes seja anônima, o aplicativo de cliente (que é um roteador) pode estabelecer vários túneis de entrada ou saída com outros pares (clientes) I2P.

Para se ter acesso à rede I2P, inicialmente o *software* cliente faz uma busca clientes *online* em uma base de dados distribuída. Isto é feito através de túneis específicos estabelecidos pelo I2P *client* I2P (2017b). Uma vez atualizada esta informação, o *software* cria túneis de saída e de entrada. O objetivo de se criar túneis de entrada e de saída é motivado pelo fato de que o cliente também passa a ser uma rota para que outros utilizadores da rede possam usufruir. Determinado o *website* de destino, como por exemplo `http://identiguy.i2p`, o aplicativo seleciona a melhor rota, isto é, o melhor túnel de saída para chegar ao destino. A Figura 38 (pág. 91) apresenta uma área do painel de controle do I2P *client*, no qual observa-se um túnel de entrada e dois túneis de saída. Na coluna "participantes" pode-se observar a quantidade de nós envolvidos no túnel, sendo

[14] `https://geti2p.net/pt-br/download`

que esta quantidade também pode ser pré-definida pelo usuário. A mensagem é então encriptada de ponta-a-ponta, ou seja, ambos os lados são criptografados e também os destinos são identificadores criptográficos, ou seja, chaves públicas criptográficas.

Figura 38: Exibição de túneis disponíveis conforme painel de controle do cliente I2P.

A rede I2P é um recurso viável para anonimato na Internet, entretanto funciona como uma rede a parte do mundo tradicional. Em vista da sua natureza em só permitir o acesso a *websites* internos da própria rede e com isto tornar-se incomunicável com a Internet tradicional, faz-se uma situação que a torna inviável como solução para a IoT. Esta natureza não permitiria por exemplo que um fabricante disponibilizasse recursos de acesso remoto a partir da Internet tradicional, seja para manutenção autorizada ou qualquer outra atividade cadastrada pelo usuário final e que necessite de comunicação com a rede mundial tradicional. Talvez fosse útil para aplicações extremamente críticas, porém, mesmo assim, uma vez que o cliente é também uma rota da própria rede, ele pode comprometer a sua capacidade de *hardware*.

3.4.5 Freenet

A Freenet também é uma rede que funciona sobreposta à Internet. Assim como na rede Tor e I2P, o acesso ao conteúdo da rede Freenet só é possível quando conectado a esta rede. Seu funcionamento é realizado de forma descentralizada e conforme Roos et al. (2014, p. 2) a conexão é realizada com pares confiáveis para garantir tal funcionalidade[15]. A rede funciona em dois modos denominados *Opennet* e *Darknet*. O modo *Opennet* é quando se conecta com pares desconhecidos, o que pela própria definição do Projeto Freenet não é assegurada a garantia de anonimato. No segundo modo denominado *Darknet*, ocorre a conexão com pares confiáveis, o que pode ter uma melhor garantia do anonimato. De forma geral, quanto mais pares forem conectados, maior é a chance de anonimato, entretanto o desempenho da rede é diretamente comprometido.

Esta rede possui recursos próprios para publicação de *websites*, sistemas de e-mail e mensageiros instantâneos. Tanto arquivos quanto usuários são identificáveis através de chaves criptográficas criadas no momento de inicialização do nó na rede. A incialização só é possível através de um *client* Freenet[16].

[15] Para usuários iniciantes a conexão ocorre com pares não confiáveis e à medida que se obtem a confiança com outras pessoas, estas passam a ser os nós confiáveis.

[16] Disponível em `https://freenetproject.org/download.html`

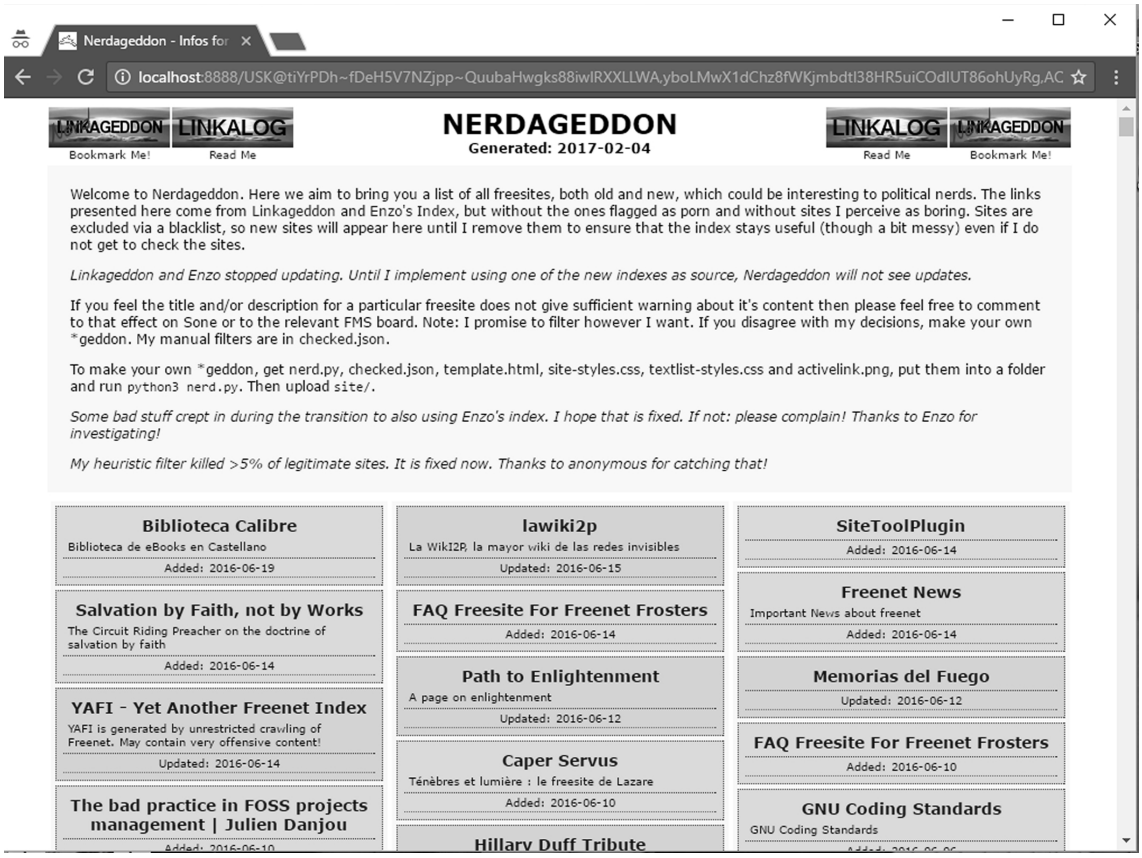


Figura 39: Visualização de *website* da Freenet e sua URL

A Freenet assim como as outras VPNs mencionadas possui uma estrutura de URL própria (Figura 39, pág. 92) que na verdade é uma extensa sequência de caracteres, acessível a partir de uma porta local[17] utilizada pelo *client* Freenet. Uma vez selecionado o destino, o *client* Freenet fará o *download* da página escolhida, motivo pelo qual deve-se usar pares confiáveis, pois qualquer arquivo da rede será baixado e não se sabe de onde e de quem pertence, pois há o anonimato.

Assim como no modelo I2P a qualidade de se tornar incomunicável com a Internet tradicional, faz da Freenet também uma solução inviável para IoT. Tem-se os mesmos problema identificados em razão da I2P, ou seja, maior dificuldade de comunicação entre fabricante e equipamento, diagnósticos, bem como a administração remota de dispositivos. Em contrapartida, tanto a rede Freenet como a I2P são soluções pouco prováveis para possíveis ataques cibernéticos em IoT. Fazendo uma analogia, seria como utilizar equipamentos navais da Marinha para submeter um ataque por terra.

Tanto a rede I2P como a Freenet são ótimas soluções para a privacidade e anonimato. Estas duas redes possuem a qualidade de manter o anonimato e privacidade na origem, destino e conteúdo da mensagem, entretanto em vista de não se comunicarem diretamente com a Internet tradicional, se tornam uma solução tecnológica com menos

[17] Por padrão o Freenet utiliza a porta local 8888 para acesso à rede.

peso no quesito usabilidade ao considerar a equação Usabilidade *Versus* Segurança.

Ao usar uma VPN para IoT é essencial que haja comunicação com a Internet tradicional e considerando esta qualidade exigida, o uso de VPN criada por meios tradicionais para uma finalidade específica ou mesmo a rede Tor poderiam ser mais adequadas ao contexto. Conforme mencionado, tais VPNs não são concorrentes e sim tecnologias diferentes. Com isto, a Tabela 8 (pág. 93) apresenta o resumo comparativo no contexto de anonimato e privacidade entre estas redes perante a Internet.

Tabela 8: Resumo comparativo no contexto de proteção à privacidade entre as redes Tor, I2P e Freenet perante a Internet.

Tecnologia	**Origem**	**Destino**	**Conteúdo**	**Internet**
Tor	não conhecido	conhecido ou não	conhecido ou não	acessível
I2P	não conhecido	não conhecido	não conhecido	não acessível
Freenet	não conhecido	não conhecido	não conhecido	não acessível
VPN própria	não conhecido	conhecido	conhecido ou não	acessível

3.5 Trabalhos relacionados

Considerando as entidades elencadas na Figura 5 (pág. 33) foi feito um levantamento de registros de padronização e normatização diretamente relacionados à IoT com o objetivo de filtrar e analisar documentos que propõem diretrizes no mesmo âmbito da presente tese, ou seja, abordagens exclusivamente em nível de política & governança:

a. **ITU**: consta uma totalidade de 56 documentos relativos à *Internet of Things, smart cities and communities*, dentro dos quais 5 são relativos à identificação e segurança, identificados pela nomenclatura Y.4800-Y.4.899 conforme consulta na base em ITU (2017b). Nenhum dos documentos refere-se a uma proposição de modelo de segurança ou discussão de proteção à privacidade em IoT, mas no que tange a esta tese destaca-se ITU-T (2014a, p. 7) que descreve requisitos e características para serviços em IoT, sugerindo a proteção da privacidade durante a captura, transferência, armazenamento e validação de dados.

b. **ISO/IEC**: conforme IEC (2017b) a ISO e IEC possuem 9 documentos em coautoria, mas nenhum deles discute efetivamente a privacidade ou propõe um modelo de segurança, entretanto destaca-se o documento ISO/IEC CD 30141:2016 (ISO, 2016) que visa propor uma referência de arquitetura para IoT. Trata-se de um documento em fase de desenvolvimento e que sinaliza uma possível primeira padronização ISO em termos de arquitetura IoT. Considerada a importância da organização ISO diante do cenário de padronização em vista de sua correlação com diversas organizações (conforme observado pela Figura 5) é um documento que convém ser observado. Não

se trata de uma norma específica para segurança da informação, mas sugere dentre seus objetivos que se tenha como princípio a proteção de informações de identificação pessoal. A contribuição que a ISO/IEC 30141:2016 trás a esta tese é sugerir como característica de um sistema IoT que todas as informações de identificação pessoal sejam protegidas (ISO, 2016). Esta mesma proposição é realizada por Evangelista, Nogueira e Santos (2015) que de um modo mais agressivo, sugere que todos os dados (não somente de identificação pessoal) adquiridos/gerados por dispositivos IoT sejam classificados como privados.

c. **IETF**: a busca na base de dados em IETF (2017b) retornou um total de 11 registros. Nenhum deles se refere a modelo de segurança ou discorre especificamente sobre a privacidade. Entretanto, existe diversos documentos de padronização produzidos pelos grupos mantidos pelo IETF que contribuem para a evolução da tecnologia, como por exemplo a definição de métodos[18] para adaptação do IPv6 ao padrão IEEE 802.15.4[19] (IETF, 2014).

d. **IAB**: conforme pesquisa na base disponível em Sullivan (2017), foram encontrados apenas dois documentos (duas RFCs *draft*) relacionados à IoT e que são *reports* de *workshops* específico de IoT realizados no ano de 2016. Tschofenig e Farrell (2017) tem como informação relevante a sugestão de classificação dos dispositivos de IoT em dois tipos diferentes e Jimenez, Tschofenig e Thaler (2016) discorre sobre aspectos de linguagem formal para documentação e geração de código. Em consulta realizada em 06/07/2017 por e-mail ao mantenedor da base disponível em Sullivan (2017), Andrew Sullivan, este retornou informando não acreditar que a IAB escreva alguma RFC sobre o assunto, mas apenas promove eventos relacionados ao tema. Porém trazendo a busca para uma visão mais abrangente, através da RFC 6973 a IAB descreve considerações de privacidade para protocolos de Internet. O documento trás de forma relevante a classificação de ameaças que envolvam a privacidade (COOPER et al., 2013):

   - **segurança**: observação e monitoramento de uma atividade ou comunicação individual;
   - **comprometimento de dados armazenados**: sistemas finais que não tomam providências para proteger dados armazenados
   - **intrusão**: ações invasivas que geram disturbios ou interrompem na vida ou atividade das pessoas;
   - ***misattribution***: atribuição de dados ou comunicações de uma pessoa à outra pessoa. Relacionado à falsificação, uso de identificação de outro usuário.

[18] Disponível através da RFC 4944 e atualizações realizadas através das RFCs 6282, 6775, 8025, 8066 (IRTF, 2007).

[19] Padrão IEEE para redes sem fio de baixa frequência, disponível em IEEE (2015a).

- **correlação**: combinação de várias informações de um indivíduo ou que obtém essa característica quando combinados vários dados.
- **identificação**: ligação de informações a um usuário em particular, permitindo a inferência de identidade.
- **uso secundário**: coleta de dados do indivíduo sem o seu consentimento, para uma finalidade diferente daquela para a qual foi coletada.
- **exposição**: revelação de dados de um indivíduo de modo a influenciar o modo como outras pessoas o julgam.
- **exclusão**: não permitir que o indivíduo saiba sobre seus dados que outros possuam e participar do seu tratamento e uso.

e. **ISOC**: possui um *whitepaper* com uma visão geral sobre a IoT no qual aborda problemas e desafios relacionados e dentre estes estão a segurança e privacidade. É levantado que a segurança é fundamental para que as pessoas confiem na IoT. A falta de confiança nos dispositivos conectados pode ocasionar uma global relutância no uso da tecnologia. O documento sugere também que um dispositivo mal protegido e conectado à Internet pode comprometer a segurança e resiliência global da rede e não apenas localmente (ISOC, 2015, p. 32). Esta sugestão reforça a necessidade de um modelo de segurança em nível de política e governança, o qual possa instigar os demais níveis de padronização. Em termos de privacidade, o desafio é crítico em vista do poder de vigilância, coleta e análise de dados que a IoT pode propiciar (ISOC, 2015, p. 40-41). Uma das iniciativas da ISOC é executado pela *Online Trust Alliance* conforme (OTA, 2014). Esta iniciativa possui um *framework* relativo à confiança na IoT com o intuito de priorizar a segurança e privacidade (OTA, 2017a). Como contribuição relevante à esta tese, o documento sugere que dispositivos IoT possuam um "tempo de validade" de modo que fique explícito até quando o dispositivo poderá receber atualizações de segurança e receber suporte por parte do fabricante. Após este prazo, o dispositivo passe a operar sem conectividade.

   Em OTA (2017b) é abordada a questão do procedimento de descarte ou transferência de dispositivos IoT para outras pessoas. O trabalho ressalta o problema da descontinuação de suporte quando determinado dispositivo se torna obsoleto. Para reduzir o risco de segurança à privacidade, é sugerido que alguns de pouco impacto passem a funcionar sem conectividade. Também é sugerido a existência de um botão de *reset* em todos os equipamentos. Uma vez acionado, todos os dados de usuário seriam apagados do dispositivo. Este recurso seria útil em processos de descarte ou transferência de propriedade do equipamento para outro usuário.

f. **W3C**: esta organização mantém um grupo de trabalho (iniciado em fevereiro de 2017) especialmente criado para traçar diretrizes para a IoT (W3C, 2017a). A con-

tribuição por parte da W3C é a inserção do termo *Web of Things* ou WoT. No *White Paper for the Web of Things* (RAGGETT; ASHIMURA; CHEN, 2016) reforça-se a necessidade de busca de uma padronização que permita a fácil integração entre sistemas IoT e aplicações. Trata-se de uma documentação voltada à interoperabilidade e não à segurança e privacidade.

g. **ETSI**: foi feita a busca na base de dados em ETSI (2017b) utilizando como chave a expressão "*internet of things*" foi obtido um resultado com mais de 8 mil registros. Deste modo fez-se necessário a adição de um segundo filtro, sendo o termo "*privacy*". Com a combinação dos dois termos, a resposta foram 8 registros de documentos que falam sobre IoT e privacidade. São tratados assuntos relacionados à rádio frequência, importância de cuidados com o *gateway*, proteção para dispositivos móveis e dados armazenados em rede, segurança em sistema de transporte inteligente, entre outros tópicos, mas não há a proposição de modelos de segurança para IoT.

h. **IEEE**: assim como nos casos anteriores, foi realizada a busca utilizando como critério as expressões "*internet of things*" e "*privacy*" no título, resultando em 74 registros[20]. Dentre os registros encontrados, Pishva (2017) propõe um modelo apenas em nível de *software* e que atua no *gateway*. Com isto, a proposta consegue mitigar ataques *man-in-the-midle* mas não ataques internos como sybil[21], sinkhole[22] e outros possíveis. Hernandez-Ramos, Bernabé e Skarmeta (2016) propõe um modelo apenas em nível de *software* que foca-se na autenticação e autorização. Stout e Urias (2016) foca-se na CIA-triad, fazendo uma revisão de possíveis ameaças bem como o comprometimento da privacidade quanto a estes, mas não adiciona novo modelo de segurança.

O Internet of Things European Research Cluster (IERC) é uma organização que funciona como uma plataforma de cooperação entre desenvolvedores IoT da Europa. Em Levitt (2015) são descritos os projetos de pesquisa europeus voltados para IoT: iCore IoT, Iot@Work, BUTLER, RERUM (RERUM, 2013), COMPOSE (MANDLER, 2015), GAMBAS (GAMBAS, 2016), OpenIoT (OPENIOT, 2016) e SPaCIoS. Cada um destes projetos tem foco em um ambiente específico para aplicabilidade: trabalho, saúde, automação industrial, entre outros.

Em todos estes projetos as principais questões estudadas são a governança, a segurança e a privacidade. A privacidade é apontada como algo difícil de ser tratada em vista de três fatores: tamanho e heterogeneidade de equipamentos (em consonância com a

[20] Também foi realizada a busca dos termos "*internet of things*" e "*privacy*" apenas nos metadados. Com isto, obteve-se um total de 1.106 registros, dos quais vários não tinham a privacidade como elemento principal, mas de algum modo tocavam neste assunto.

[21] Ataque que caracteriza-se pela manipulação de identidades fabricadas ou roubadas.

[22] Este tipo de ataque consiste em atrair a maior quantidade de tráfego de uma determinada área, prejudicando um ponto de coleta de receber dados enviados pelos nós, sendo considerado um dos ataques mais destrutivos em IoT (CERVANTES et al., 2014) *apud* (QI et al., 2012).

conclusão de Sengul (2017)), proteção dos dados armazenados e proteção da comunicação dos dados. A diversificação de dispositivos IoT dificulta a existência de um modelo de segurança que se aplique de igual maneira para todos. Diversos autores propõem soluções específicas a cada contexto conforme observado em Cervantes et al. (2014), Baldini et al. (2016), Schurgot, Shinberg e Greenwald (2015), Teixeira et al. (2014), Abdullah, Rahman e Roy (2015), Shafiei et al. (2014), Johnston, Scott e Cox (2016), Ge e Kim (2015), Neisse et al. (2014), Jacobsson e Davidsson (2015) que são soluções apenas em nível de *software* ou *hardware* ou algum cenário específico. Entretanto, convém a proposição de um modelo em nível de política e governança, de forma que este possa facilitar a condução de modelos concernentes à segurança da privacidade em nível de *hardware*, *software* ou serviço & infraestrutura.

Dentre as pesquisas encontradas, Pentland (2014) e Kranenburg (2008) apresentam propostas para eliminação do problema com a privacidade. Apesar da simplicidade de solução proposta, são complexos para aceitação na sociedade, principalmente empresas e governos pois envolvem questões éticas.

Pentland (2014) baseia-se na transparência, propondo uma forma para definir a propriedade dos dados e controle do fluxo. A ideia é dar às pessoas a capacidade de ver que informações estão sendo coletadas a seu respeito (sejam privadas ou não) e deixar que estas pessoas aceitem ou não o compartilhamento. Esta proposta é uma forma de equilibrar o poder da informação. Não faz parte da proposta proibir empresas de criar produtos a partir dos dados das pessoas (no caso seus clientes), mas especificar regras e princípios de transparência.

Kranenburg (2008) propõe uma linha mais radical da transparência total. Nesta proposta todos os dados seriam públicos. Isto quer dizer que dados pessoais, empresariais e também governamentais seriam públicos e qualquer pessoa teria acesso a tudo. A ideia nesta proposta é permitir que ao mesmo tempo empresas e governos possam tomar decisões baseado em informações privadas das pessoas, bem como as pessoas poderiam interferir de forma mais efetiva nas diretrizes empresariais e governamentais. Este tipo de solução é retratada no filme "O círculo" (BREGMAN et al., 2017). Se trata de uma obra de ficção científica mas é tocante em dois pontos interessantes. O primeiro ponto diz respeito a um bordão do filme que é a expressão "compartilhar é cuidar". Tendo este como um princípio a ideia discorre em torno de que quanto mais compartilhada a privacidade, maior será a segurança das pessoas. Convém que tudo seja compartilhado, incluindo imagens em tempo real e histórico de ações. Em contrapartida o segundo ponto diz respeito à referência do uso de dados pessoais para acúmulo de riquezas. Os dados incluem: fotos, histórico de ações, alimentação, círculo de amizade, prontuário médico, situação da saúde em tempo real, entre outras possibilidades. São muitos dados gerados para se processar e uma vez processados, poderiam ser explorados economicamente. Ressalta-se novamente

que é um ambiente de ficção científica mas ambos os pontos são possíveis situações de se alcançar através da IoT na vida real. Por isto, o excesso de exposição da privacidade pode ser mais maléfico do que benéfico.

Também foi identificado o *whitepaper* ARM (2017) que propõe um modelo para aplicação na IoT chamado *Platform Security Archictecture* (PSA) que é um conjunto holístico de modelos de ameaças, análise de segurança e *hardware* bem como especificações de *firmware*. O modelo proposto tem foco inicialmente nos dispositivos baseados em processadores desenvolvidos pela própria empresa e trata-se de um modelo aplicável no âmbito de *hardware* e *software*.

Por fim, é apropriado citar o estudo "Internet das Coisas: um plano de ação para o Brasil". É um estudo liderado pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES) em parceria com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC). Sua finalidade é diagnosticar e propor um plano de ação para a viabilização da IoT no país. A visão do plano de ação é:

> 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, 2017, p. 12)

Um dos relatórios do estudo está em BNDES (2017) no qual constam as quatro frentes prioritárias[23] de IoT para o país e que são: cidades, saúde, fábricas e rural. Para todas estas frentes o documento aponta dentre seus desafios, quesitos relativos à segurança e privacidade e que são pertinentes.

O primeiro diz respeito à estrutura de criação de um marco regulatório de proteção de dados pessoais. "*O desenvolvimento de soluções de Internet das Coisas perpassa pela edição de norma sobre proteção de dados pessoais que lide com a complexidade e as nuances do contexto tecnológico(...)*" BNDES (2017, p. 40). A falta de regulação da proteção de dados pessoais ainda é considerado um desafio para evolução da IoT no Brasil. Mesmo diante da legislação vigente (Brasil (2014) entre outros), cita-se como desafio esta regulação.

O segundo quesito sugere o incentivo à iniciativa privada para a criação de sistemas que certifiquem a segurança da informação em dispositivos IoT. (BNDES, 2017, p. 41)

[23] O processo de priorização detalhado está disponível no link `https://www.bndes.gov.br/wps/portal/site/home/conhecimento/estudos/chamada-publica-internet-coisas/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil`

4 PROTEÇÃO DA PRIVACIDADE NO AMBIENTE IOT

Embasando-se nas análises exploratórias e críticas realizadas no decorrer dos capítulos anteriores é possível completar o objetivo da tese através do paradigma de proteção da privacidade na IoT. Entretanto, tal descrição é precedida pela explicação dos pontos (requisitos e definições) então estabelecidos nesta tese como determinantes para condução do trabalho:

1. **Onipresença de dados**: é uma tendência comprovada a observar pela industria 4.0, o conceito de *Cyber Physical Systems* como nova área computacional e demais tecnologias para cidades inteligentes. A Internet permite que dados e informações através de textos, imagens, sons e vídeos estejam disponíveis como previa (MCLUHAN, 1964) na década de 60. A integração das "coisas inteligentes" à Internet trás consigo um novo patamar em termos de quantidade de dados onipresente, permitindo uma "digitalização" cada vez maior das ações e também previsões de ações humanas. Este fator permite que a IoT compartilhe e favoreça os princípios de evolução da Internet: prosperidade sadia da humanidade e igualdade entre povos. A onipresença de dados viabiliza estes objetivos. A interoperabilidade com a grande rede torna possível a integração com outros sistemas que conjuntamente podem ser utilizados para o bem comum das pessoas. Entretanto, sempre há quem explore e utilize algo bom para finalidades não boas. Ainda assim, este requisito é salutar de modo que possibilita ações como a aplicação de atualizações de segurança por parte de fabricantes, manobra esta que é elementar na mitigação de ataques *zero day*. Também há situações em que a interoperabilidade deve limitar-se à rede local, seja em sistemas de defesa, equipamentos militares autônomos, monitoração de sinais vitais, entre outras possibilidades. Por fim, não é um recurso obrigatório mas no entanto é apropriado que "coisas inteligentes" estejam conectadas à Internet.

2. **uso de VPN em casos críticos**: são redes que se utilizam da estrutura da Internet e que possibilitam uma forma de encobrir o conteúdo das mensagens. É um recurso essencial e fortemente sugerido para aplicabilidade principalmente quando a IoT envolver tarefas críticas ou vitais como: suporte à vida, segurança de pessoas ou defesa considerando que o espaço cibernético é agora considerado um novo domínio de guerra. No mundo físico, ataques (de qualquer magnitude) ocorrem esporadicamente: um ladrão não fica insistentemente tentando arrombar uma casa; uma nação não fica insistentemente lançando mísseis para tentar derrubar determinado alvo em

outra nação; uma pessoa mal intencionada não fica insistentemente tentando entrar no cofre do banco. Diferentemente, no espaço cibernéticos tentativas de acesso ilegítmo, roubo de dados, adulteração de sistemas, são exemplos que ocorrem de forma insistente e sem descanso. A constante ameaça de invasão é real. Deste modo, são necessários recursos de proteção que garantam a comunicação entre os dispositivos inteligentes para cumprimento de seus objetivos.

3. ***log* de todo e qualquer acesso ao equipamento IoT**: convém registrar todos os acessos ao equipamento de IoT de forma a manter um histórico local ou em nuvem de todos os acessos realizados por outro equipamento IoT ou por humano. Este requisito torna possível a auditoria de equipamentos e acessos, o que poderá ser útil em questionamentos judiciais ou auditorias.

4. ***log* de consentimento**: convém manter registro de todos os consentimentos dados pelo usuário armazenando esta informação em nuvem. Este registro é uma forma de manter inventariado o termo de ciência do usuário, atestando que este tem conhecimento que seus dados serão utilizados na IoT. Este registro é uma forma de monitoração persistente e com isto pode ser submetido ao procedimento de auditoria.

5. **confiabilidade ao destino vinculado**: convém que cada outro equipamento que se conecte ao dispositivo IoT seja confiável para tal. Esta confiança será determinada pelo usuário e com isto eleva a responsabilidade humana diante dos próprios dados privados.

6. ***log* de confiabilidade ao destino vinculado**: é recomendado nos mesmo moldes que o *log* de consentimento. Este funciona como um registro de vínculo entre o usuário e o dispositivo destino dos dados.

7. **política restritiva e controle de acesso realizado por humano**: convém manter um mecanismo que faça o controle de quais origens são permitidas acessar o dispositivo. Este mecanismo pode se dar através da associação de IPs e usuários ou equipamentos previamente cadastrados. Sugere-se que o equipamento inicie com uma política restritiva, ou seja, a liberação ocorre à medida que necessário.

8. **recurso de amnésia**: convém que todo dispositivo IoT possua um mecanismo de amnésia. Este recurso é imprescindível no descarte de equipamentos obsoletos ou na transmissão de propriedade para outro usuário. Uma vez acionado este mecanismo, todo o conteúdo de dados de usuário armazenado devem ser apagados.

9. **restrição total quanto ao anonimato para IoT**: anonimato não é uma qualidade aceitável quando se fala em dispositivos que funcionem sem a coordenação humana. Recomenda-se fortemente a proteção contra acesso anônimo ao dispositivo IoT. Isto

pode ser conseguido através do mecanismo de controle de acesso, bem como através de um mecanismo de bloqueio de acessos originados a partir da rede Tor (única rede oculta que se comunica com *hosts* da Internet tradicional). O próprio projeto Tor disponibiliza um *link*[1] que permite identificar todos os *relays* de saída que chegam a um IP da Internet. O Apêndice C sugere um *shell script* como exemplo de implementação deste bloqueio.

10. **confidencialidade**: o modelo ora proposto sugere como princípio básico que todos os dados sejam classificados como privados. Logo, é necessário tornar estes dados confidenciais, provendo recursos que tornem a confidencialidade uma característica indispensável aos dados armazenados ou que trafegam do dispositivo para qualquer destino remoto.

11. **integridade**: os dados adquiridos ou gerados pelo dispositivo IoT devem manter-se inteiros e intatos. A integridade de dados é fundamental para que a IoT alcance seu objetivo. A violão da integridade compromete a IoT, induzindo-a a um comportamento com intenções.

12. **disponibilidade**: convém que os dados adquiridos ou gerados pelo dispositivo IoT estejam disponíveis quando solicitados. Este requisito é questionável uma vez que existem situações nas quais os dispositivos estarão localizados em regiões de difícil acesso ou qualidade baixa de sinais. Entretanto, sem a disponibilidade de dados, a IoT perde sentido de existência. Em casos extremos, sugere-se um mecanismo pré-estabelecido para a coleta ou fornecimento de/para o dispositivo IoT. Isto pode ocorrer conectando-se fisicamente ao dispositivo ou por "visitas" cronológicas em proximidade que permita a interconexão.

4.1 Descrição do paradigma

O objeto desta tese é apresentado através do paradigma demonstrado na Figura 40 (pág. 102). Este não se constitui um modelo de referência, mas uma prévia, um exemplo de modelo que pode tornar-se referência mediante submissão a um método de experimentação em laboratório. Sobretudo, este modelo foi concebido observando os requisitos e definições então estabelecidos.

Este paradigma tem como característica ser especialmente criado para aplicação no contexto de IoT e sugere como inovação os seguintes fatores:

a. propõe a inserção do novo objetivo de segurança para IoT a saber: **permissão explícita**, isto é, sem ambiguidade, clara, suficientemente esclarecedora de que o usuário deu o consentimento para uso de seus dados por parte do dispositivo IoT;

[1] `https://check.torproject.org/cgi-bin/TorBulkExitList.py?`

b. propõe a inserção do novo objetivo de segurança para IoT a saber: **confiabilidade no destino vinculado** de forma que a segurança da privacidade seja atrelada ao destinatário e não somente ao próprio dispositivo IoT e a comunicação entre este e o destino.

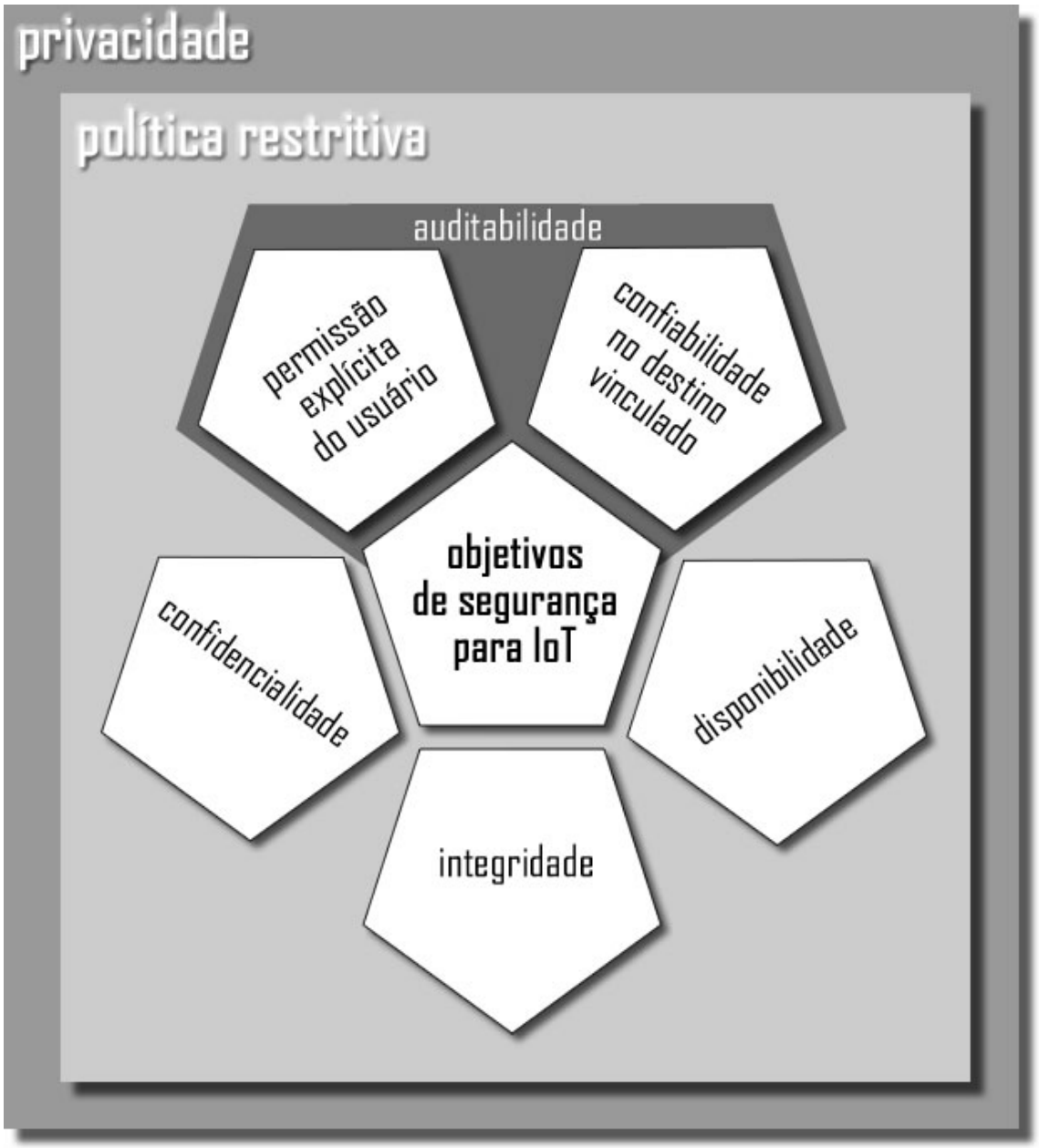


Figura 40: Objetivo principal desta tese: paradigma para segurança da informação específica para IoT.

Conforme demonstra-se na Figura 42 (pág. 103) o limite de atuação abrange o dispositivo IoT, estende-se pela comunicação dos dados e vai até o encontro com o destino vinculado à conexão. Observa-se que o modelo não abrange a segurança do recurso remoto em si. No âmbito dos níveis de padronização da Internet, o modelo é específico do nível de política e governança, o que o torna uma possível base para elaboração de políticas dos níveis inferiores (Figura 41, pág. 103).

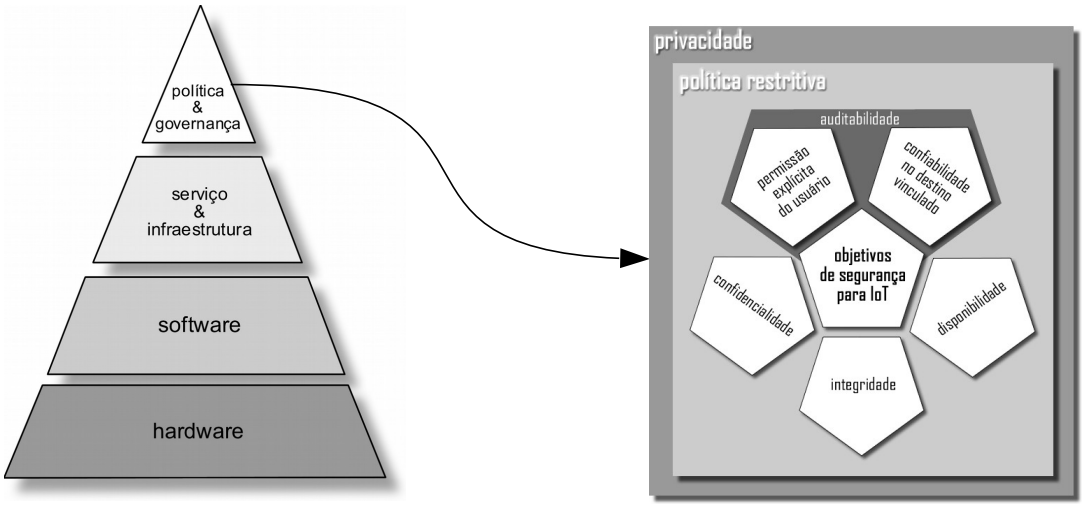


Figura 41: Correlação entre os níveis seccionados de padronização e a sistematização ora proposta.

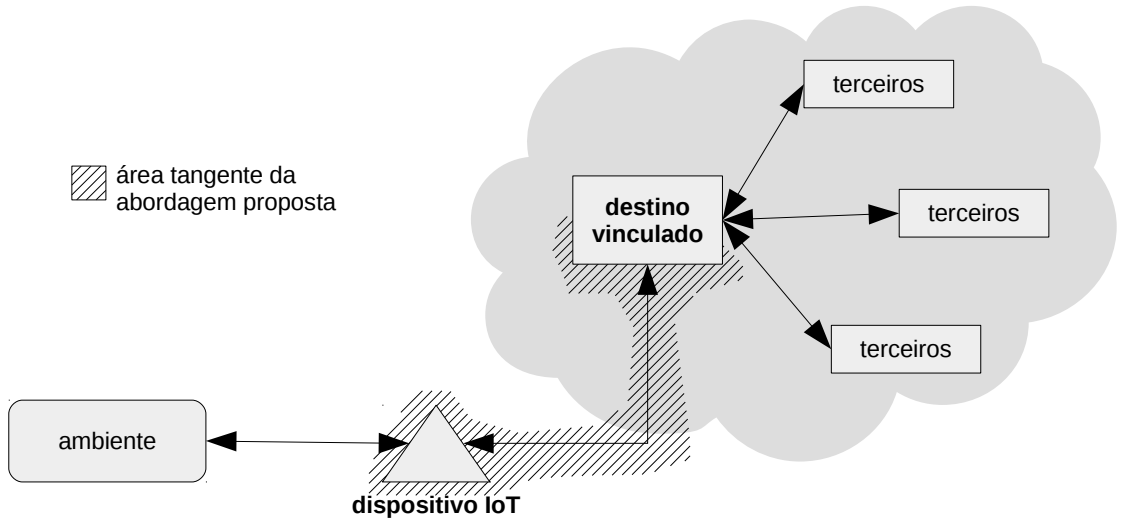


Figura 42: Demonstração visual da área tangente do paradigma proposto nesta abordagem.

A Figura 43 (pág. 104) apresenta o fluxograma que demonstra a integração da CIA-triad à inserção proposta nesta abordagem. São considerados inicialmente os princípios "privacidade" e "política restritiva". Em seguida tem-se a fase de validação humana que é composta pelo consentimento para uso de dados e afirmação da confiança no dispositivo remoto ao qual os dados serão enviados. Estas ações são registradas em *log* viabilizando a auditabilidade. Uma vez cumpridas estas etapas, integra-se a CIA-triad como é conhecida. A etapa de validação humana é determinante para que os dados (privados) sejam utilizados. Em seguida serão descritos cada um dos elementos do fluxograma.

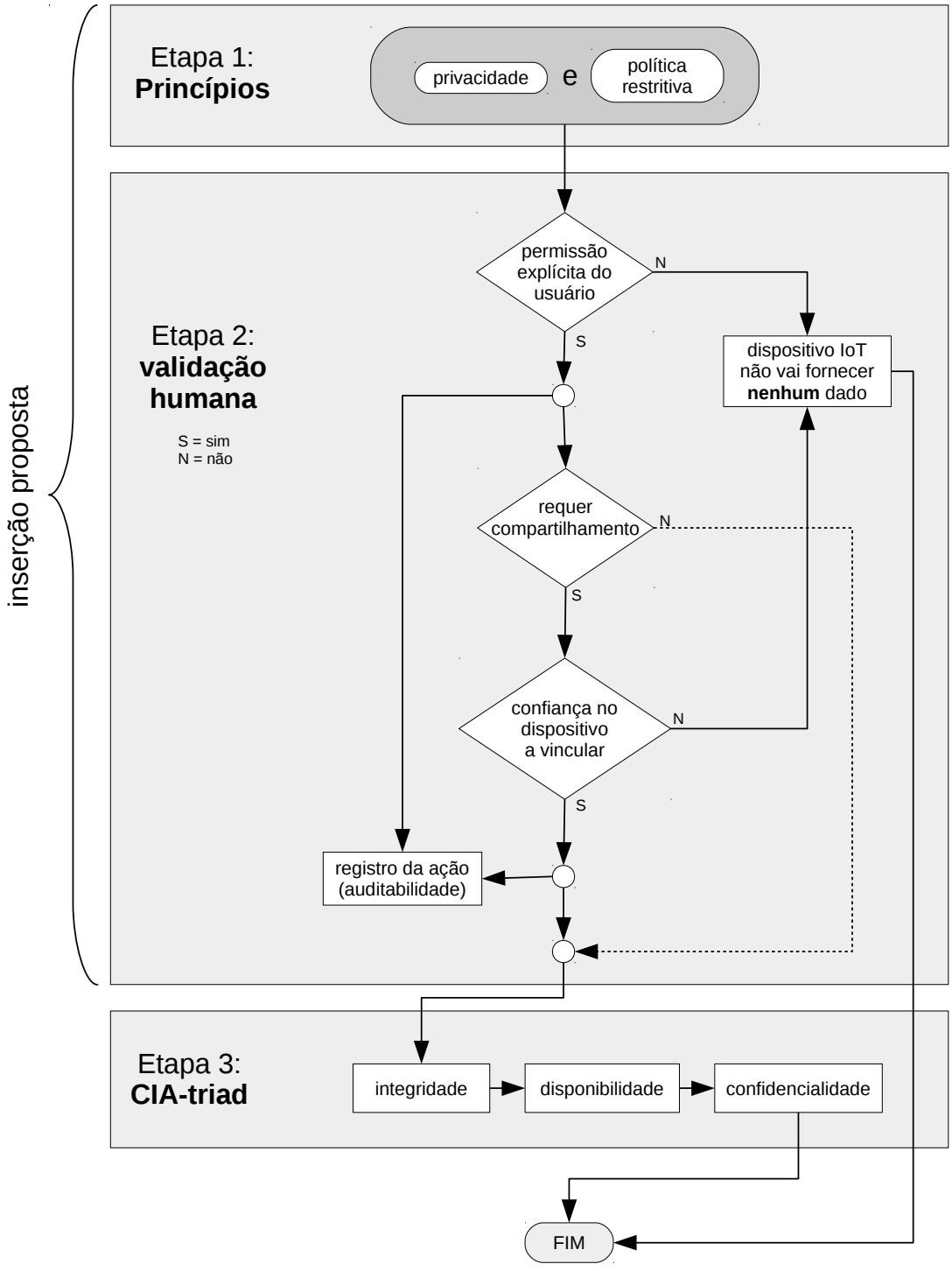


Figura 43: Fluxograma funcional demonstrando a integração da CIA-triad à inserção proposta nesta abordagem.

4.1.1 Princípios

A palavra "princípio" origina-se do latim *principium* que significa aquilo que serve de base para alguma coisa, uma regra fundamental a ser considerada (VIEIRA; MICALES, 2016, p. 331), (HOUAISS; VILLAR; FRANCO, 2009, p. 1552). Deste modo, assume-se para o início do processo de segurança à privacidade na IoT que sejam considerados como

princípios, isto é, o mínimo aceitável: a privacidade e a política restritiva.

No primeiro princípio tem-se a **classificação de todos os dados como privados (privacidade por padrão)**. Cada dado ou informação sobre um indivíduo vale algo para alguém e poderá ser usado para fins ilícitos. Conforme observado por CERT.br (2012, p.85) é comum na Internet a exposição/uso de dados independente da vontade do proprietário. Com o advento da IoT em que dados pessoais estão em maior evidência, torna-se visível a necessidade da classificação de todos estes como privado. Uma vez assumida a privacidade como princípio básico, por padrão todos os dados (sem exceção) que o dispositivo tenha contato, sejam adquiridos ou gerados, serão classificados como privados, isto é, passam a ser considerados como conteúdo particular, próprio, que não diz respeito a terceiros. Com isto, elimina-se a necessidade de qualquer procedimento de classificação de dados em termos de privacidade. Uma vez dentro da IoT, qualquer dado é classificado como tal. Esta generalização é conveniente perante a nova realidade tecnológica e a privacidade das pessoas.

Tal universalização também elimina a necessidade de configurações de privacidade por parte do usuário. Anteriormente observado em Lee e Kobsa (2016) a maior parte das pessoas não possuem ou não se interessam por conhecimento suficiente para entender o poder que seus dados possam ter quando em posse de computadores ou pessoas, sejam estas com intenções ilícitas, comerciais ou qualquer outra. Evidentemente este é um outro problema crítico e a generalização de todos os dados como privados dispensa o usuário do processo de classificação, mas realça o poder do consentimento de uso dos dados enfatizando que em IoT todos os dados sem exceção serão considerados privados. Dentre os modelos levantados, a privacidade é algo intrínseco, mas não é assumida de forma explícita. A única exceção é o modelo RMIAS (CHERDANTSEVA; HILTON, 2013) que trás a privacidade como objetivo explícito de segurança, mas este não é um modelo específico para IoT.

O segundo princípio é a **definição da política geral (restritiva por padrão)**. Definir a política geral da segurança é estabelecer o critério ao qual todas as regras de segurança deverão seguir. São duas as formas básicas de política: permissiva e restritiva. As duas são eficientes mas nem sempre funcionam bem no mesmo contexto. É necessário um estudo de caso para avaliar a melhor política em cada circunstância específica.

Uma política permissiva é aquela em que por padrão tudo é liberado e os bloqueios ou restrições de acesso são aplicados à medida que necessário. Um exemplo de uso desta política está na configuração de regras do *firewall*[2] de um *serviço web*. A política permissiva permite que o conteúdo do *site* seja acessível a partir de qualquer origem na rede. Quando detectadas tentativas de ciberataques, então é realizado o bloqueio dos IPs específicos que

[2] Ponto de controle entre duas ou mais redes, composto por regras que liberam ou negam a passagem de pacotes de dados entre as mesmas (MACHADO JR, 2015).

originaram a ofensiva. Deste modo, a *blacklist*[3] deverá ser alimentada com endereços tidos como perigosos.

Uma política restritiva é aquela em que por padrão tudo é bloqueado e as liberações ocorrem à medida que vão sendo realmente necessárias. É o tipo de política adotada na configuração do *firewall* de um ambiente institucional por exemplo. Este tem como auxílio uma *whitelist*[4].

Com isto, é proposto que por padrão todo e qualquer equipamento de IoT deve trabalhar adotando uma política restritiva e assim todas as conexões (saída e entrada) são inicialmente bloqueadas. A liberação/consentimento de acessos devem ser concedidos à medida que necessário. O *firewall* responsável por este gerenciamento pode ser individual em cada dispositivo IoT ou no caso de sistemas nos quais diversos dispositivos conversam entre si e se comunicam com a Internet através de um mesmo dispositivo de *gateway*, este dispositivo de saída poderá realizar o controle.

4.1.2 Validação humana

Uma vez satisfeitos os princípios, a próxima etapa (conforme Figura 43) refere-se à validação humana. Nesta fase o fator humano torna-se parte do modelo de segurança e portanto é co-responsável pelo controle da privacidade de dados. Não se trata de uma classificação conforme mencionado, mas é uma etapa que acentua a autoridade do usuário no consentimento do uso dos dados privados na IoT. Conforme observado, o direito à privacidade é assegurado por Lei e ao mesmo tempo não há garantia se observado em Brasil (2014, Art. 7, Inciso III). Deste modo, o modelo ora proposto conta com a confidencialidade, mas acima desta, a validação humana é reinvindicada de modo que o usuário tenha a percepção da manipualação de dados privados. Participam desta etapa as seguintes decisões humanas: **permissão explícita do usuário** (consentimento para uso), **ciência da necessidade de compartilhamento externo** e **confiabilidade no dispositivo vinculado**.

Em termos de segurança da informação o fator humano é tido como o elo mais fraco da corrente. A privacidade nem sempre é objeto proeminente para a grande maioria dos usuários, quanto mais a segurança desta. Tal descaso é um ponto enfraquecedor de quaquer sistema de segurança da informação. A inserção da etapa de validação humana no modelo de segurança ressoa como algo contraditório, mas uma vez delegadas as funções de consentimento e confiabilidade no destino dos dados, o usuário tem a oportunidade de questionar o motivo de seus dados pessoais serem enviados a determinado destino. É um meio permanente de conscientização do usuário para que acidentes envolvendo violação de

[3] "Lista Negra" de endereços IPs a serem bloqueados por motivo de desconfiança ou autoria de ações ofensivas realizadas.

[4] "Lista Branca" de endereços IPs a serem liberados, ou seja, só deve constar nesta lista atores confiáveis.

privacidade sejam mitigados. Mesmo que ocorra, que seja resolvido no prazo mais curto e com o menor prejuízo possível (SASSE; BROSTOFF; WEIRICH, 2001), (MARCIANO; LIMA-MARQUES, 2006), (ALENCAR; LIMA; FIRMO, 2013), (ROCHA, 2008), (OTA, 2017b).

O consentimento, isto é, a **permissão explícita do usuário** é um dos novos objetivos propostos. Este "estar de acordo" faz com que o usuário se torne parcialmente responsável pela segurança de seus dados privados na IoT. Uma vez que o usuário não autorize o uso, o dispositivo IoT não vai fornecer ou gerar nenhum dado. Obviamente este controle de permissão está limitado quando a tentativa de aquisição de dados ocorre em dispositivos em poder do usuário, ou seja, quando há a necessidade de comunicação de "coisas inteligentes" como *wearables*, *smartphone*, entre outros. Todos os consentimentos dados pelo usuário podem ser armazenados em uma base na nuvem, associando usuário, equipamento e transação permitida/negada. Esta informação poderia ser usada em processos jurídicos que envolvam o comprometimento de privacidade.

A inserção do termo "explícito" é motivada levando em consideração sua definição do latim ***explicitus*** que significa aquilo que é explicado, que é claro, sem ambiguidades (HOUAISS; VILLAR; FRANCO, 2009, p. 858), (VIEIRA; MICALES, 2016, p.148). Deste modo, a adoção da expressão "permissão explícita" tem por objetivo forçar a exclusão de qualquer ambiguidade ou obscuridade nos termos de permissão. Tal objetivo acontece em consonância com a *General Data Protection Regulation* (GDPR) que entrou em vigor no dia 25 de maio de 2018. A GDPR é uma nova Lei européia que reforça a proteção de dados dos cidadãos europeus (SCHULZ; HENNIS-PLASSCHAERT, 2018). Dentre as características desta nova lei, destaca-se a ênfase na transparência, de modo que consentimentos sejam realizados de forma clara o suficiente para não se confundir com outros assuntos.

(SCHULZ; HENNIS-PLASSCHAERT, 2016; UNION, 2016)

É importante que se tenha mecanismo de revogação de consentimento, mecanismo este com efeito imediato. Este tipo de recurso é essencial em situações em que ocorra a quebra de confiança ou pelo simples desejo de que seus dados (privados) não sejam mais utilizados. Tal mecanismo pode ser alocado na primeira decisão na etapa de validação humana, de modo que a revogação refere-se ao ato de alterar um consentimento estabelecido e armazenado em nuvem. Esta informação também deve ser registrada em *log*.

Se na situação os dados forem gerados, adquiridos ou manipulados localmente, sem necessidade de conexão com qualquer outro equipamento, segue-se para a etapa da CIA-triad. Do contrário, passa-se para a próxima decisão de validação. É estranho um equipamento de IoT que não se comunica com qualquer outro, mas este cenário também existe na IoT (ex.: monitor de sinais vitais que alerta o usuário sobre possível problemas).

A segunda etapa no âmbito da validação humana consiste na ciência do comparti-

lhamento externo, ou seja, refere-se ao ato de que o usuário tome **ciência da necessidade de compartilhamento de seus dados adquiridos/gerados com agentes externos**. Existem situações em que não há tal necessidade como por exemplo um sistema de apoio ao esportista que monitora sinais vitais. Neste caso o monitoramento é exibido na própria rede pessoal do usuário. Entretanto, há situações em que é necessário o compartilhamento externo. Um mesmo sistema de apoio ao esportista que venha a se comunicar com o médico. Enfim, quando há a necessidade de compartilhamento com qualquer agente externo, convém que o usuário esteja ciente do fato.

A última responsabilidade por parte humana refere-se à **confiabilidade no dispositivo vinculado**, isto é, o destino dos dados consentidos pelo usuário. Caso este seja definido como não confiável, não haverá o fornecimento de dados, ação também registrada em *log* na nuvem.

Confiar é crer que algo é forte o suficiente para cumprir sua função. O termo tem como etimologia o latim *confidare* que significa pôr confiança (HOUAISS; VILLAR; FRANCO, 2009, p. 519). Deste modo, é necessário que além de consentir o uso dos dados privados, o usuário deponha confiança no destino que os receberão. Nenhum dos modelos de segurança elencados tange a confiabilidade no destino, mas apenas na origem e conteúdo da mensagem como ocorre por exemplo com o uso de certificados digitais. A título de complemento deste objetivo, convém de algum modo haver uma memória da decisão associando usuário e dispositivo vinculado. Tal informação pode ser utilizada em decisões futuras de modo que se diversos dispositivos IoT tenham o mesmo destino vinculado, não é necessário um novo voto de confiança.

Em termos de política de segurança o objetivo **confiabilidade no destino vinculado** propõe uma inversão ao objetivo **autenticidade**. A autenticidade fornece uma garantia de que quem originou a mensagem é quem diz sê-lo, cuja autoria é atestada (HOUAISS; VILLAR; FRANCO, 2009, p. 223). Logo, a autenticidade é uma característica que diz respeito à origem da mensagem. Não refere-se ao conteúdo ou ao destino. Considerando que o conteúdo seja tratado através dos objetivos integridade-disponibilidade-confidencialidade, resta um objetivo de segurança em relação ao destinatário da mensagem. A confiabilidade no dispositivo vinculado busca fornecer uma garantia de que o destino da mensagem é quem diz sê-lo e que a origem poderá enviar dados. Deste modo, os objetivos desta abordagem tangem a origem, mensagem e destino (Figura 42).

Por fim, ressalta-se que esta etapa não equivale ao uso de SSL. O SSL promove a confidencialidade e integridade (ambas garantindo a confiabilidade) de dados através da criação de um tunel criptográfico entre um servidor *web* e o *browser* para transmissão dos dados, ao passo que a confiabilidade aqui proposta refere-se à confiança exclusiva no destinatário dos dados, e não nos dados.

Com o objetivo legitimar a etapa de validação humana, tem-se a característica da

auditabilidade. O consentimento de uso de dados bem como a confiança no dispositivo que receberá os dados são recursos eficientes para tratamento da proteção à privacidade. Entretanto, para que estas ações sejam irrefutáveis, convém produzir registros os quais podem servir de monitoramento persistente e assim caracterizar a auditabilidade.

A etimologia da palavra auditabilidade remete ao latim ***auditor*** que significa ouvinte (VIEIRA; MICALES, 2016, p. 53), ou seja, aquela pessoa que no processo de comunicação recebe enunciados (HOUAISS; VILLAR; FRANCO, 2009, p. 1.406). Conforme Houaiss, Villar e Franco (2009, p. 221) a auditoria é o processo de exame de validação. Logo, este processo de exame de validação ocorre embasado nos dados e informações ouvidos do ambiente em questão. Deste modo, o registro das ações humanas, isto é, do consentimento explícito de uso de dados privados, bem como do termo de confiabilidade no destino vinculado, permitirão que o ambiente IoT seja auditável.

4.1.3 Inserção proposta integrada à CIA-triad

A tríade confidencialidade-integridade-disponibilidade tem sua relevância na segurança da informação e conforme observado pela análise histórica após a concepção da CIA-triad, os modelos de segurança corporativos, militares e pesquisa acadêmica, todos possuem esta como base.

Do mesmo modo, a CIA-triad é aplicável à IoT e juntamente com os novos objetivos de segurança aqui adicionados, viabiliza a proteção com ênfase na proteção de dados privados.

i **Confidencialidade**: considerando que por princípio básico esta sendo adotado que todos os dados são privados, é necessário estabelecer uma proteção, uma fronteira entre os dados e o restante do ciberespaço. Deste modo a confidencialidade se torna essencial no processo de proteção à privacidade. Sugere-se estabelecer pelo menos um nível de encriptação a exemplo do protocolo https. Em situações em que o funcionamento em tempo real não seja prioridade, é facultado a adoção do uso de VPN. Apesar do retardo em questão de tempo de acesso, a VPN em si não exige alto poder de processamento e armazenamento o que é exatamente o caso da IoT. A implementação de um túnel pode ser realizado de forma bem simples como sugerido no Apêndice A o qual utiliza-se de uma conexão SSH para estabelecimento do circuito, tendo como requisito apenas que ambas as máquinas (cliente e servidor) possuam o SSH[5] instalado, o que é comum em distribuições *like* Unix como Linux, FreeBSD, entre outros.

[5] Acrônimo de *Secure Shell*. Trata-se de uma ferramenta para acesso à linha de comando remota e protegida por criptografia.

ii **Integridade**: quando se falava em garantia da integridade no ambiente digital, qualquer problema relacionado a esta tinha na pior das hipóteses limitação ao ciberespaço. Uma vez estabelecida a interoperabilidade entre o mundo físico e digital através dos *Cyber Physical Systems*, ações partidas do ciberespaço influenciam fatos ocorridos no mundo real. Deste modo, a integridade digital pode comprometer diretamente a integridade no mundo real. Considerando tal crucialidade, a integridade manteve-se como objetivo final (Figura 40).

iii **Disponibilidade**: conforme observado, a disponibilidade não é a característica mais lembrada quando se fala em segurança da informação. Entretanto é um sustentáculo essencial à segurança. Uma que que a integridade ou confidencialidade são mais dificilmente quebradas, uma vez comprometida a disponibilidade, tal ação pode favorecer consequências no mundo real através da suspensão de serviços ou mesmo fornecimento errôneo de dados para outros sistemas coadjuvantes do ambiente IoT. Com isto, novamente o mundo físico é afetado por ações praticadas no mundo digital. Ressalta-se também que a disponibilidade tem maior importância comparando-se à integridade e disponibilidade pois a IoT precisa da acessibilidade de dados para desenvolver seu objetivo. Diante de tais motivos, a disponibilidade é mantida no modelo ora proposto.

4.2 Como deve ser a aplicação do paradigma

A sugestão de aplicação deste paradigma pode partir da seguinte referência:

> Uma alternativa seria a certificação voluntária sobre a segurança de dispositivos ligados à Internet das Coisas. A estruturação de sistema de certificação baseado na auto-avaliação voluntária, sem a imposição de obrigações legais aos aderentes, teria o potencial de criar cultura de transparência na prestação de informações ao usuário e incentivar a adoção de alto padrão de segurança pela iniciativa privada. (BNDES, 2017, p. 40-41)

À luz do que se descreve nesta citação no que diz respeito à segurança da informação, uma vez aplicado/adotado voluntariamente o direcionamento proposto (Figura 40), todos os dados passam a ser classificados com privados, entretanto, para o usuário do sistema a transparência é consequência dos objetivos de segurança propostos, incentivando a adoção do modelo em todos os equipamentos IoT do ambiente. A não imposição de obrigações legais é fator favorável na adoção do modelo viabilizando a cultura de transparência bem como realçar a importância dos dados privados e para qual destino estão sendo direcionados.

4.2.1 Aplicação teórica

Através dos cenários descritos em seguida, observar-se-á que o modelo pode ser aplicável nos mais diversos segmentos. Contudo espera-se submetê-lo em ambientes de prova de conceito de modo a validar o uso real nos mais diversos ambientes possíveis.

Considere três ambientes distintos:

a. **Casa inteligente**:

- **Funcionalidade IoT**: controle de iluminação e eletrodomésticos com base na presença dos moradores.
- **Tipo de dado capturado pela IoT**: presença humana.
- **Como adquire**: sensores de presença.
- **aplicação do paradigma**:

  i Por padrão de fábrica o equipamento inicia com política restritiva. No primeiro momento o usuário poderá (caso queira), liberar no *firewall* a comunicação com o fabricante para fins de atualização futura, bem como a comunicação com o servidor em nuvem da aplicação IoT caso exista. Neste momento, o usuário pode realizar também o consentimento explícito de uso de seus dados (que é o registro da presença física de pessoas) por parte do equipamento IoT, dados estes que serão classificados como privados.

  ii Em seguida, o equipamento IoT deve solicitar (caso exista) que o usuário ateste sua confiança em um serviço em nuvem, ou um outro sistema IoT que possa se interrelacionar como por exemplo o sistema de monitoramento de outra casa, ou ainda um serviço terceirizado de monitoramento e segurança. O atestamento do usuário deve ser registrado localmente ou em nuvem.

  iii Prover recursos que garantam a confidencialidade de modo que os dados não sejam legíveis se interceptados por terceiros;

  iv Prover recursos que garantam a integridade dos dados adquiridos/gerados, de modo que não possam ser adulterados de forma ilícita;

  v Prover recursos que garantam a disponibilidade dos dados. Conforme mencionado, a falta de disponibilidade pode comprometer todo o sistema. É necessário que se estabeleça recursos alternativos ou contingência.

b. **sistema público de *marketing* inteligente**:

- **Funcionalidade IoT**: faz propaganda em vídeo com base nas preferências do usuário que circula próximo ao equipamento.

- **Tipo de dado capturado pela IoT**: preferências de compra ou procura na Internet, gosto pessoal de uma forma geral.
- **Como adquire**: Aquisição com base em comunicação *bluetooth* ou RFID com dispositivos do usuário, tais como *smartphone*, *wearable*, ou recursos de *biohacking*[6].
- **aplicação do paradigma**:
  - i Por padrão de fábrica o equipamento do usuário (*smartphone, wearable, biohacking device*) funciona com política restritiva. Na primeira proximidade com o equipamento de *marketing* inteligente, o equipamento remoto solicita ao equipamento do usuário que se estabeleça a confiança de vínculo entre ambos, bem como o consentimento do usuário em compartilhar seus dados privados. Se aceito, estas decisões são registradas tanto em base relativa ao usuário, bem como em base relativa ao sistema público. Esta decisão do usuário poderá ser "aproveitada" caso um outro equipamento IoT que se comunique com o mesmo servidor (tido como confiável) faça a requisição.
  - ii Prover recursos que garantam a confidencialidade de modo que se os dados forem interceptados por terceiros, que não sejam legíveis;
  - iii Prover recursos que garantam a integridade dos dados adquiridos/gerados, de modo que não possam ser adulterados de forma ilícita;
  - iv Prover recursos que garantam a disponibilidade dos dados. Como este não é um serviço trivial, a contingência poderia ser a exibição de publicidade no modo tradicional em que não há aquisição de dados do usuário.

4.2.2 Contextualização de usabilidade IoT relativa a uma geladeira inteligente adotando a diretiva proposta

A aplicabilidade à geladeira inteligente proposta através da Figura 1 seria da seguinte forma:

- **Funcionalidade IoT**: monitora os produtos existentes identificando ítens vencidos ou ausentes. Em ambos faz o pedido de reposição. Também confronta informações médicas dos usuários da geladeira com os ingredientes de produtos então presentes na geladeira.
- **Tipo de dado capturado pela IoT**: dados dos produtos (nome, data de validade e ingredientes de composição); dados de saúde dos usuários (nome, produtos alérgios

[6] técnica de melhoria do corpo humano através da implantanção de dispositivos eletrônicos, tais como chips de RFID.

e ingredientes contra indicados). Os dados de saúde podem ser cadastrados pelo próprio usuário ou mediante outra relação de confiança para profissional de saúde.

- **Como adquire**: os dados de produtos (etiqueta comunicável através RFID) são adquiridos por sensor no interior da geladeira. Os dados de saúde dos usuários são adquiridos por acesso à Internet.

- **aplicação do paradigma**:

  i Inicialmente a geladeira funciona com política restrita e por padrão todos os dados adquiridos serão classificados como privados (não há meio termo).

  ii Cada usuário a ser cadastrado na geladeira deve realizar o consentimento explícito para uso de seus dados de saúde ou manter uma lista única sob responsabilidade de uma única pessoa.

  iii Deve ser estabelecida a confiabilidade nos destinos vinculados e que neste caso são o mercado e a base de dados de saúde. Para cada um destes, deve haver um consentimento. Especificamente no caso de saúde, este deve ser concedido por cada usuário.

  iv Todos os consentimentos realizados devem ser armazenados em memória da própria geladeira bem como em base de dados própria do mercado e o sistema de saúde.

  v todo o tráfego de dados deve ser realizado de modo a garantir a CIA-triad: confidencialidade, integridade e disponibilidade de todos os dados.

CONCLUSÃO

Uma vez que esta tese teve por método de pesquisa a análise exploratória em uma área emergente, a pesquisa se limitou à investigação crítica, apontando uma solução à lacuna identificada e que caracteriza-se pela constatação da preocupação da privacidade em quase todos os documentos pesquisados, mas notando-se a falta de um direcionamento efetivo e que possa ser aplicável em qualquer ambiente de IoT. Deste modo, a solução apresentada foi um paradigma (Figura 40) como possível maneira para que "privacidade" e "IoT" convivam sem que a privacidade seja totalmente sucumbida à evolução tecnológica.

A integração entre mundo real e digital que então é proporcionada pela IoT, dá margem aos questionamentos relativos à privacidade e assim incitam os problemas de pesquisa inicialmente propostos nesta tese e que após a análise crítica realizada, foram respondidos (em caráter de objetivo secundário) como segue:

- **Como direcionar a abrangência de documentação?** Em vista da extensa dimensão que a computação alcança, buscou-se uma forma de direcionar esta tese em um contexto mais pontuado. Assim, foi realizado o seccionamento de diretrizes e padrões da Internet de modo a direcionar uma abrangência específica em termos documentais. Como resultado, estabeleceu-se a delimitação ao nível de Política & governança (Figura 41, página 103);

- **Quem determina diretrizes e padrões na Internet?** Foi identificada a estrutura (Figura 4, página 30) através da qual se estabelecem as diretrizes e padrões da Internet. Deste modo, foi possível analisar em fontes oficiais, a situação em termos de documentos produzidos relativos à segurança da informação com direcionamento à IoT e mais especificamente, em termos de privacidade no âmbito de Política & Governança.

- **Qual é o correto uso das terminologias "dado" ou "informação" na IoT?** Uma vez que se propõe uma diretiva de segurança, é fundamental que cada um dos termos envolvidos seja corretamente utilizado. Assim, este estudo incluiu uma breve revisão para justificar a utilização do termo "dado" no contexto de IoT.

- **É possíve determinar um cenário padrão IoT?** Foi realizada uma revisão dos cenário de IoT, elecando formas de composição do ambiente, variedade de protocolos, abrangência e com isto definindo um cenário padrão de IoT aplicável a qualquer segmento (Figura 9, página 43).

- **Existe classificação padrão para IoT?** Foi realizada uma investigação em termos de registro de marcas e patentes. Como resultado observou-se dois fatores importantes: não foram identificados pedidos ou registro de patentes relacionadas à proteção da privacidade em IoT; também constatou-se a ausência de uma classificação mundial específica para padronização de patentes de IoT, com excessão do Japão que possui um projeto de classificação específicou para aquele país.

- **Como se constituiu a CIA-triad?** A CIA-triad é a base dos modelos de referência em segurança da informação. Deste modo, foi realizada uma análise documental de modo a delinear a *timeline* que culmina na tríade confidencialidade-integridade-disponibilidade.

- **Quais são os principais modelos baseados na CIA-triad?** Novos modelos de referência em segurança da informação foram criados posteriormente. Eles basicamente são a CIA-triad somada com novos objetivos de segurança. A análise de cada um destes modelos permitiu elencar os objetivos pertinentes à IoT, e com isto, justificar a necessidade de uma nova abordagem.

- **Existe diferenciação etimológica entre os termos "privacidade" e "confidencialidade"?** A privacidade é um termo frequentemente utilizado na Internet e não equivale à confidencialidade. Esta confusão de termos pode promover erros conceituais na definição de diretivas. Deste modo, este estudo permitiu investigar a etimologia e resgatar o sentido latino dos termos, diferenciando-os para a correta aplicação. Observou-se de forma especial que a privacidade não se refere aos mecanismos de proteção, mas apenas a uma classificação de dados. Já a confidencialidade sugere o mecanismo de proteção bem como o objeto a que se esconder.

- **Quais as diferenças entre "confidencialidade" e "anonimato" como ferramentas de proteção da privacidade?** Realizou-se uma análise que evidencia as diferenças entre confidencialidade e anonimato, demonstrando que ambas as técnicas podem ser utilizadas para proteção da privacidade. Também foram realizados experimentos que demonstram a utilização de tais recursos.

- **Como aplicar o conceito de "privacidade"?** É difícil em um ambiente computacional determinar com precisão o que é e o que não é privado. Conforme analisado, o conceito de privacidade aplica-se primeiramente à vida pessoal, ao que refere-se à pessoa em particular. Deste modo, todos dados que dizem respeito ao indivíduo, podem ser classificados como privados. No âmbito de IoT o conceito passa a ser uma característica relativa de modo que o ponto de vista é o fator que influenciará em tal classificação.

Análise comparativa entre objetivos de segurança dos modelos de referência

Por fim, faz-se uma conclusão justificando respostas aos questionamentos: Por qual razão não usar apenas o tripé da segurança como modelo de segurança para IoT? Ou ainda, por que não aplicar qualquer dos modelos levantadas para uso na IoT? A Tabela 9 apresenta o resumo dos objetivos de segurança identificados em cada um dos modelos citados, justificando o parecer contrário ou favorável em termos de aplicabilidade na IoT.

É importante ressaltar que alguns objetivos tidos como essenciais à IoT, são indicados como não necessários por conta de redundância de objetivos. Esta tabela trás todos os objetivos de uma maneira geral e os objetivos definidos no paradigma, contemplam os casos redundantes.

Tabela 9: Justificativas de parecer contrário ou favorável em termos de aplicabilidade na IoT.

Objetivos de segurança identificados	**Aplicabilidade na IoT**	**Justificativa**
Auditabilidade	SIM	O monitoramento persistente de ações se torna uma trilha de auditoria. Este procedimento é realizado através do registro das permissões concedidas pelo usuário, bem como o consentimento dado aos destinos vinculados. Deste modo, é favorecida a auditabilidade e se reconhecida por órgãos competentes, passa a ter validade jurídica.

– continua

Tabela 9 – continuação

Objetivos de segurança identificados	**Aplicabilidade na IoT**	**Justificativa**
Autenticação	NÃO	Autenticação é um procedimento intrínseco à confidencialidade. Por redundância, não é necessária. Não há sentido lógico em autenticar-se para acessar um conteúdo que não seja protegido, fronteirizado. A autenticação funciona como uma chave de acesso. Logo, se não há fronteira para acesso ao conteúdo, a autenticação é desnecessária. Uma vez que esta tese preza pela proteção dos dados privados, não é concebível incluir a autenticação sem a confidencialidade. Em vista disto, não é necessário um objetivo específico isolado para tal.
Autenticidade	NÃO	Por redundância, o objetivo de autenticidade não é necessário. Considerando que dois equipamentos IoT conversem entre si e ambos utilizem-se do paradigma proposto nesta tese, a autenticidade será garantida através do objetivo de integridade (CIA-triad) de cada lado. Esta decisão também é corroborada pelo fato de que a IoT trabalha em sua grande maioria com dados em tempo real e realizar procedimento de autenticidade a cada momento, isto é, atestar se o dado adquirido/gerado é real a cada momento, torna-se algo dispendioso em termos de processamento e uso de memória, além ainda de promover atraso no envio dos dados.
Confiabilidade	NÃO	Diz respeito à fidedignidade de dados gerados. É uma característica intrínseca da CIA-triad. Uma vez aplicada a CIA-triad, o dado se torna confiável. Não há razão para se ter este objetivo sem a CIA-triad.

– continua

Tabela 9 – continuação

Objetivos de segurança identificados	**Aplicabilidade na IoT**	**Justificativa**
Confiabilidade no destino vinculado	SIM	É o novo objetivo proposto no paradigma e ainda não presente em nenhum dos modelos levantados. É um objetivo essencial, principalmente quando haverá a interação entre equipamentos pessoais de IoT com equipamentos de terceiros ou públicos. Auxiliado pelo objetivo de auditabilidade, todos os consentimentos devem ser registrados.
Confidencialidade	SIM	Considerando que todos os dados são privados é necessário manter a confidencialidade dos mesmos. O paradigma trabalha com a constante de que todos os dados são privados, logo precisam ser confidenciais.
Disponibilidade	SIM	É característica essencial para funcionamento da IoT. A interrupção da disponibilidade é fator que pode afetar de forma considerável o objetivo fim da IoT.
Integridade	SIM	É um fator imprescindível pois dado adulterados no mundo virtual influenciam os resultados no mundo físico.
Não repúdio	NÃO	Diante da confidencialidade já estabelecida como objetivo, não é trivial estabelecer objetivo específico de garantia que a origem é quem diz ser. Esta ação será confirmada com base na CIA-triad que tem como garantia inclusa a integridade e confidencialidade. A geração e armazenamento de chaves para não repúdio em todos os equipamentos IoT pode ser algo inviável para mantença.

– continua

Tabela 9 – continuação

Objetivos de segurança identificados	**Aplicabilidade na IoT**	**Justificativa**
Possessão (controle)	NÃO	A IoT promove a integração entre o mundo físico e virtual, de modo que ações do mundo virtual influenciem no mundo físico. Entretanto, do ponto de vista de política & governança o empoderamento de equipamentos de IoT com certo grau de autonomia não deve ainda ser concedido como um objetivo de segurança, principalmente quando se trata de ambiente crítico. Trabalhos futuros sobre inteligência artificial poderão discutir e explorar melhor este objetivo de segurança.
Privacidade	SIM, mas como princípio básico	Permitir que o usuário controle sempre que possível seus dados pessoais é característica fundamental na IoT. Deste modo a privacidade foi colocada não como um objetivo, mas um princípio básico que será mantido com suporte dos objetivos de segurança.
Responsabilidade	NÃO	Responsabilização é uma ação aplicada a seres humanos. A responsabilização de máquinas não produz resultado lógico, uma vez que não há legislação de penalidades para máquinas, mas apenas pessoas. Deste modo, não faz sentido lógico responsabilizar equipamentos IoT por suas ações. Entretanto, através dos objetivos da CIA-triad e auditabilidade, estes são suficientes para reconhecer origem e destino de requisições IoT.

– continua

Tabela 9 – continuação

Objetivos de segurança identificados	**Aplicabilidade na IoT**	**Justificativa**
Utilidade	NÃO	Equipamentos IoT são por natureza limitados conforme já observado. Deste modo trabalham com quantidade limitada de dados, o que não requer um objetivo de segurança específico de utilidade, corroborado ainda pelo fato de que todos os dados são classificados como privados no direcionamento proposto, isentando classificação de dados.

O paradigma (Figura 40, página 102) tem abrangência para proteção da privacidade de dados na IoT além de observar condições em consonância com iniciativas como o "IoT - Plano de Ação para o Brasil" (BNDES, 2017), *Cyber Physical Systems Education* (STANKOVIC et al., 2016) e também a *General Data Protection Regulation* (SCHULZ; HENNIS-PLASSCHAERT, 2016), (SCHULZ; HENNIS-PLASSCHAERT, 2018), os quais enfatizam a transparência como pilar. Sobretudo, trata-se de um modelo não testado. A validação que é um trabalho futuro, deve ser realizada em laboratório com ambiente controlado, servindo como prova de conceito. Espera-se como trabalho futuro e continuidade da pesquisa, executar tal processo de validação.

A proteção da privacidade favorece tanto pessoas de bem quanto pessoas promotoras de ações ilícitas como o terrorismo. A própria rede *Onion* possui diversas páginas com conteúdos ilícitos os quais não precisam ser citados. Entretanto, a pesquisa acadêmica preza pela evolução de estudos de modo a beneficiar pessoas de bem. É fato que a forma de proteção proposta para IoT não faz discriminação de pessoas. Neste caso, outros tipos de medidas devem ser tomados, como apoio de Leis e a própria IoT com soluções de monitoramento, reconhecimento e previsão de ações maléficas.

Trabalhos Futuros

Há a necessidade de desdobramento do estudo de modo a submeter o exemplo proposto à experimentação para validação prática. Em seguida, parte-se para uma nova etapa que também é viável como trabalho futuro ao que se refere à interpretação por parte da ciência do direito, buscando uma discussão e validação do modelo no contexto judicial, podendo fornecer meios para a responsabilização de ações de pessoas.

Sugere-se como outra possível linha de trabalho futuro desenvolver e propor mé-

todo de associação de usuário dono de dispositivo IoT, um modo que possa minimizar riscos para que outros usuários não assumam a identidade do respectivo dono do dispositivo. Deve-se desenvolver uma proposta levando em consideração as limitações dos dispositivos IoT conforme já descrito.

Por fim, sugere-se a evolução da discussão envolvendo o fator de inteligência artificial. Dentre os objetivos de segurança discutidos, descreveu-se a possessão como não viável para IoT. Este tipo de poder requer uma boa discussão envolvendo a inteligência artificial no contexto de IoT.

REFERÊNCIAS

ABAWAJY, J. H.; HASSAN, M. M. Federated internet of things and cloud computing pervasive patient health monitoring system. *IEEE Communications Magazine*, IEEE, v. 55, n. 1, p. 48–53, 2017. Citado na página 38.

ABDULLAH, I.; RAHMAN, M. M.; ROY, M. C. Detecting sinkhole attacks in wireless sensor network using hop count. *International Journal of Computer Network and Information Security (IJCNIS)*, v. 7, n. 3, p. 50, 2015. Citado na página 97.

ABI. *The Internet of Things Will Drive Wireless Connected Devices to 40.9 Billion in 2020*. ABI Research, 2014. Acesso em 09 de março de 2017". Disponível em: <https:-//www.abiresearch.com/press/the-internet-of-things-will-drive-wireless-connect/>. Citado na página 40.

ABNT. *Conheça a ABNT: Missão, Visão e Valores*. 2017. Acesso em 01 de maio de 2017". Disponível em: <www.abnt.org.br/abnt/missao-visao-e-valores>. Citado na página 36.

AGRAWAL, P.; CHITRANSHI, G. Internet of things for monitoring the environmental parameters. In: IEEE. *Information Technology (InCITe)-The Next Generation IT Summit on the Theme-Internet of Things: Connect your Worlds, International Conference on*. [S.l.], 2016. p. 48–52. Citado na página 38.

AKKERMANS, S. et al. Towards efficient publish-subscribe middleware in the iot with ipv6 multicast. In: IEEE. *Communications (ICC), 2016 IEEE International Conference on*. [S.l.], 2016. p. 1–6. Citado na página 38.

ALENCAR, G. D.; LIMA, M.; FIRMO, A. C. O efeito da conscientização de usuários no meio corporativo no combate à engenharia social e phishing. *IX Simpósio Brasileiro de Sistemas de Informação (SBSI'13)*, p. 254–259, 2013. Citado na página 107.

ALLIANCE, L. *LoRaWAN 101 - A technical introduction*. 2017. Accesso em 01 de dezembro de 2017". Disponível em: <https://www.lora-alliance.org/technology>. Citado na página 40.

ALLISON, J. R. et al. Valuable patents. *Geo. Lj*, HeinOnline, v. 92, p. 435, 2003. Citado na página 52.

ALMEIDA, M. B. Aplicação de ontologias em segurança da informação. *Diretoria da Prodemge*, 2007. Citado na página 63.

ALSEN, D.; PATEL, M.; SHANGKUAN, J. The future of connectivity: Enabling the internet of things. *McKinsey & Company Internet of Things*, 2017. Disponível em `https://www.mckinsey.com/global-themes/internet-of-things/our-insights/the-future-of-connectivity-enabling-the-internet-of-things`. Citado 3 vezes nas páginas 8, 40 e 41.

ANDERSON, J. P. *Computer Security Technology Planning Study. Volume 2*. [S.l.], 1972. 142 p. Disponível em: <http://seclab.cs.ucdavis.edu/projects/history/papers-/ande72.pdf>. Citado na página 58.

ANGELES, P. et al. Automated assessment of symptom severity changes during deep brain stimulation (dbs) therapy for parkinson's disease. In: IEEE. *Rehabilitation Robotics (ICORR), 2017 International Conference on*. [S.l.], 2017. p. 1512–1517. Citado na página 38.

ANJANA, S. et al. An iot based 6lowpan enabled experiment for water management. In: IEEE. *Advanced Networks and Telecommuncations Systems (ANTS), 2015 IEEE International Conference on*. [S.l.], 2015. p. 1–6. Citado na página 38.

ARM. *Arm Platform Security Architecture Overview*. 2017. Disponível em `https://developer.arm.com/products/architecture/platform-security-architecture`. Acesso em 27 de outubro de 2017. Citado na página 98.

ASSUMPÇÃO, F. S.; SANTANA, R. C. G.; SANTOS, P. L. VA da C. Coleta de dados a partir de imagens: considerações sobre a privacidade dos usuários em redes sociais. *Em Questão*, Universidade Federal do Rio Grande do Sul, v. 21, n. 2, 2015. Citado na página 80.

BACON, M. D.; BULL, G. M. Data transmission. *Macdonald*, 1973. Citado na página 37.

BALDINI, G. et al. Security certification and labelling in internet of things. In: IEEE. *Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on*. [S.l.], 2016. p. 627–632. Citado 2 vezes nas páginas 38 e 97.

BAUER, H. et al. Internet of things: Opportunities and challenges for semiconductor companies. *McKinsey & Company Semiconductors*, 2015. Citado 2 vezes nas páginas 40 e 41.

BNDES. *Produto 8: Relatório do Plano de Ação - Iniciativas e Projetos Mobilizadores*. 2017. 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 6 de dezembro de 2017. Citado 4 vezes nas páginas 40, 98, 110 e 120.

BOS, B. *Extensible Markup Language (XML),*. 2016. Disponível em `https://www.w3.org/Style/CSS20/`. Acesso em 30 de junho de 2017. Citado na página 32.

BOSCH. *Bosch is using Industry 4.0 to increase its competitiveness*. 2016. Accesso em 21 de outubro de 2017". Disponível em: <http://www.bosch-presse.de/pressportal/de-/en/bosch-is-using-industry-4-0-to-increase-its-competitiveness-44805.html>. Citado 2 vezes nas páginas 8 e 47.

BOSCH. *Intelligent sensor systems for Industry 4.0*. 2016. Accesso em 21 de outubro de 2017". Disponível em: <http://www.bosch-presse.de/pressportal/de/en-/intelligent-sensor-systems-for-industry-4-0-44893.html>. Citado 2 vezes nas páginas 8 e 48.

BOSCH. *Bosch Smart Home*. 2018. Accesso em 16 de janeiro de 2018". Disponível em: <https://www.bosch-smarthome.com/uk/en/home>. Citado na página 18.

BOSWORTH, S.; KABAY, M. E. *Computer security handbook*. John Wiley & Sons, 2002. Disponível em: <http://www.computersecurityhandbook.com/csh4/chapter5.html>. Citado na página 67.

BRADNER, S.; MANKIN, A. Rfc 1752: The recomendation for the ip next generation protocol. *IETF*, january 1995. Disponível em: <https://www.ietf.org/rfc/rfc1752.txt>. Citado na página 34.

BRASIL. *Constituição da República Federativa do Brasil de 1988* . 1988. Disponível em `http://www.planalto.gov.br/ccivil_03/Constituicao/\Constituicao.htm`. Acesso em 24 de janeiro de 2016. Citado na página 77.

BRASIL. *Lei 10.406 de 10 de janeiro de 2002 - Institui o Código Civil*. 2002. Disponível em `http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm\`. Acesso em 24 de janeiro de 2016. Citado na página 77.

BRASIL. *Lei 12.527 de 18 de novembro de 2011*. 2011. Disponível em `http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm\`. Acesso em 21 de agosto de 2017. Citado na página 77.

BRASIL. *Lei 12.737 de 30 de novembro de 2012*. 2012. Disponível em `http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm\`. Acesso em 21 de agosto de 2017. Citado na página 77.

BRASIL. *Lei nº 12.965 de 23 de abril de 2014*. 2014. Disponível em `http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm`. Acesso em 17 de janeiro de 2017. Citado 4 vezes nas páginas 78, 79, 98 e 106.

BRASIL. *Lei nº 8.771 de 11 de maio de 2016*. 2016. Disponível em `http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8771.htm`. Acesso em 11 de agosto de 2017. Citado na página 78.

BRASIL. *Acesso à Informação, Governo Federal*. 2017. Disponível em `http://www.acessoainformacao.gov.br\`. Acesso em 22 de agosto de 2017. Citado na página 77.

BRAY, T.; PAOLI, J.; SPERBERG-MCQUEEN, C. M. Extensible markup language (xml),. *W3C*, 1998. Disponível em: <https://www.w3.org/TR/1998/REC-xml-19980210>. Citado na página 32.

BREGMAN, A. et al. *The circle*. [S.l.]: Europacorp, 2017. Citado 2 vezes nas páginas 72 e 97.

CERT.BR, E. do. *Cartilha de Segurança para a Internet*. Comitê Gestor da Internet, 2012. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Citado 2 vezes nas páginas 73 e 105.

CERVANTES, C. et al. Um sistema de detecção de ataques sinkhole sobre 6lowpan para internet das coisas. *XIV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais – SBSeg 2014*, 2014. Disponível em: <http://www.lbd-.dcc.ufmg.br/colecoes/sbseg/2014/0012.pdf>. Citado 3 vezes nas páginas 39, 96 e 97.

CETIC. *TIC Domicílios*. 2015. Disponível em `http://data.cetic.br/cetic/explore?idPesquisa=TIC_DOM&idUnidadeAnalise=Usuarios&ano=2015`. Acesso em 30 de agosto de 2017. Citado na página 28.

CETIC. *TIC Domicílios*. 2015. Disponível em `http://data.cetic.br/cetic/explore?idPesquisa=TIC_DOM&idUnidadeAnalise=Domicilios&ano=2015`. Acesso em 30 de junho de 2017". Citado na página 28.

CETIC. *TIC Domicílios*. 2017. Disponível em `http://cetic.br/media/docs/publicacoes/2/TIC_DOM_2016_LivroEletronico.pdf`. Acesso em 18 de junho de 2018. Citado na página 28.

CHANDRAN, S.; CHANDRASEKAR, S.; ELIZABETH, N. E. Konnect: An internet of things (iot) based smart helmet for accident detection and notification. In: IEEE. *India Conference (INDICON), 2016 IEEE Annual*. [S.l.], 2016. p. 1–4. Citado na página 38.

CHERDANTSEVA, Y.; HILTON, J. A reference model of information assurance & security. In: IEEE. *Availability, reliability and security (ares), 2013 eighth international conference on*. 2013. p. 546–555. Disponível em: <http://users.cs.cf.ac.uk/Y.V-.Cherdantseva/RMIAS.pdf>. Citado 8 vezes nas páginas 8, 22, 56, 60, 62, 69, 71 e 105.

CIA. *The World Factbook - Central Intelligence Agency*. 2017. Disponível em `https://www.cia.gov/library/publications/the-world-factbook/rankorder/2153rank.html#it`. Acesso em 30 de agosto de 2017. Citado na página 28.

COLUMBUS, L. Roundup of internet of things forecasts and market estimates, 2016. *Forbes*, november 2016. Disponível em: <https://www.forbes.com/sites/louiscolumbus-/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016-/1e0defad292d>. Citado na página 40.

COMPONENTS, R. *11 Internet of Things (IoT) Protocols You Need to Know About*. 2017. Accesso em 01 de dezembro de 2017". Disponível em: <https://www.rs-online.com-/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about>. Citado na página 40.

COOPER, A. et al. Privacy considerations for internet protocols. *IETF*, july 2013. Disponível em: <https://trac.tools.ietf.org/html/rfc6973>. Citado 2 vezes nas páginas 35 e 94.

CORCORAN, P. M. A privacy framework for the internet of things. In: IEEE. *Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on*. [S.l.], 2016. p. 13–18. Citado 2 vezes nas páginas 21 e 72.

COROS. *Coros Omni smart cycling helmet*. 2018. Accesso em 16 de janeiro de 2018". Disponível em: <https://www.bikeradar.com/road/gear/category/helmets-and-protection/helmet-standard/product/coros-omni-smart-cycling-helmet-51712/>. Citado na página 18.

COSTA, J. A. M. d. *Releitura constitucional no conflito entre os direitos fundamentais na proteção conferida à privacidade e o acesso à informação*. Tese (Doutorado), 2018. Citado 2 vezes nas páginas 20 e 77.

COULOURIS, G. et al. *Sistemas Distribuídos-: Conceitos e Projeto*. [S.l.]: Bookman Editora, 2007. Citado na página 28.

COYNE, J. W. A practical application of commercial-off-the shelf products to the automated information systems security of the nasa johnson space center control center complex. In: DIANE PUBLISHING. *National Computer Security Conference, 1993 (16th) Proceedings: Information Systems Security: User Choices*. [S.l.], 1995. p. 210. Citado na página 60.

DANTAS, M. L. *Segurança da Informação: uma abordagem focada em gestão de riscos*. [S.l.]: Livro Rápido-Elógica, 2011. 150 p. Citado 4 vezes nas páginas 22, 56, 62 e 66.

DARPA. Rfc 791: Internet protocol - protocol specification. *IETF*, september 1981. Disponível em: <https://tools.ietf.org/html/rfc791>. Citado na página 34.

DARPA. Rfc 793: Transmission control protocol. *IETF*, september 1981. Disponível em: <https://tools.ietf.org/html/rfc793>. Citado na página 34.

DAVID. *How to use I2P*. [S.l.]: The Tin Hat, 2017. Disponível em `http://secure.thetinhat.i2p/tutorials/darknets/i2p.html` (acessível somente com I2P *client*), Acesso em 08 de fevereiro de 2017,. Citado na página 90.

DEERING, S.; HINDEN, R. Rfc 2460: Internet protocol, version 6 (ipv6). *IETF*, December 1998. Disponível em: <https://www.ietf.org/rfc/rfc2460.txt>. Citado na página 34.

DEFESA, M. da. *Política Nacional de Defesa, Estratégia Nacional de Defesa*. [S.l.], 2012. 155 p. Citado na página 56.

DELEUZE, G. Post-scriptum sobre las sociedades de control. *Polis. Revista Latinoamericana*, Centro de Investigación Sociedad y Politicas Públicas (CISPO), n. 13, 2006. Citado na página 28.

DERLY, J. *Projeto de Lei 6291/2016*. 2016. Disponível em `http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2113796\`. Acesso em 6 de dezembro de 2017. Citado na página 78.

DOMALYS. *Domalys - Aladin: stay at home longer in healthy condition*. 2018. Accesso em 16 de janeiro de 2018". Disponível em: <https://www.domalys.com/products/aladin>. Citado na página 18.

DRATH, R.; HORCH, A. Industrie 4.0: Hit or hype?[industry forum]. *IEEE industrial electronics magazine*, IEEE, v. 8, n. 2, p. 56–58, 2014. Citado na página 47.

EDACENTRUM. *RoMulus research project: Intelligent sensor systems for Industry 4.0*. 2016. Accesso em 21 de outubro de 2017". Disponível em: <https://www.edacentrum.de-/romulus/node/24>. Citado na página 47.

ELLINGWOOD, J. *How To Set Up an OpenVPN Server on Ubuntu 16.04*. Digital Ocean, 2016. Acesso em 13 de janeiro de 2017. Disponível em: <https://www-.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-ubuntu-16-04?comment=54809>. Citado na página 154.

ETCIO. *IoT Tech spend is expected to grow at 16% and reach USD 253 Billion by 2021*. 2016. Disponível em `http://cio.economictimes.indiatimes.com/news/internet-of-things/global-iot-technology-spend-expected-to-grow-16-pc-to-touch-253-billion\-by-2021-study/53843443`. Acesso em 30 de maio de 2017". Citado na página 40.

ETSI. *About ETSI*. 2017. Disponível em `http://www.etsi.org/about`. Acesso em 16 de maio de 2017". Citado na página 35.

ETSI. *ETSI Internet of Things Standards*. 2017. Disponível em `http://www.etsi.org/standards-search#page=1&search=internetofthings&title=1&etsiNumber=1&content=1&version=0&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2017-07-06&harmonized=0&keyword=privacy&TB=&stdType=&frequency=&mandate=&collection=&sort=1`. Acesso em 6 de julho de 2017. Citado na página 96.

ETSI. *Mobile Communications*. 2017. Disponível em `http://www.etsi.org/technologies-clusters/technologies/mobile`. Acesso em 16 de maio de 2017". Citado 2 vezes nas páginas 33 e 35.

EVANGELISTA, D.; NOGUEIRA, M.; SANTOS, A. Avaliação das técnicas de detecção do ataque sybil na disseminação de conteúdo da internet das coisas. *XV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais – SBSeg 2015*, 2015. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/sbseg/2014/0012.pdf>. Citado na página 94.

EXECUTIVO, P. *Projeto de Lei 5276/2016*. 2016. Disponível em `http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378&ord=1\`. Acesso em 6 de dezembro de 2017. Citado na página 78.

EXECUTIVO, P. *Projeto de Lei 5276/2016 - inteiro teor*. 2016. Disponível em `http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459&filename=PL+5276/2016\`. Acesso em 6 de dezembro de 2017. Citado na página 78.

FACEBOOK. *Facebook - Política de dados*. 2017. Acesso em 08 de janeiro de 2018". Disponível em: <https://pt-br.facebook.com/privacy/explanation>. Citado na página 72.

FARMOBILE. *Farmobile - Your data. Real-time. Anytime.* 2017. Acesso em 16 de janeiro de 2018". Disponível em: <https://www.farmobile.com/product/pucpricing>. Citado na página 18.

FERBER, S. *Industry 4.0 – Germany takes first steps toward the next industrial revolution*. Bosch, 2012. Disponível em: <http://blog.bosch-si.com/categories-/manufacturing/2012/10/industry-4-0-germany-takes-first-steps-toward-the-next-industrial-revolution/>. Citado na página 46.

FIELDING, R. et al. Rfc 2616: Hypertext transfer protocol – http/1.1. *IETF*, June 1999. Disponível em: <https://tools.ietf.org/html/rfc2616>. Citado na página 34.

FOROUZAN, B. A. *Protocolo TCP/IP*. 3. ed. [S.l.]: McGraw-Hill, 2008. 864 p. Citado na página 27.

GALLOWAY, A. R. *Protocol: How control exists after decentralization*. [S.l.]: MIT press, 2004. Citado na página 28.

GAMBAS. *Generic Adaptative Middleware for Behavior-driven Autonomous Services*. 2016. Accesso em 06 de outubro de 2017". Disponível em: <http://www.gambas-ict.eu>. Citado na página 96.

GAO, I. Using the social network internet of things to mitigate public mass shootings. In: IEEE. *Collaboration and Internet Computing (CIC), 2016 IEEE 2nd International Conference on*. [S.l.], 2016. p. 486–489. Citado na página 38.

GE, M.; KIM, D. S. A framework for modeling and assessing security of the internet of things. In: IEEE. *Parallel and Distributed Systems (ICPADS), 2015 IEEE 21st International Conference on*. [S.l.], 2015. p. 776–781. Citado na página 97.

GOOGLE. *Controles de Atividade*. 2017. Accesso em 15 de março de 2018". Disponível em: <https://myaccount.google.com/intro/activitycontrols>. Citado na página 73.

GOOGLE. *Google - Política de Privacidade*. 2017. Accesso em 08 de janeiro de 2018". Disponível em: <https://www.google.com/intl/pt-BR/policies/privacy/>. Citado na página 72.

GORDON, W. T. *Marshall Who?* 2002. Disponível em `https://www.marshallmcluhan.com/biography/`. Acesso em 30 de junho de 2017". Citado na página 27.

GOTOVTSEV, P. M.; DYAKOV, A. V. Biotechnology and internet of things for green smart city application. In: IEEE. *Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on*. [S.l.], 2016. p. 542–546. Citado na página 38.

GUBBI, J. et al. Internet of things (iot): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, Elsevier, v. 29, n. 7, p. 1645–1660, 2013. Citado 2 vezes nas páginas 45 e 46.

GUTIERRES, L. N. M. *O conceito de big data: novos desafios, novas oportunidades*. Dissertação (Mestrado) — Pontifícia Universidade Católica de São Paulo - PUC-SP, Tecnologias da Inteligência e Design Digital - TIDD, 2017. Citado na página 27.

HALIM, N. H. B.; YAAKOB, N. B.; ISA, A. B. A. M. Congestion control mechanism for internet-of-things (iot) paradigm. In: IEEE. *Electronic Design (ICED), 2016 3rd International Conference on*. [S.l.], 2016. p. 337–341. Citado na página 38.

HERMANN, M.; PENTEK, T.; OTTO, B. Design principles for industrie 4.0 scenarios. In: IEEE. *System Sciences (HICSS), 2016 49th Hawaii International Conference on*. [S.l.], 2016. p. 3928–3937. Citado 3 vezes nas páginas 46, 47 e 48.

HERNANDEZ-RAMOS, J. L.; BERNABÉ, J. B.; SKARMETA, A. Army: architecture for a secure and privacy-aware lifecycle of smart objects in the internet of my things. *IEEE Communications Magazine*, IEEE, v. 54, n. 9, p. 28–35, 2016. Citado na página 96.

HOFFMAN, P. *O Tao do IETF: Guia destinado aos novos participantes do Internet Engineering Task Force*. 2013. Acesso em 01 de maio de 2017". Disponível em: <https://www.ietf.org/tao-translated-br.html>. Citado 2 vezes nas páginas 32 e 34.

HOLLNAGEL, E.; WOODS, D. D. *Joint cognitive systems: Foundations of cognitive systems engineering*. [S.l.]: CRC Press, 2005. Citado na página 39.

HOU, J.; HONG, Y.-G.; TANG, X. Transmission of ipv6 packets over plc networks draft-hou-6lo-plc-00. *IETF*, 2017. Disponível em: <https://datatracker.ietf.org/doc-/html/draft-hou-6lo-plc-00>. Citado na página 32.

HOU, L. et al. Internet of things cloud: Architecture and implementation. *IEEE Communications Magazine*, IEEE, v. 54, n. 12, p. 32–39, 2016. Citado 3 vezes nas páginas 11, 38 e 86.

HOUAISS, A.; VILLAR, M. d. S.; FRANCO, F. M. d. M. *Dicionário Houaiss da língua portuguesa*. 1. ed. [S.l.]: Objetiva, 2009. 1986 p. Citado 8 vezes nas páginas 18, 21, 75, 80, 104, 107, 108 e 109.

HU, P. et al. Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things. *IEEE Internet of Things Journal*, IEEE, 2017. Citado na página 38.

I2P. *Projeto Internet Invisível I2P*. [S.l.]: I2P, 2017. Disponível em `https://geti2p.net/pt-br/about/intro`, Acesso em 08 de fevereiro de 2017. Citado na página 90.

I2P. *Tunnel Overview*. [S.l.]: I2P, 2017. Disponível em `https://geti2p.net/pt-br/docs/tunnels/implementation`, Acesso em 08 de fevereiro de 2017. Citado na página 90.

IAB. *Internet Architecture Board*. 2017. Disponível em `https://www.iab.org/about/`. Acesso em 09 de maio de 2017". Citado 2 vezes nas páginas 32 e 35.

IANA. *Internet Assigned Numbers Authority*. 2017. Disponível em `https://www.iana.org/`. Acesso em 08 de maio de 2017". Citado 2 vezes nas páginas 29 e 30.

IANA. *List of Root Servers*. 2017. Disponível em `https://www.iana.org/domains/root/servers`. Acesso em 08 de maio de 2017". Citado na página 30.

ICANN. *Who runs the Internet?* 2013. Disponível em `https://www.icann.org/sites/default/files/assets/governance-2500x1664-21mar13-en.png`. Acesso em 23 de maio de 2017". Citado 2 vezes nas páginas 23 e 31.

ICANN. *Address Supporting Organization*. 2017. Acesso em 08 de maio de 2017". Disponível em: <https://aso.icann.org/>. Citado na página 29.

ICANN. *Internet Corporation for Assigned Names and Numbers*. 2017. Acesso em 08 de maio de 2017". Disponível em: <https://www.icann.org/>. Citado 2 vezes nas páginas 29 e 31.

IDC; INTEL; NATIONS, U. *A Guide to the Internet of Things Infographic*. Intel, 2014. Acesso em 09 de março de 2017". Disponível em: <http://www.intel.in/content-/www/in/en/internet-of-things/infographics/guide-to-iot.html>. Citado na página 40.

IEC. Safety requirements for power electronic converter systems and equipment - part 2: Power electronic converters from 1000 v a.c. or 1500 v d.c. up to 36 kv a.c. or 54 kv d.c. *IEC*, september 2016. Disponível em: <http://www.iec.ch/dyn/www-/f?p=103:30:2320265952345::::FSP_ORG_ID,FSP_LANG_ID:1293,25>. Citado na página 35.

IEC. *About the IEC: vision and mission*. 2017. Disponível em `http://www.iec.ch/about/`. Acesso em 10 de maio de 2017". Citado 2 vezes nas páginas 33 e 35.

IEC. *Internet of Things and related technologies, ISO/IEC JTC 1/SC 41*. 2017. Disponível em `http://www.iec.ch/dyn/www/f?p=103:23:12443893291932::::FSP_ORG_ID,FSP_LANG_ID:20486,25`. Acesso em 6 de julho de 2017. Citado na página 93.

IEEE. Ieee standard for low-rate wireless networks. 2015. Acesso em 01 de maio de 2017". Disponível em: <http://standards.ieee.org/getieee802/download/802.15.4-2015.pdf>. Citado 2 vezes nas páginas 34 e 94.

IEEE. *Local and Metropolitan Area Network Standards*. 2015. Disponível em `http://standards.ieee.org/getieee802/download/802.3-2015.zip`. Acesso em 09 de maio de 2017". Citado 2 vezes nas páginas 32 e 35.

IEEE. *IEEE 802.11^{TM}: Wireless LANs*. 2017. Disponível em `http://standards.ieee.org/about/get/802/802.11.html`. Acesso em 09 de maio de 2017". Citado na página 35.

IEEE. *IEEE 802.15^{TM}: Wireless Personal Area Networks (PANs)*. 2017. Disponível em `http://standards.ieee.org/about/get/802/802.15.html`. Acesso em 09 de maio de 2017". Citado na página 35.

IEEE. *IEEE Mission & Vision*. 2017. Acesso em 02 maio de 2017". Disponível em: <http://www.ieee.org/about/vision_mission.html>. Citado 2 vezes nas páginas 32 e 35.

IESG. *The IESG*. 2017. Disponível em `https://www.ietf.org/iesg/`. Acesso em 09 de maio de 2017". Citado 2 vezes nas páginas 32 e 35.

IETF. *IPv6 over Low power WPAN (6lowpan)*. 2014. Acesso em 01 de maio de 2017". Disponível em: <https://datatracker.ietf.org/wg/6lowpan/about/>. Citado 2 vezes nas páginas 34 e 94.

IETF. *Request for Comments (RFC)*. 2017. Acesso em 01 de maio de 2017". Disponível em: <https://www.ietf.org/rfc.html>. Citado 2 vezes nas páginas 32 e 34.

IETF. *RFC Editor*. 2017. Disponível em `https://www.rfc-editor.org/search/rfc_search_detail.php?title=Internet+of+things&pubstatus%5B%5D=Any&pub_date_type=any`. Acesso em 6 de julho de 2017. Citado na página 94.

INPI, C. de Comunicação Social do. *Classificação - patentes*. 2015. Acesso em 25 de abril de 2017". Disponível em: <http://www.inpi.gov.br/menu-servicos/informacao-/classificacao-patentes>. Citado 2 vezes nas páginas 11 e 50.

INTELLIGENCE, B. *Here's how the Internet of Things will explode by 2020*. Business Insider, 2016. Acesso em 09 de março de 2017". Disponível em: <http://www.businessinsider.com/iot-ecosystem-internet-of-things-forecasts-and-business-opportunities-2016-2>. Citado na página 40.

IPINFO.IO. *ipinfo.io - Hosted Domain Names*. 2017. Accesso em 29 de novembro de 2017". Disponível em: <https://ipinfo.io/8.8.8.8>. Citado na página 154.

IRTF. *Transmission of IPv6 Packets over IEEE 802.15.4 Networks*. 2007. Acesso em 01 de maio de 2017". Disponível em: <https://tools.ietf.org/html/rfc4944>. Citado 2 vezes nas páginas 34 e 94.

IRTF. *Internet Research Task Force*. 2017. Acesso em 01 de maio de 2017". Disponível em: <https://irtf.org/>. Citado na página 34.

ISACA, A. *Introduction to the Business Model for Information Security*. 2009. Disponível em: <http://www.isaca.org/Knowledge-Center/Research/Documents/Introduction-to-the-Business-Model-for-Information-Security_res_Eng_0109.pdf>. Citado 2 vezes nas páginas 8 e 68.

ISLAM, S. R. et al. The internet of things for health care: a comprehensive survey. *IEEE Access*, IEEE, v. 3, p. 678–708, 2015. Citado na página 38.

ISO. *Information technology - Internet of Things Reference Architecture (IoT RA)*. 2016. Acesso em 25 de abril de 2017". Disponível em: <https://www.w3.org/WoT/IG/wiki-/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf>. Citado 4 vezes nas páginas 32, 44, 93 e 94.

ISO. *About ISO*. 2017. Acesso em 01 de maio de 2017". Disponível em: <https://www-.iso.org/about-us.html>. Citado 2 vezes nas páginas 33 e 36.

ISO. *ISO: a global network of national standards bodies*. 2017. Acesso em 01 de maio de 2017". Disponível em: <https://www.iso.org/members.html>. Citado 2 vezes nas páginas 33 e 36.

ISO. *Organizations in Cooperation with ISO*. 2017. Disponível em `https://www.iso.org/organizations-in-cooperation-with-iso.html?f=FULL`. Acesso em 3 de agosto de 2017. Citado na página 36.

ISO, A. N. *IEC 27001:2006: Tecnologia da informação–Técnicas de segurança–Sistemas de gestão de segurança da informação–Requisitos*. [S.l.: s.n.], 2006. 42 p. Citado 2 vezes nas páginas 8 e 66.

ISO, A. N. *IEC 27001:2013: Tecnologia da informação–Técnicas de segurança–Sistemas de gestão de segurança da informação–Requisitos*. [S.l.: s.n.], 2013. 42 p. Citado na página 65.

ISO, A. N. *IEC 27002:2013: Tecnologia da informação Técnicas de segurança Sistemas de gestão da segurança da informação Requisitos*. 2. ed. [S.l.]: Associação Brasileira de Normas Técnicas, 2013. 99 p. Citado 4 vezes nas páginas 32, 36, 56 e 65.

ISOC. *Internet Ecosystem: Naming and addressing, shared global services and operations, and open standards development*. 2014. Disponível em `https://www.internetsociety.org/who-makes-internet-work-internet-ecosystem`. Citado 6 vezes nas páginas 8, 28, 30, 32, 34 e 35.

ISOC. The internet of things: an overview. *Internet Society*, October 2015. Disponível em: <https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151221-en.pdf>. Citado 2 vezes nas páginas 32 e 95.

ISOC. *Internet Society Mission*. 2017. Disponível em `https://www.internetsociety.org/who-we-are/mission`. Acesso em 09 de maio de 2017". Citado 2 vezes nas páginas 32 e 34.

ISO/IEC. *ISO/IEC 15408-1: Information technology Security techniques Evaluation criteria for IT security Part 1: Introduction and general model*. 1. ed. [S.l.]: ISO/IEC, 1999. 62 p. Citado na página 63.

ITAC. *ITAC Members*. 2017. Disponível em `http://www.internetac.org/members`. Acesso em 09 de maio de 2017". Citado 2 vezes nas páginas 33 e 34.

ITAC. *ITAC Mission*. 2017. Disponível em `http://www.internetac.org/`. Acesso em 09 de maio de 2017". Citado na página 33.

ITU. *ITU-T Recommendations*. 2017. Disponível em `http://www.itu.int/en/ITU-T/publications/Pages/recs.aspx`. Acesso em 09 de maio de 2017". Citado 2 vezes nas páginas 32 e 35.

ITU. *ITU-T Recommendations by series*. 2017. Disponível em `https://www.itu.int/itu-t/recommendations/index.aspx?ser=Y`. Acesso em 5 de julho de 2017. Citado na página 93.

ITU. *ITU-T Recommendations G.872 - Architecture of optical transport networks - Series G: Transmission System and media, digital systems and networks*. 2017. Disponível em `https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13086`. Acesso em 4 de julho de 2017". Citado na página 35.

ITU-T. Itu-t recommendation g.801 - digital networks - digital transmission models. *ITU*, 1988. Citado na página 32.

ITU-T. Sensor control networks and related applications in a next generation network environment. *ITU*, 2013. Disponível em: <https://www.itu.int/itu-t/recommendations-/rec.aspx?rec=11912>. Citado na página 32.

ITU-T. Common requirements of the internet of things. *ITU*, 2014. Citado na página 93.

ITU-T. Itu-t recommendation g.9903 - series g: Transmission systems and media, digital systems and networks - narrowband orthogonal frequency division multiplexing power line communication transceivers for g3-plc networks. *ITU*, 2014. Citado na página 32.

JACOBSSON, A.; DAVIDSSON, P. Towards a model of privacy and security for smart homes. In: IEEE. *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on*. [S.l.], 2015. p. 727–732. Citado na página 97.

JANKOWSKI, S. et al. The internet of things: Making sense of the next mega-trend - the third wave of the internet may be the biggest one yet. *Goldman Sachs*, 2014. Citado 2 vezes nas páginas 40 e 46.

JAZDI, N. Cyber physical systems in the context of industry 4.0. In: IEEE. *Automation, Quality and Testing, Robotics, 2014 IEEE International Conference on*. [S.l.], 2014. p. 1–4. Citado 2 vezes nas páginas 46 e 48.

JHA, N. K. et al. A review paper on deep web data extraction using wordnet. *International Research Journal of Engineering and Technology (IRJET)*, IRJET, v. 03, n. 03, p. 1003–1006, 2016. Citado na página 86.

JIMENEZ, J.; TSCHOFENIG, H.; THALER, D. draft-iab-iotsi. *IETF*, november 2016. Disponível em: <https://trac.tools.ietf.org/html/draft-iab-iotsi-workshop-01>. Citado na página 94.

JOHNSTON, S. J.; SCOTT, M.; COX, S. J. Recommendations for securing internet of things devices using commodity hardware. *WF-IoT 2016*, 2016. Citado 2 vezes nas páginas 38 e 97.

JPO, J. P. O. *Establishment of a New Classification regarding IoT (Internet of Things)*. 2017. Acesso em 25 de abril de 2017". Disponível em: <http://www.wipo.int/edocs-/mdocs/classifications/en/ipc_wk_ge_17/ipc_wk_ge_17_item2_3_jpo.pdf>. Citado 4 vezes nas páginas 8, 51, 52 e 53.

KADOW, A. L. D. S. *A importância dos 2 Vs - Velocidade e Variedade - do Big Data em situações de busca da internet: um estudo envolvendo alunos do ensino superior*. Tese (Doutorado) — Pontifícia Universidade Católica de São Paulo - PUC-SP, Tecnologias da Inteligência e Design Digital - TIDD, 2017. Citado na página 28.

KOCHAVI, M.; JORDAN, G. *Dark Net - Episódio 2: Upgrade*. [S.l.]: Showtime, 2016. Citado 2 vezes nas páginas 21 e 72.

KRANENBURG, R. V. A critique of ambient technology and the all-seeing network of rfid. Insitute of Network Cultures, 2008. Citado na página 97.

KRANENBURG, R. V. Internet das coisas: como viver (e o que esperar) num mundo 100% conectado. *Revista IT Management*, v. 1, n. 2, p. 36–41, 2014. Citado 2 vezes nas páginas 21 e 38.

KRUMM, J. *Ubiquitous computing fundamentals*. [S.l.]: CRC Press, 2010. 394 p. Citado 3 vezes nas páginas 8, 45 e 46.

KUROSE, J.; ROSS, K. *Computer Network: A Top-Down Approach*. sixth. [S.l.]: Pearson, 2013. Citado 5 vezes nas páginas 9, 31, 81, 82 e 83.

LASI, H. et al. Industry 4.0. *Business & Information Systems Engineering*, Springer, v. 6, n. 4, p. 239–242, 2014. Citado na página 46.

LATHAM, D. C. Department of defense trusted computer system evaluation criteria. *Department of Defense*, 1985. Citado 2 vezes nas páginas 59 e 60.

LAUDON, K. C.; LAUDON, J. P. *Sistemas de informação gerenciais*. 7. ed. [S.l.: s.n.], 2007. Citado na página 37.

LEE, H.; KOBSA, A. Understanding user privacy in internet of things environments. *Internet of Things (WF-IoT)*, 2016. Citado 2 vezes nas páginas 76 e 105.

LEE, S.; JEONG, J. P.; PARK, J.-S. Dnsna: Dns name autoconfiguration for internet of things devices. In: IEEE. *Advanced Communication Technology (ICACT), 2016 18th International Conference on*. [S.l.], 2016. p. 410–416. Citado na página 38.

LEVITT, T. Internet of things - iot governance, privacy and security issues - european research cluster on internet of things. 2015. Citado 5 vezes nas páginas 22, 40, 46, 87 e 96.

LEXINNOVA. *Internet of Things: Patent Landscape Analysis*. 2014. Disponível em `www.wipo.int/edocs/plrdocs/en/internet_of_things.pdf`. Acesso em 23 de maio de 2017". Citado 2 vezes nas páginas 40 e 52.

LEXINNOVA. *Internet of Things: 2016, Patents and Perspectives*. 2016. Disponível em `http://www.lex-innova.com/resources-reports/?id=73`. Acesso em 23 de maio de 2017". Citado 3 vezes nas páginas 8, 52 e 53.

LUCERO, S. Iot platforms: enabling the internet of things - whitepaper. *IHS Technology*, march 2016. Disponível em: <https://cdn.ihs.com/www/pdf/enabling-IOT.pdf>. Citado 4 vezes nas páginas 21, 38, 39 e 46.

MACHADO JR, D. M. *Funcionamento interno de um firewall*. 1. ed. [S.l.]: Novas Edições Acadêmicas, 2015. 113 p. Citado 3 vezes nas páginas 44, 105 e 146.

MACONACHY, W. V. et al. A model for information assurance: An integrated approach. In: NEW YORK, USA. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*. [S.l.], 2001. v. 310. Citado 3 vezes nas páginas 8, 66 e 69.

MANDLER, B. *Collaborative Open Market to Place Objects at your Service*. 2015. Accesso em 06 de outubro de 2017". Disponível em: <http://www.compose-project.eu>. Citado na página 96.

MARCIANO, J. L.; LIMA-MARQUES, M. O enfoque social da segurança da informação. *Ci. Inf., Brasília*, SciELO Brasil, v. 35, n. 3, p. 89–98, 2006. Citado na página 107.

MCCUMBER, J. Information systems security: A comprehensive model. In: *Proceedings of the 14th National Computer Security Conference*. [S.l.: s.n.], 1991. Citado 4 vezes nas páginas 8, 63, 65 e 69.

MCLUHAN, M. *Os meios de comunicação como extensões do homem (understanding media)*. [S.l.]: Editora Cultrix, 1964. Citado 3 vezes nas páginas 27, 46 e 99.

MEDICINE, T. N. A. of S. E. *The National Academies of Sciences, Engineering, and Medicine - Who whe are*. 2017. Accesso em 22 de outubro de 2017". Disponível em: <http://www.nationalacademies.org/about/whoweare/index.html>. Citado na página 49.

MG, C. G. do Estado de. *Portal da Transparência do Estado de Minas Gerais*. 2017. Disponível em `http://www.transparencia.mg.gov.br\`. Acesso em 22 de agosto de 2017. Citado na página 77.

MONTEIRO, E.; BOAVIDA, F. *Engenharia de Redes Informáticas*. 10. ed. [S.l.]: FCA-Editora Informática, 2011. 540 p. Citado 3 vezes nas páginas 32, 34 e 36.

NACIONAL, I. Publicação de atos normativos. *Diário Oficial da União - Seção 1*, n. 94, maio 2012. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index-.jsp?jornal=1pagina=2data=16/05/2012>. Citado na página 77.

NAKAMURA, E. T.; GEUS, P. L. *Segurança de redes em ambientes cooperativos*. [S.l.]: Novatec, 2007. 482 p. Citado na página 55.

NASA. *Mission Operations Directorate Automated Information Systems Security Manual, JSC 23982*. [S.l.], 1990. Citado na página 60.

NAWIR, M. et al. Internet of things (iot): Taxonomy of security attacks. In: IEEE. *Electronic Design (ICED), 2016 3rd International Conference on*. [S.l.], 2016. p. 321–326. Citado na página 38.

NEISSE, R. et al. A model-based security toolkit for the internet of things. In: IEEE. *Availability, Reliability and Security (ARES), 2014 Ninth International Conference on*. [S.l.], 2014. p. 78–87. Citado na página 97.

NETCRAFT. *January 2017 Web Server Survey*. netcracft, 2017. Acesso em 21 de março de 2017". Disponível em: <https://news.netcraft.com/archives/2017/01/12/january-2017-web-server-survey.html>. Citado na página 146.

NIC.BR. *Atividades*. 2017. Acesso em 08 de maio de 2017". Disponível em: <https://www.nic.br/atividades/>. Citado na página 30.

NIC.BR. *Simet Box*. 2017. Accesso em 29 de novembro de 2017". Disponível em: <https://simet.nic.br/simetbox.html>. Citado na página 154.

NIC.BR. *Sobre o Registro.br*. [S.l.]: Nic.br, 2017. Disponível em `https://registro.br/sobre/`, Acesso em June, 06, 2017. Citado na página 31.

NIC.BR. *Tráfego Total*. [S.l.]: Nic.br, 2017. Disponível em `https://ix.br`, acesso em 28 de novembro de 2017. Citado 4 vezes nas páginas 9, 31, 154 e 156.

NIEMINEN, J. et al. Rfc 7668: Ipv6 over bluetooth(r) low energy. *IETF*, october 2015. Disponível em: <https://tools.ietf.org/html/rfc7668>. Citado na página 32.

NING, H.; LIU, H. Cyber-physical-social based security architecture for future internet of things. *Advances in Internet of Things*, Scientific Research Publishing, v. 2, n. 01, p. 1, 2012. Citado na página 49.

NING, H. et al. Cybermatics: Cyber–physical–social–thinking hyperspace based science and technology. *Future Generation Computer Systems*, Elsevier, v. 56, p. 504–522, 2016. Citado na página 48.

NRO. *Number Resource Organization*. 2017. Acesso em 08 de maio de 2017". Disponível em: <https://www.nro.net/>. Citado na página 29.

O'BRIEN, J. A. *Sistemas de informação e as decisões gerenciais na era da internet*. 3. ed. [S.l.]: Saraiva, 2011. Citado na página 36.

OECD. *Internet Access*. 2015. Disponível em `https://data.oecd.org/ict/internet-access.htm`. Acesso em 30 de junho de 2017". Citado 2 vezes nas páginas 11 e 29.

OECD. *About the OECD*. 2017. Disponível em `https://www.oecd.org/about/`. Acesso em 09 de maio de 2017". Citado 2 vezes nas páginas 32 e 33.

OECD. *Country statistical profile: Brazil 2017/2*. 2017. Disponível em `http://dx.doi.org/10.1787/csp-bra-table-2017-2-en`. Acesso em 11 de maio de 2017". Citado na página 33.

OECD. *OECD Data: Brazil*. 2017. Disponível em `https://data.oecd.org/brazil.htm`. Acesso em 11 de maio de 2017". Citado 2 vezes nas páginas 32 e 33.

OLIVEIRA, J. F. d. *Sistemas de informação: um enfoque gerencial inserido no contexto empresarial e tecnológico*. 9. ed. [S.l.: s.n.], 2004. 166–173 p. Citado na página 37.

OPENIOT. *Open Source cloud solution for the Internet of Things*. 2016. Accesso em 06 de outubro de 2017". Disponível em: <http://www.openiot.eu>. Citado na página 96.

OTA. *Online Trust Alliance, an Internet Society initiative*. OTA, 2017, 2014. Disponível em: <https://www.internetsociety.org/blog/institutional/2017/04/reaching-next-level-online-trust>. Citado na página 95.

OTA. *IoT Vision*. OTA, 2017, 2017. Disponível em: <https://otalliance.org/initiatives-/internet-things>. Citado na página 95.

OTA. *Securing the Internet of Things - A Collaborative & Shared Responsability*. OTA, 2017, 2017. Disponível em: <https://otalliance.org/system/files/files/resource-/documents/iot_sharedroles.pdf>. Citado 2 vezes nas páginas 95 e 107.

PAESANI, L. M. *Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil*. 4. ed. [S.l.]: Editora Atlas, 2008. Citado 2 vezes nas páginas 21 e 72.

PANASONIC. *Panasonic Home Monitoring & Control Kit*. 2018. Accesso em 16 de janeiro de 2018". Disponível em: <https://www.panasonic.com/uk/consumer/smart-home/kx-hn6012ew.html>. Citado na página 18.

PARKER, D. B. *Fighting Computer Crime: A new framework for protecting information*. [S.l.]: Wiley, 1998. 528 p. Citado 3 vezes nas páginas 8, 67 e 70.

PENTLAND, A. S. With big data comes big responsability. *Harvard Business Review*, november 2014. Disponível em: <https://hbr.org/2014/11/with-big-data-comes-big-responsibility>. Citado na página 97.

PISHVA, D. Internet of things: Security and privacy issues and possible solution. In: IEEE. *Advanced Communication Technology (ICACT), 2017 19th International Conference on*. [S.l.], 2017. p. 797–808. Citado na página 96.

POLLONI, E. G. F. *Administrando sistemas de informação: estudo de viabilidade*. [S.l.]: Futura, 2000. Citado na página 37.

POSTEL, J. Rfc 768: User datagram protocol. *IETF*, August 1980. Disponível em: <https://tools.ietf.org/html/rfc768>. Citado na página 34.

POSTEL, J. Rfc 792: Internet control message protocol. *IETF*, september 1981. Disponível em: <https://tools.ietf.org/html/rfc792>. Citado na página 34.

PWC. *The Global State of Information Security - Survey*. 2018. Disponível em `https://www.pwc.com/us/en/cybersecurity/information-security-survey.html`. Acesso em 24 de abril de 2018. Citado na página 22.

QI, J. et al. Detection and defence of sinkhole attack in wireless sensor network. In: IEEE. *Communication Technology (ICCT), 2012 IEEE 14th International Conference on*. [S.l.], 2012. p. 809–813. Citado na página 96.

RAGGETT, D.; ASHIMURA, K.; CHEN, Y. White paper for the web of things. *W3C*, W3C, 2016. Disponível em: <http://w3c.github.io/wot/charters/wot-white-paper-2016-.html>. Citado 2 vezes nas páginas 32 e 96.

RAJPUT, D. S.; GOUR, R. An iot framework for healthcare monitoring systems. *International Journal of Computer Science and Information Security*, LJS Publishing, v. 14, n. 5, p. 451, 2016. Citado na página 38.

RAMOS, C. M. O direito fundamental à intimidade e à vida privada. *Revista de Direito da Unigranrio*, 2008. Disponível em: <http://publicacoes.unigranrio.edu.br/index.php-/rdugr/article/view/195>. Citado 2 vezes nas páginas 20 e 77.

RAND. *History and Mission*. 2016. Disponível em: <http://www.rand.org/about-/history.html>. Citado na página 56.

RANSBOTHAM, S.; MITRA, S. Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research*, INFORMS, v. 20, n. 1, p. 121–139, 2009. Citado 2 vezes nas páginas 8 e 69.

RERUM. *RERUM: REliable, Resilient and secUre IoT for sMart city applications*. 2013. Accesso em 06 de outubro de 2017". Disponível em: <https://ict-rerum.eu>. Citado na página 96.

RIR nro. *Global Internet Resources Administration*. 2017. Acesso em 08 de maio de 2017". Disponível em: <https://www.nro.net/about-the-nro/regional-internet-registries/>. Citado na página 30.

ROCHA, P. C. C. Segurança da informação–uma questão não apenas tecnológica. *Monografia de Conclusão de Curso (Especialização)-Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília, Brasília, Brasil*, 2008. Citado na página 107.

ROOS, S. et al. Measuring freenet in the wild: Censorship-resilience under observation. In: SPRINGER. *International Symposium on Privacy Enhancing Technologies Symposium*. [S.l.], 2014. p. 263–282. Citado na página 91.

SALTZER, J. H.; SCHROEDER, M. D. The protection of information in computer systems. *Proceedings of the IEEE*, IEEE, v. 63, n. 9, p. 1278–1308, 1975. Citado 2 vezes nas páginas 59 e 68.

SAMONAS, S.; COSS, D. The cia strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, v. 10, n. 3, p. 21–45, 2014. Citado 3 vezes nas páginas 56, 58 e 59.

SAMSUNG. *Samsung Family Hub - Home has a new hub*. 2017. Accesso em 09 de janeiro de 2018". Disponível em: <https://www.samsung.com/us/explore/family-hub-refrigerator/connected-hub/>. Citado na página 18.

SAMSUNG. *Samsung Whole Home Wi-Fi*. 2018. Accesso em 16 de janeiro de 2018". Disponível em: <https://www.samsung.com/us/smart-home/>. Citado na página 18.

SANTOS, G. A. D. et al. Internet of things (iot): Um cenário guiado por patentes industriais. *GESTÃO. Org: Revista Eletrônica de Gestão Organizacional*, v. 13, 2015. Citado 2 vezes nas páginas 50 e 51.

SASSE, M. A.; BROSTOFF, S.; WEIRICH, D. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal*, Springer, v. 19, n. 3, p. 122–131, 2001. Citado na página 107.

SCHULZ, M.; HENNIS-PLASSCHAERT, J. Regulamento (ue) 2016/679 do parlamento europeu e do conselho de 27 de abril de 2016. *Jornal Oficial da União Europeia*, 2016. Disponível em `https://publications.europa.eu/pt/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-pt`, acesso em 11 de dezembro de 2017. Citado 2 vezes nas páginas 107 e 120.

SCHULZ, M.; HENNIS-PLASSCHAERT, J. *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*. 2018. Disponível em `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679`. Acesso em 21 de junho de 2018. Citado 2 vezes nas páginas 107 e 120.

SCHURGOT, M. R.; SHINBERG, D. A.; GREENWALD, L. G. Experiments with security and privacy in iot networks. In: IEEE. *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015 IEEE 16th International Symposium on a*. [S.l.], 2015. p. 1–6. Citado na página 97.

SEHGAL, V. K.; MEHROTRA, S.; MARWAH, H. Car security using internet of things. In: IEEE. *Power Electronics, Intelligent Control and Energy Systems (ICPEICES), IEEE International Conference on*. [S.l.], 2016. p. 1–5. Citado na página 38.

SENGUL, C. Privacy, consent and authorization in iot. In: IEEE. *Innovations in Clouds, Internet and Networks (ICIN), 2017 20th Conference on*. [S.l.], 2017. p. 319–321. Citado 6 vezes nas páginas 8, 22, 43, 44, 46 e 97.

SHAFIEI, H. et al. Detection and mitigation of sinkhole attacks in wireless sensor networks. *Journal of Computer and System Sciences*, Elsevier, v. 80, n. 3, p. 644–653, 2014. Citado na página 97.

SILVA, C. da S.; SARINHO, V. T. Openserum–um sistema aberto de monitoramento de soro hospitalar. *Journal of Health Informatics*, v. 8, n. 2, 2016. Citado na página 38.

SILVEIRA, S. A. da. Economia da intrusão e modulação na internet. *Pesquisa Brasileira em Ciência da Informação e Biblioteconomia*, v. 11, n. 2, 2016. Citado na página 28.

SMARTPARKING. *Smart Parking Limited - A global parking business*. 2018. Accesso em 16 de janeiro de 2018". Disponível em: <https://www.smartparking.com>. Citado na página 18.

SOUMYA, S. et al. Internet of things based home automation system. In: IEEE. *Recent Trends in Electronics, Information & Communication Technology (RTEICT), IEEE International Conference on*. [S.l.], 2016. p. 848–850. Citado na página 38.

SP, E. de. *Governo do Estado de São Paulo, Portal da Transparência Estadual*. 2017. Disponível em `http://www.transparencia.sp.gov.br\`. Acesso em 22 de agosto de 2017. Citado na página 77.

STAIR, R. M.; REYNOLDS, G. W. *Principios de sistemas de informação: uma abordagem gerencial*. 4. ed. [S.l.]: LTC Editora, 2000. Citado na página 37.

STALLINGS, W. *Criptografia e segurança de redes: Princípios e práticas*. 4. ed. [S.l.]: Pearson, 2008. 693 p. Citado na página 62.

STALLINGS, W. *Business data communications*. 6. ed. [S.l.]: Prentice Hall PTR, 2009. Citado na página 28.

STANKOVIC, J. A. et al. *A 21st Century Cyber-Physical Systems Education*. 1. ed. Washington DC: The National Academies Press, 2016. Citado 4 vezes nas páginas 48, 49, 50 e 120.

STATS, I. L. *Internet users in the world*. 2016. Disponível em `http://www.internetlivestats.com/internet-users/`. Acesso em 05 de junho de 2016. Citado na página 20.

STOUT, W. M.; URIAS, V. E. Challenges to securing the internet of things. In: IEEE. *Security Technology (ICCST), 2016 IEEE International Carnahan Conference on*. [S.l.], 2016. p. 1–8. Citado 2 vezes nas páginas 38 e 96.

SULLIVAN, A. *Iab Status Pages*. 2017. Disponível em `https://trac.tools.ietf.org/group/iab/`. Acesso em 6 de julho de 2017. Citado na página 94.

SYMANTEC. *DoS (denial-of-service) attack (ataque de DoS(negação de serviço)*. 2016. Disponível em `https://www.symantec.com/pt/br/security_response/glossary/define.jsp?letter=d&word=dos-denial-of-service-attack\`. Acesso em 29 de setembro de 2016. Citado na página 63.

TEIXEIRA, F. A. et al. Siot–defendendo a internet das coisas contra exploits. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, 2014. Citado na página 97.

TONG, C. K.; WONG, E. T. *Governance of Picture Archiving and Communications Systems: Data Security and Quality Management of Filmless Radiology: Data Security and Quality Management of Filmless Radiology*. [S.l.]: IGI Global, 2008. 366 p. Citado na página 64.

TOR, P. *Tor: overview*. 2017. Disponível em `https://www.torproject.org/about/overview.html.en`, Acesso em 06 de janeiro de 2017. Citado 2 vezes nas páginas 9 e 87.

TORMETRICS. *Servers*. 2017. Disponível em `https://metrics.torproject.org/relayflags.html`, Acesso em 11 de janeiro de 2017. Citado 3 vezes nas páginas 9, 88 e 90.

TSCHOFENIG, H. et al. Rfc 7452: Architectural considerations in smart object networking. *IETF*, march 2015. Acesso em 08 de setembro de 2017. Disponível em: <https://www.ietf.org/rfc/rfc7452.txt>. Citado na página 42.

TSCHOFENIG, H.; FARRELL, S. Report from the internet of things (iot) semantic interoperability (iotsi) workshop 2016 draft-iab-iotsi-workshop-01.txt. *IETF*, february 2017. Disponível em: <https://trac.tools.ietf.org/html/draft-iab-iotsu-workshop-01>. Citado na página 94.

TURNER, W. P. et al. Tier classifications define site infrastructure performance. *Uptime Institute*, 2015. Disponível em: <http://pueda.tep-energy.ch/wp-content/uploads/2015-/08/Uptime_Institute_Data_Center_Tier_Classification_5th.pdf>. Citado na página 32.

UNCHARTED. *Tor Flow*. 2016. Accesso em 30 de outubro de 2017". Disponível em: <http://torflow.uncharted.software>. Citado na página 89.

UNION, E. *Frequently Asked Questions about the incoming GDPR*. 2016. Disponível em `https://www.eugdpr.org/gdpr-faqs.html`, acesso em 11 de dezembro de 2017. Citado na página 107.

VERAS, M. *Computação em nuvem: nova arquitetura da TI*. [S.l.]: Brasport, 2015. Versão digital Kindle. Citado 2 vezes nas páginas 32 e 63.

VIEIRA, J. L.; MICALES, M. L. V. *Dicionário Latim-Português*. 1. ed. [S.l.]: Editora Edipro, 2016. Citado 4 vezes nas páginas 75, 104, 107 e 109.

W3C. *W3C HTML*. 2017. Disponível em `https://www.w3.org/html/`. Acesso em 09 de maio de 2017". Citado na página 34.

W3C. *Web of Things Working Group*. 2017. Acesso em 27 de abril de 2017". Disponível em: <https://www.w3.org/WoT/WG/>. Citado na página 95.

W3C. *What does W3C do?* 2017. Acesso em 01 de maio de 2017". Disponível em: <https://www.w3.org/Help/activity>. Citado 2 vezes nas páginas 32 e 34.

W3TECHS. *Usage of web servers for websites*. w3techs, 2017. Acesso em 21 de março de 2017". Disponível em: <https://w3techs.com/technologies/overview/web_server/all>. Citado na página 146.

WARE, W. H. *Security controls for computer systems. report of defense science board task force on computer security*. [S.l.], 1979. Disponível em: <http://www.rand.org-/pubs/reports/R609-1/index2.html>. Citado na página 58.

WEBER, P. et al. Ipv6 over lorawan™. In: IEEE. *Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), 2016 3rd International Symposium on*. [S.l.], 2016. p. 75–79. Citado na página 38.

WEINRIB, A.; POSTEL, J. Irtf research group guidelines and procedures. *IETF*, october 1996. Disponível em: <https://tools.ietf.org/html/rfc2014>. Citado na página 34.

WHITE, C. M. *Redes de computadores e comunicação de dados*. 6. ed. [S.l.]: Cengage Learn, 2012. Citado na página 28.

WHITMAN, M. E.; MATTORD, H. J. *Principles of Information Security*. 5. ed. [S.l.]: Cengage Learn, 2015. 656 p. Citado 3 vezes nas páginas 22, 56 e 62.

WIPO. *Patentscope: Search International and National Patent Collections*. 2017. Disponível em `https://patentscope.wipo.int/search/en/result.jsf`. Acesso em 16 de maio de 2017". Citado 3 vezes nas páginas 8, 51 e 52.

WRIGHT, J. *How Tor Works: Part One*. 2015. Disponível em `http://jordan-wright.com/blog/2015/02/28/how-tor-works-part-one/`, Acesso em 11 de janeiro de 2017. Citado na página 88.

WTO. *The WTO*. 2017. Disponível em `https://www.wto.org/english/thewto_e/thewto_e.htm`. Acesso em 09 de maio de 2017". Citado 2 vezes nas páginas 32 e 33.

WTO. *The WTO and the Organization for Economic Cooperation and Development (OECD)*. 2017. Disponível em `https://www.wto.org/english/thewto_e/coher_e/wto_oecd_e.htm`. Acesso em 09 de maio de 2017". Citado na página 33.

YEMBRICK, J. *NASA Extends the World Wide Web Out Into Space*. [S.l.], 2010. Disponível em `https://www.nasa.gov/home/hqnews/2010/jan/HQ_M10-011_Hawaii221169.html`, Acesso em December, 10, 2015. Citado na página 55.

Apêndices

APÊNDICE A – Script para estabelecimento de tunel SSH

```
1  #!/bin/bash
2  #---------------------------------------------
3  # script para estabelecimento de tunel SSH
4  # Dorival M Machado Junior
5  #---------------------------------------------
6
7  #--| variaveis do script |-----
8  portaOrigem=60666
9  ipOrigem=127.0.0.1
10
11 portaDestino=3306
12 ipDestino=70.0.0.254
13
14 usuarioRemotoSSH=madruga
15 #------------------------------
16
17 echo ""
18 echo "Parametros do tunel:"
19 echo ""
20 echo " +----------------+ +--------------+"
21 echo " |Entrada do tunel| |Saida do tunel|"
22 echo " +----------------+ +--------------+"
23 echo " (host local) (host remota)"
24 echo ""
25 echo " $ipOrigem:$portaOrigem >===>===>===>===>===>===> $ipDestino: $portaDestino"
26 echo " ip porta ip porta"
27 echo ""
28 echo ""
29 echo "Uma vez estabelecido, basta pressionar <CTRL> + C para fechar o tunel"
30 echo ""
31 echo "Estabelecendo Tunel SSH, aguarde:"
32 ssh -N -L $portaOrigem:$ipOrigem:$portaDestino $usuarioRemotoSSH@$ipDestino
```

APÊNDICE B – Script utilizado para comparação de conexões dentro e fora do tunel VPN

```
#!/bin/bash
#-----------------------------------------------
# Script comparativo de dois arquivos de ping
# versao 1.0
# Autor: Dorival M Machado Junior ( dorivaljunior at gmail com )
#-----------------------------------------------

filePing1="p1.txt"
filePing2="p2.txt"
serverTest="8.8.8.8"
packetsForSend="70"
comparisonGraph="p1_p2-`date | awk '{print $4}'`.png"
defaultUser="djunior"


#---{begin}------

echo "Lets begin: $comparisonGraph"
echo "Starting ping without VPN ($packetsForSend packets), wait..."
ping -c $packetsForSend $serverTest > $filePing1
cat $filePing1 | awk '{print $7}' | cut -d'=' -f2 | egrep [0-9] > /tmp/p1p.txt

echo "Please, open another terminal and start the VPN tunel:"
echo "type: openvpn --config /root/openvpn/client1.ovpn &"
echo -n "Press <ENTER> to continue..."
read

echo "Starting ping with VPN ($packetsForSend packets), wait..."
ping -c $packetsForSend $serverTest > $filePing2
cat $filePing2 | awk '{print $7}' | cut -d'=' -f2 | egrep [0-9] > /tmp/p2p.txt

echo "Plotting graph..."
echo "
set terminal png
set ylabel 'Tempo (milisegundos)'
set xlabel 'Sequência de pacotes enviados'
set size 1.0,1.0
set output '$comparisonGraph'
plot 1 notitle,\
'/tmp/p1p.txt' title 'ping para 8.8.8.8 sem VPN' with linespoints lc 1, \
'/tmp/p2p.txt' title 'ping para 8.8.8.8 com VPN' with linespoints lc 2" | gnuplot ;

echo "File created: $comparisonGraph"

echo "Moving to /home/$defaultUser"
mv $comparisonGraph /home/$defaultUser

chown $defaultUser: /home/$defaultUser/$comparisonGraph
```

APÊNDICE C – Script para bloqueio de acessos originados da rede Tor

```
#!/bin/bash
#-----------------------------------------------------
# script blocker Tor exit relays blocker
# version: 5.0
# execution: every 12 hours
# author: Dorival M Machado Junior  (dorivaljunior at gmail com)
#-----------------------------------------------------

#----[environment variables]-------
logFile="/var/log/tor_relays.log"
file_tor_blacklist="/var/log/tor_blacklist.txt"
regTime=$(date | tr -s [:blank:] _)
#---------------------------------

removeBlacklist()
{
        # removing last blacklist
        testIptables=$(iptables -n -L -v | grep DROP | grep `head -1 $file_tor_blacklist` | awk '{print $8}' | sort -u)
        if [ -s $file_tor_blacklist -a -n $testIptables ]; then
                blacklist=$(cat $file_tor_blacklist)
                for x in $blacklist; do
                        echo "removendo bloqueio de $x" >> $logFile
                        iptables -D INPUT -s $x -j DROP
                        iptables -D FORWARD -s $x -j DROP
                done
        fi
}

#---------[begin]-------------
if [ -z $1 ]; then
        echo "Sintaxe: $0 <acao>"
        echo ""
        echo "Acao: \"remove\" limpa regras de bloqueio anterior (se existente)"
        echo "      \"aplica\" atualiza relays TOR e faz bloqueio"
        exit 0
fi

case $1 in
        remove)
                removeBlacklist
                exit 0
        ;;
        aplica)
                removeBlacklist
        ;;
        *)
                echo "Opcao inexistente."
                exit 0
        ;;
esac

#identifying relays with access to my IP
torExitRelays=$(links -dump https://check.torproject.org/cgi-bin/TorBulkExitList.py?ip=$(links -dump ip.dnsexit.com | sed 's/ //g') | sed 's/ /\n/g' | sed -n '/^[0-9].*\..*\..*\./p' | sed -n '2    ,$p')

#identifying my IP
thisHost=$(links -dump ip.dnsexit.com | awk '{print $1}')

echo "$regTime : bloqueando Tor Exit Relays das ultimas 16 horas com acessibilidade a este host (IP: $thisHost)" >> $logFile

#creating iptables rules to deny Tor relays
for i in $torExitRelays; do
        echo "$regTime bloqueando $i (TOR relay) para $thisHost" >> $logFile
        iptables -I INPUT -s $i -j DROP
        iptables -I FORWARD -s $i -j DROP
done

#registering current IP's Tor exit relays
echo "$torExitRelays" > $file_tor_blacklist
```

APÊNDICE D – Prova de conceito do script de bloqueio da rede Tor

Para realizar o bloqueio à rede Tor foi utilizado o *shell script* do Apêndice C. O código é uma sugestão de implementação para bloqueio de acessos originados da rede Tor. Seu funcionamento consiste em identificar o IP do *host* (neste caso o *firewall* específico da rede IoT) e inserir esta informação em uma ferramenta disponível no *site* do Tor Project. Com isto, é possível obter a lista de IPs dos *relays* de saída da rede Tor que possam entrar em contato com o IP de *host* informado. Em seguida o código executa regras Iptables[1] de bloqueio ou repasse de pacotes originados dos IPs constantes na lista obtida. Considerando que os *relays* de saída são normalmente *hosts* mais estáveis, sugere-se a automatização de execução do procedimento de forma que o *script* execute de tempos em tempos para fins de atualização da lista. O Apêndice C é uma proposta de implementação e como se trata de um software livre, está disponível para melhorias. Para fins de prova de conceito do funcionamento do código proposto, o mesmo foi aplicado a um ambiente de teste composto de um servidor *web* Apache (utilizado em mais de 50% dos servidores web em escala global (NETCRAFT, 2017) (W3TECHS, 2017)) localizado em New York e o cliente (origem do acesso) na cidade de São Sebastião do Paraíso-MG, Brasil. No primeiro momento demonstra-se o acesso tradicional e em seguida demonstra-se o ambiente após a execução do código de proteção.

Começando pela Figura 44 (pág. 147), observa-se a identificação do IP real do cliente através do *website* `http://www.dnstools.ch`. Em seguida, a Figura 45 (pág. 148) apresenta o acesso ao *website* `www.dorivaljunior.com.br` hospedado no *webserver* e criado especificamente para esta pesquisa. A Figura 46 (pág. 148) apresenta o *log* do Apache comprovando a origem do acesso através do registro do IP real do cliente (o mesmo identificado na Figura 44 no momento do teste.

Utilizando o cliente Tor a ferramenta `http://www.dns.tools.ch` identifica o IP do cliente como apresentado na Figura 47 (pág. 149) e a Figura 48 (pág. 150) demonstra o acesso ao mesmo *website* (não há qualquer diferença entre o primeiro e este acesso). Neste momento o *log* do Apache (Figura 49, pág. 150) registrar o acesso como originado de um IP diferente do apresentado na Figura 47. Isto ocorre pelo fato de que o acesso ao *website* aconteceu por um *exit relay*, ao passo que o IP identificado para o cliente, trata-se de um *guard relay*.

[1] Ferramenta nativa em distribuições Linux para implementação de regras de *firewall* (MACHADO JR, 2015)

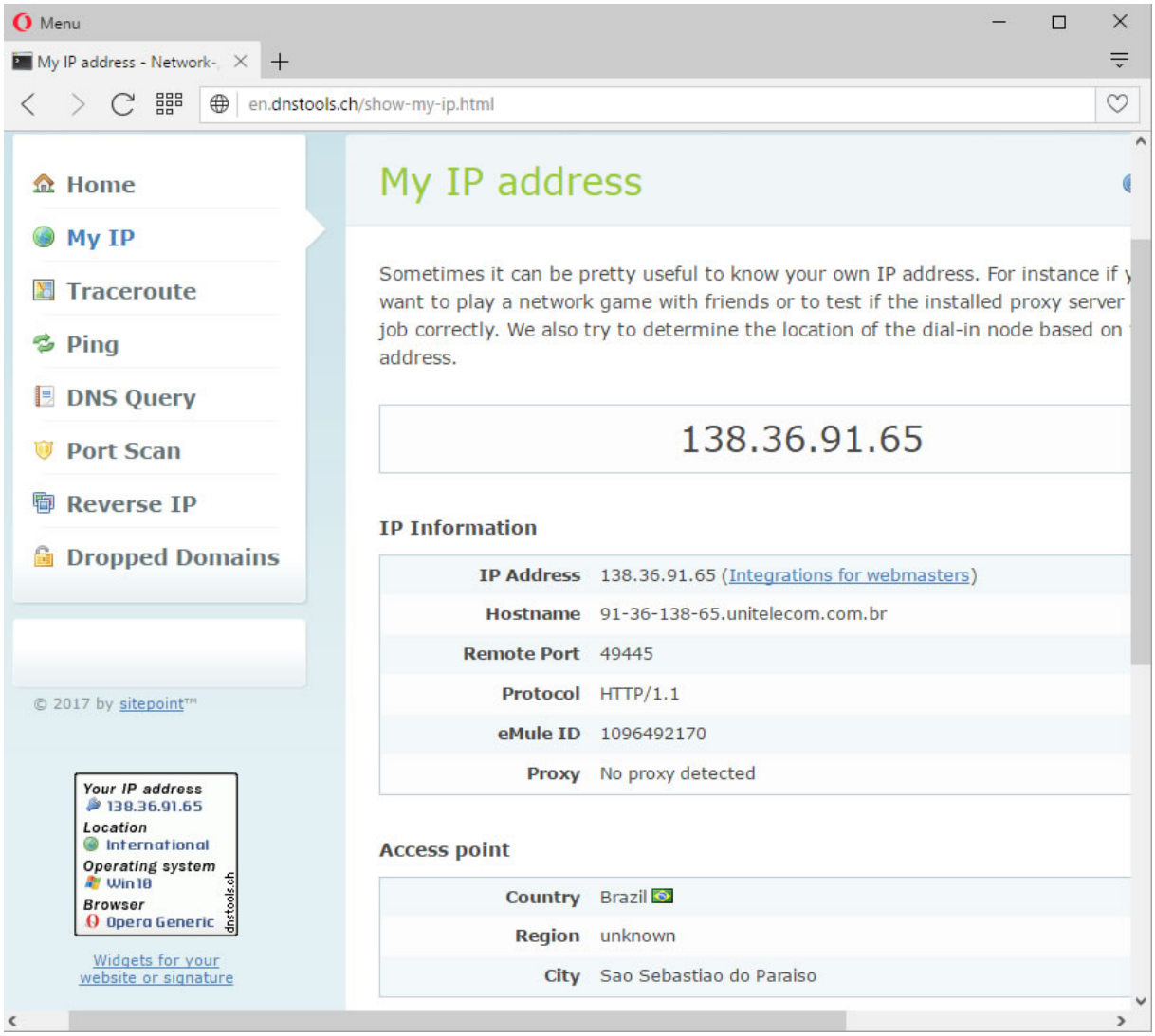


Figura 44: Identificação do IP real do cliente

Até o momento comprovou-se a disponibilidade de acesso ao *webserver* através da Internet tradicional bem como pela rede Tor. Na sequência, observa-se pela Figura 50 (pág. 151) as regras de *firewall* existentes no *host* em questão, ou seja, não há nenhuma regra de bloqueio para entrada ou repasse de pacotes, o que permitiu que ambos os acessos demonstrados ocorressem normalmente. Neste momento o *shell script* (Apêndice C) foi executado de forma a bloquear todos os acessos originados de IPs identificados pelo *script*. Com isto o acesso ao *website* não é mais possível à partir da rede Tor conforme demonstrada a tela do cliente na Figura 51 (pág. 151). Como prova de conceito, observa-se através da Figura 52 (pág. 152) a visualização de um trecho das regras de *firewall* geradas pelo *script*. A primeira coluna registrada a quantidade de pacotes que se enquadrou em determinada regra, a terceira coluna refere-se à ação a ser tomada (DROP indica a negação do pacote) e a penúltima coluna indica o IP de origem do pacote, que no caso são os IPs de saída da rede Tor. Em vista do experimento aqui realizado, observa-se na primeira coluna que duas linhas, isto é, dois IPs tiveram seus pacotes de origem bloqueados, os

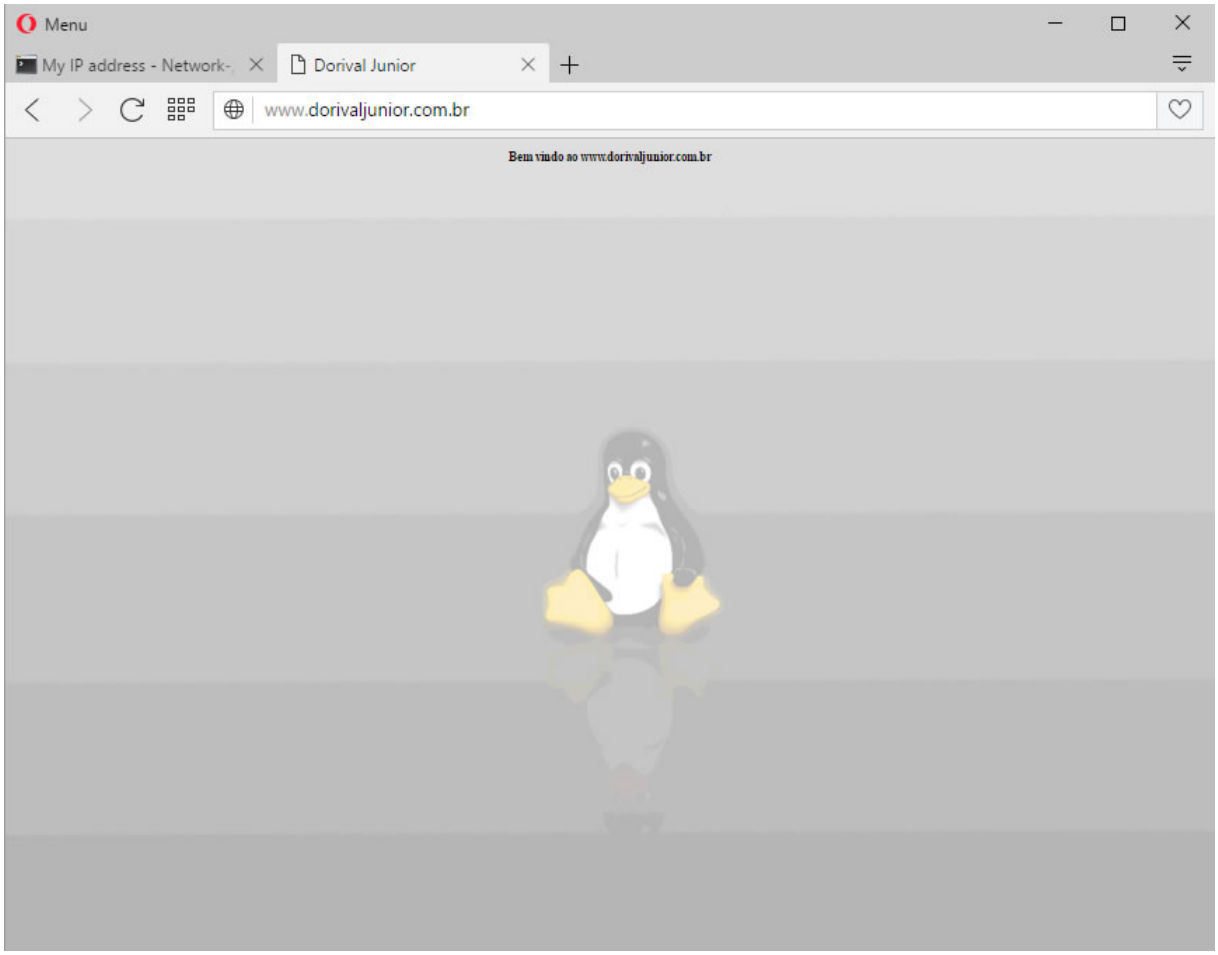


Figura 45: Acesso ao *website* hospedado no *webserver* em New York

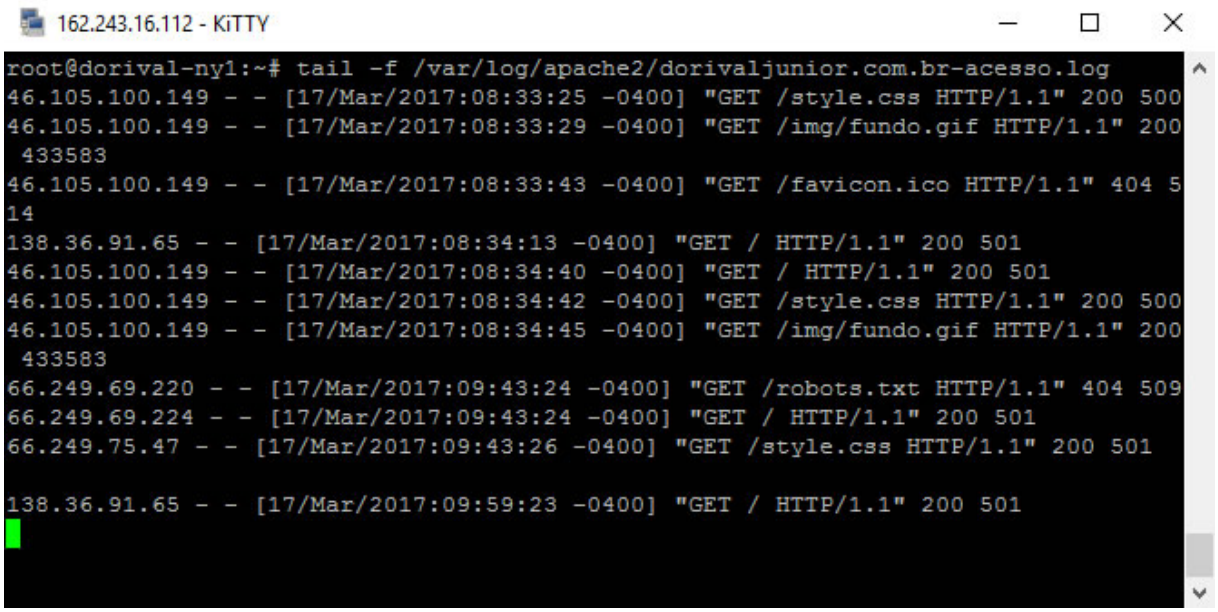


Figura 46: *Log* de acesso ao `dorivaljunior.com.br` gerado pelo Apache

quais provavelmente foram originados do cliente Tor do ambiente de experimento.

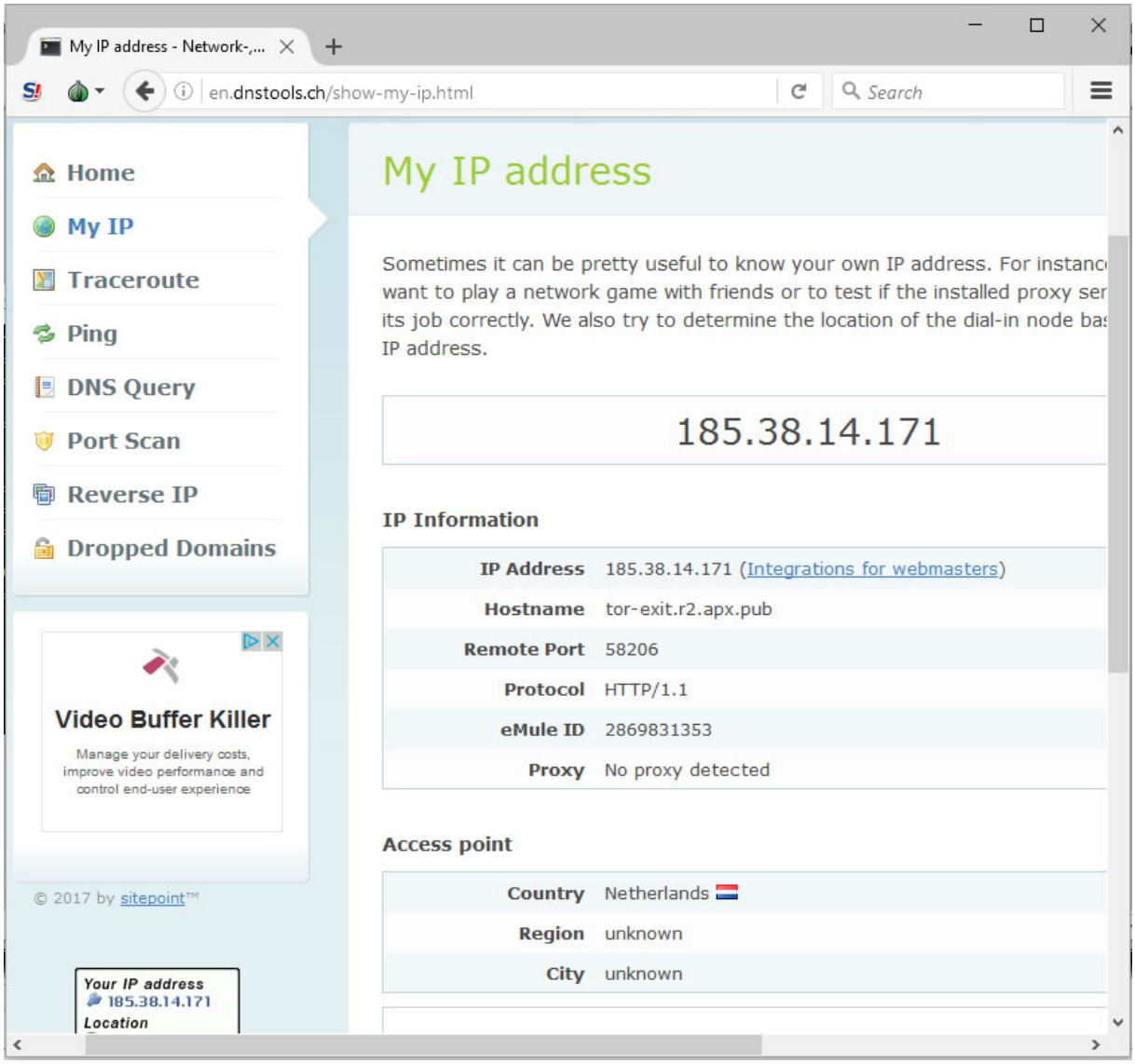


Figura 47: Identificação do IP do cliente, que por sua vez está usando a rede Tor

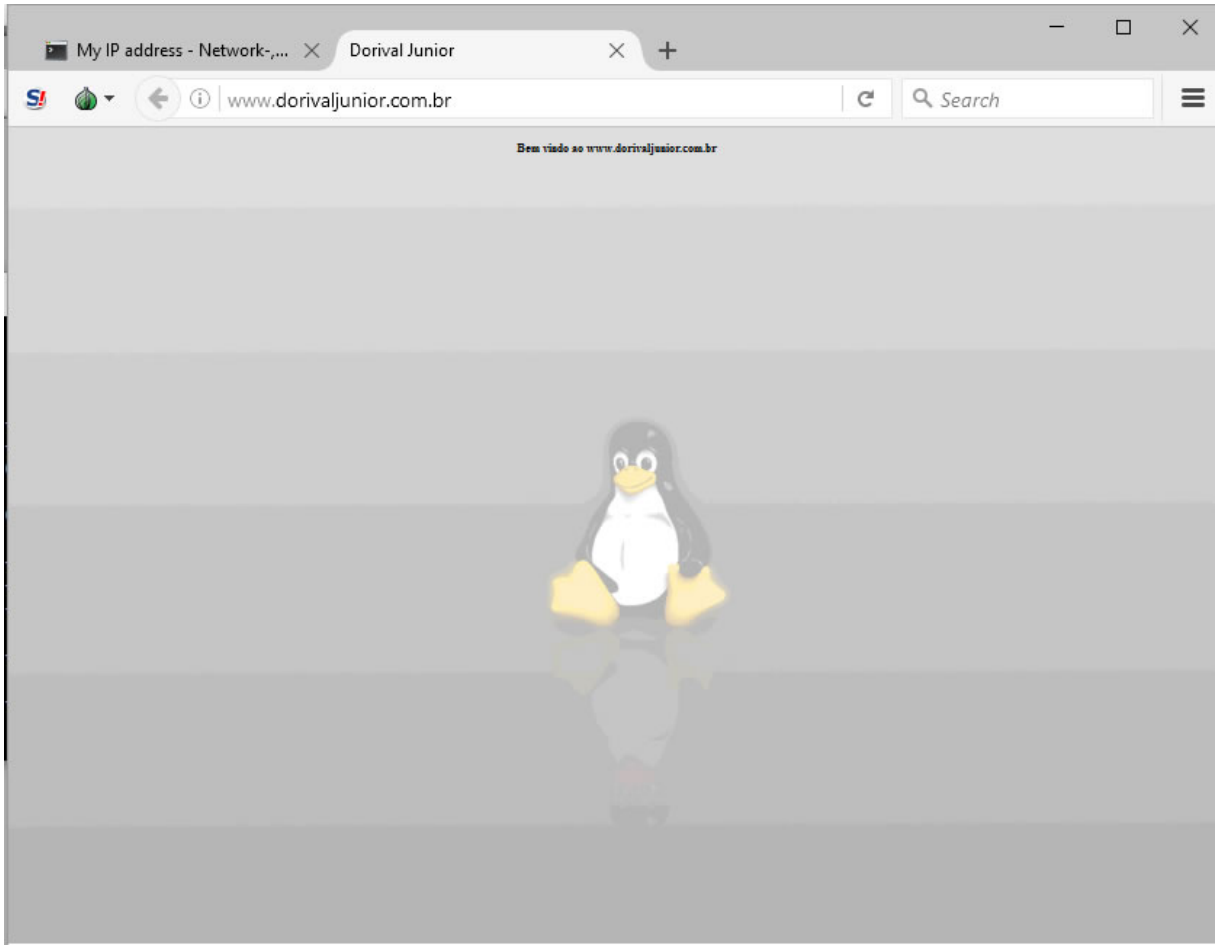


Figura 48: Acesso ao *website* via navegador Tor

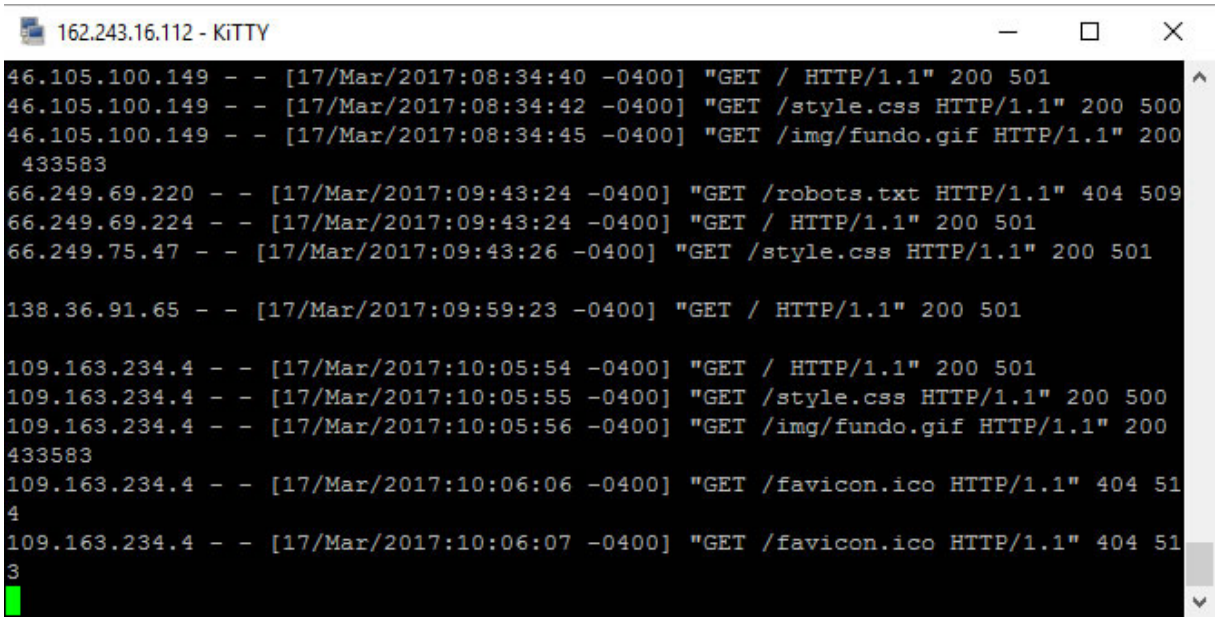


Figura 49: *Log* de acesso ao `dorivaljunior.com.br` registrando o *exit relay* da rede Tor

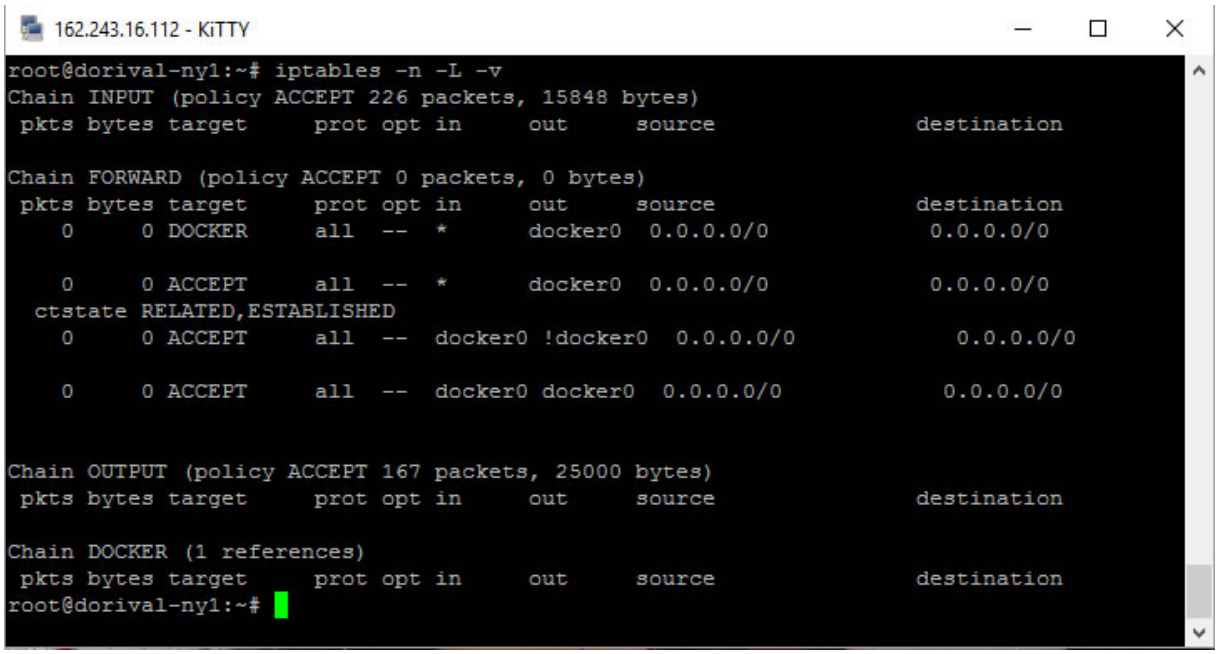


Figura 50: Visualização das regras de *firewall* existentes

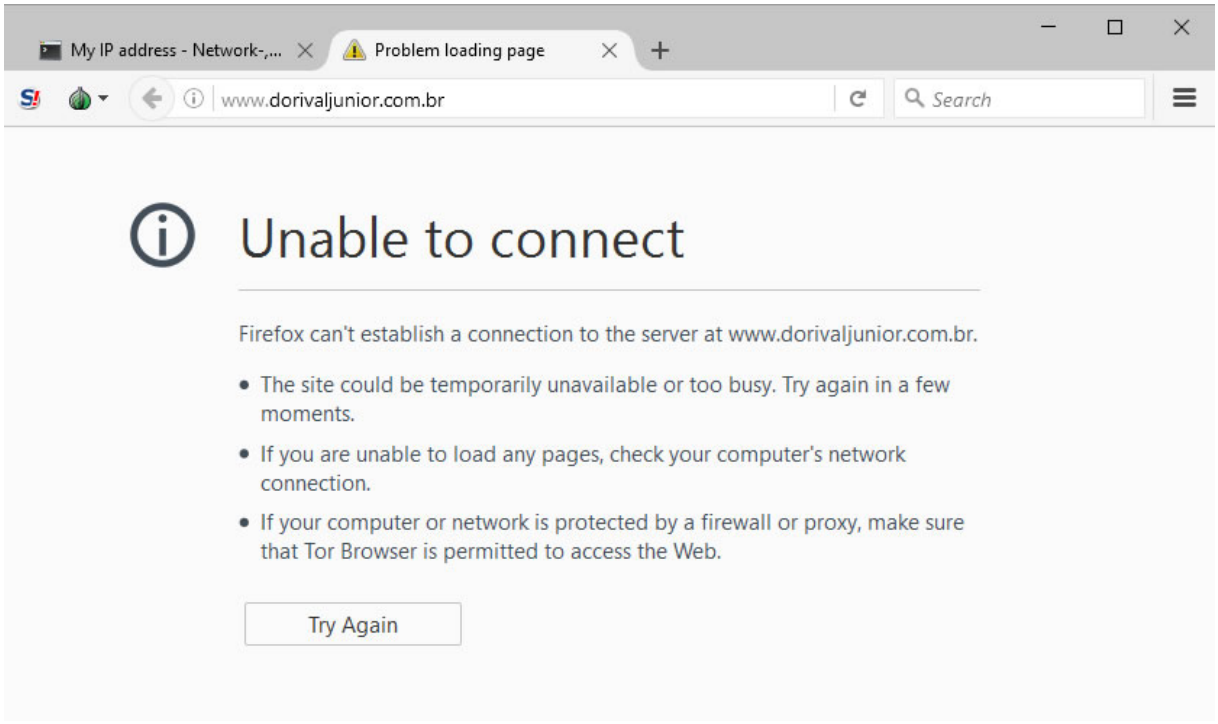


Figura 51: Tentativa acesso ao `dorivaljunior.com.br` utilizando a rede Tor

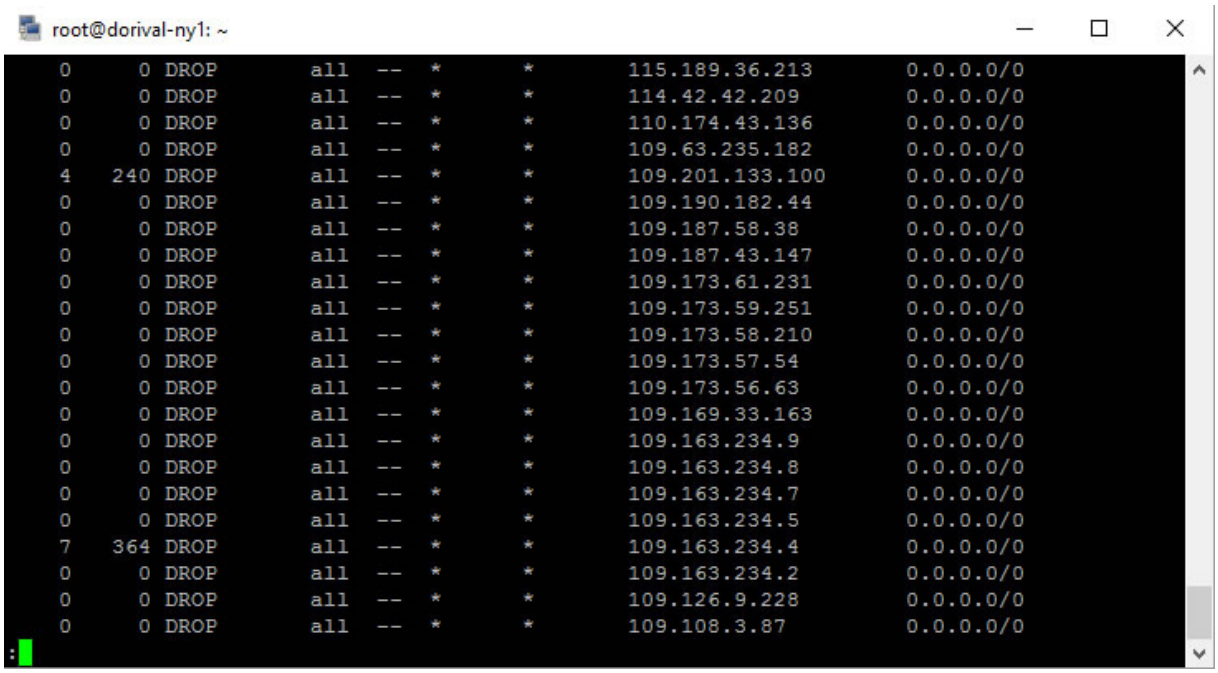


Figura 52: Visualização parcial das regras de *firewall* constando o bloqueio de pacotes originados dos IPs de *exit relays* da rede Tor

APÊNDICE E – Teste comparativo de conexão com VPN e sem VPN

O experimento consiste na realização de sequências de `ping` dentro e fora de uma VPN. O principal resultado do `ping` que é o *time to live* (tempo de ida e volta que um pacote de dados gasta para determinado *host* remoto) foi o índice utilizado para comparação e possibilitou demonstrar a diferença em termos de latência em uma conexão sem o uso de VPN e outra com o uso de VPN.

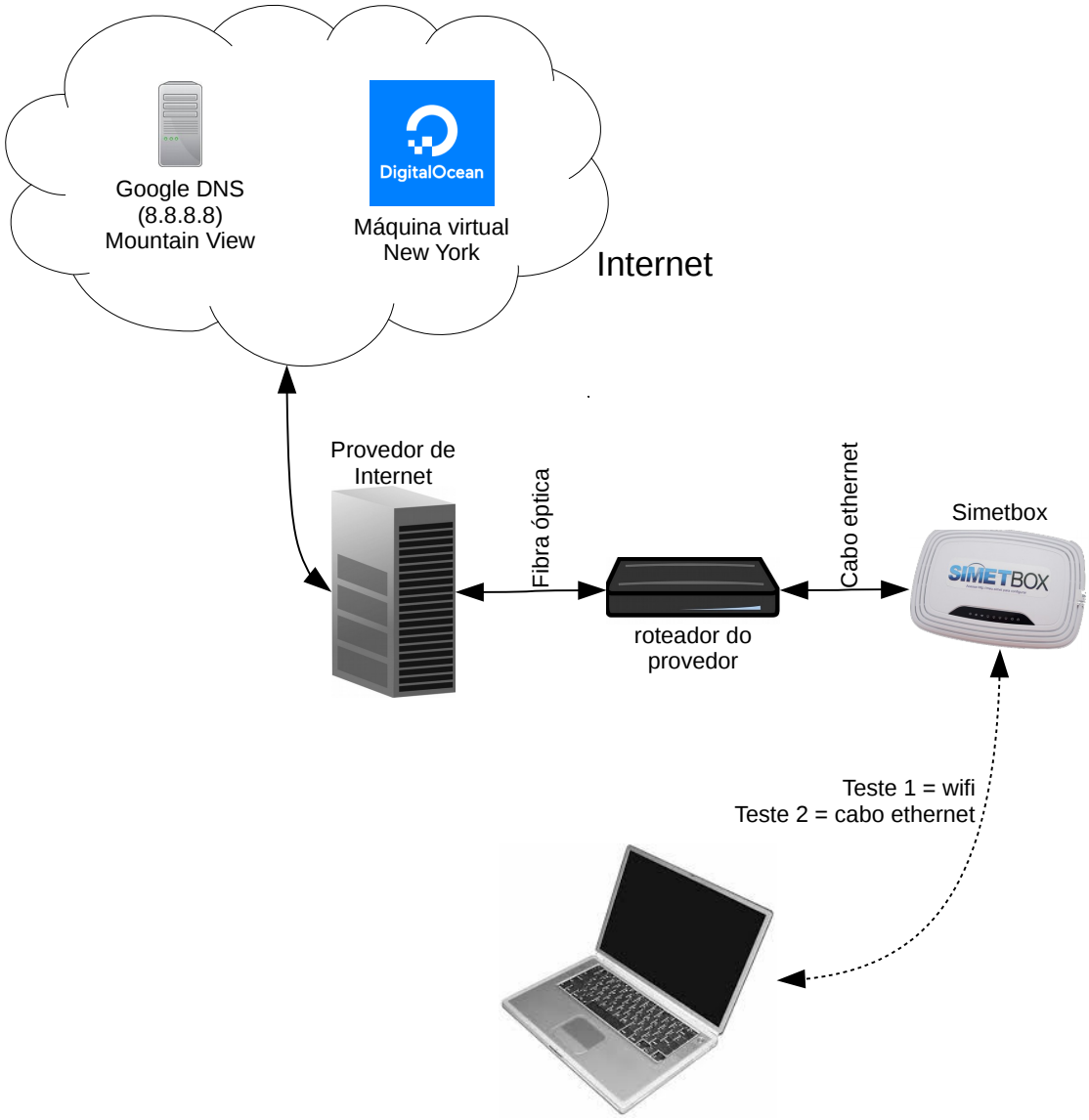


Figura 53: Representação do ambiente usado no teste.

A Figura 53 representa o ambiente de experimentação para o qual foram utilizados

os seguintes recursos:

- **Uma máquina virtual**: foi utilizado o serviço da Digital Ocean[1] para hospedagem da máquina em New York. A máquina possui sistema operacional Linux (distribuição Ubuntu 14.04.5 LTS com kernel 3.13.0-79) por ser de código aberto o que favorece melhor desenvolvedores de novas tecnologias como é o caso da IoT.

- **OpenVPN**[2]: software livre para criação de redes privadas virtuais. Para a criação do servidor VPN foram utilizadas instruções constantes no tutorial da Digital Ocean em Ellingwood (2016).

- ***Script* comparativo**: Este código (Apêndice B) realiza duas sequências de 40 `pings` a um mesmo destino previamente determinado. Na primeira sequência, utiliza-se a rede tradicional (sem VPN) salvando um arquivo texto com os resultados. Após isto, o *script* faz uma pausa para que em outro terminal o usuário execute os comandos de requisição para usar a VPN. Uma vez estabelecido o túnel, o usuário libera a continuação do *script* e este faz a mesma sequência de *pings*. Terminada esta etapa é gerado um gráfico comparativo entre as duas situações.

- **simetbox**: *firmware* oferecido pelo NIC.br utilizado para analisar a qualidade da Internet (NIC.BR, 2017b). A Figura 54 (pág. 155) apresenta o registro das medições realizadas pelo equipamento antes e durante o experimento o que demonstra uma boa qualidade de Internet (considerando o plano de 100Mbps) com latência média de 14 milissegundos (considerando todas as medições realizadas).

- **Uma máquina real**: foi utilizado um notebook Dell Vostro, 6GB de memória RAM, processador 2.4GHZ quadcore, sistema operacional Linux Ubuntu 15.04.

O destino previamente determinado foi o IP 8.8.8.8 (DNS Google) que está localizado em Mountain View nos Estados Unidos conforme ipinfo.io (2017). Este destino foi escolhido pelo fato de que o DNS é o primeiro acesso que realmente acontece em uma conexão *web*. A máquina virtual (que atua como servidor VPN) está localizada também nos Estados Unidos (New York). A máquina local (cliente VPN) está localizada no Brasil. O experimento foi realizado no dia 28 de novembro de 2017 por volta das nove horas, horário com uma intensidade de tráfego mediana tomando por base o registro do PTT conforme a Figura 55 retirada de Nic.br (2017d).

O experimento foi realizado através de dois testes: no primeiro foi utilizada uma conexão wifi entre o Simetbox e a máquina real. No segundo teste a conexão foi estabelecida através de cabeamento. No contexto de IoT a predominância está para equipamentos

[1] `https://www.digitalocean.com/`
[2] `https://openvpn.net/`

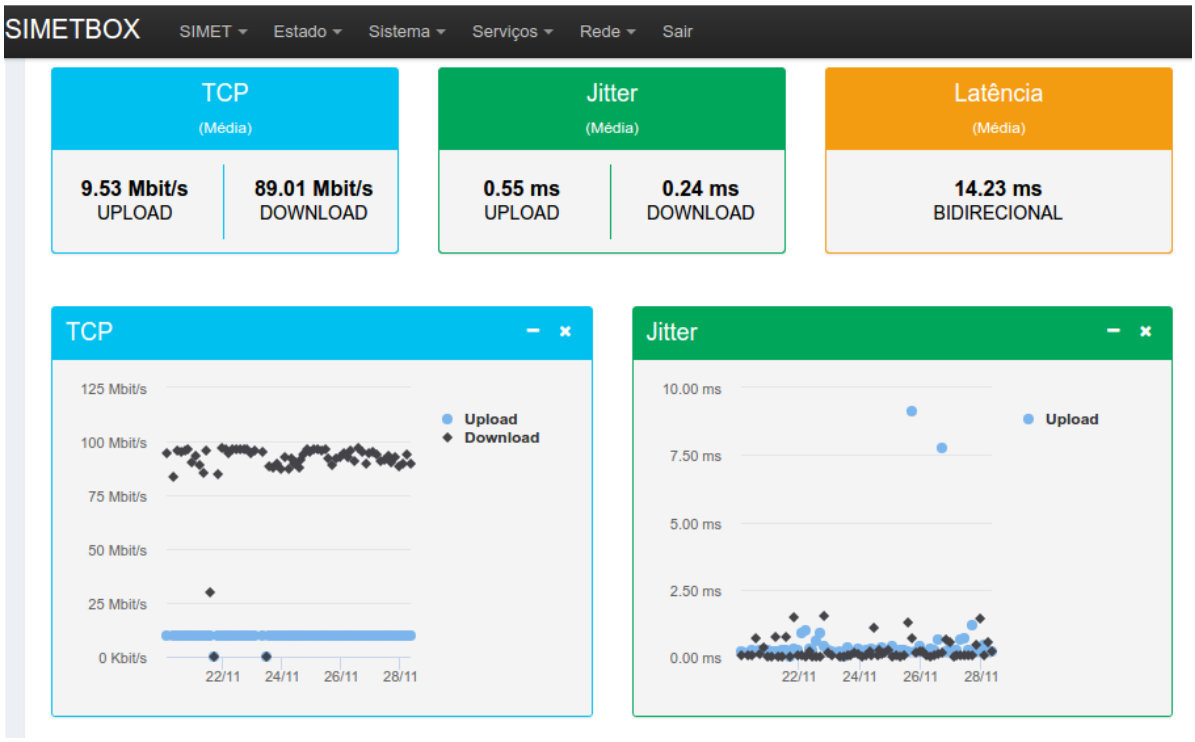


Figura 54: Painel de indicadores do Simetbox.

sem fio, mas de todo modo ambos os testes foram realizados para comprovação em relação ao processamento de VPN.

No primeiro teste (usando conexão local wifi) observa-se pela Figura 56 (pág. 157) que o fluxo de dados com uso de VPN registrou um TTL (*time to live*) em torno de 125 milissegundos, havendo picos de variação do ambiente. O fluxo de dados sem o uso de VPN assinalou um TTL em torno de 10 milissegundos.

No segundo teste (usando conexão local cabeada) observa-se através da Figura 57 (pág. 157) que o fluxo de dados com uso de VPN registrou um TTL em torno de 123 milissegundos. Apesar de ser uma marca próxima do primeiro teste, observa-se que o fluxo permanece estável em relação ao ambiente sem fio. Em relação ao fluxo de dados sem o uso de VPN, este se mostrou também estável, mas com TTL em torno de 8 milissegundos, ou seja, uma latência bem menor comparado à outra conexão.

Com o objetivo de experimentação em ambiente com mais hosts, foi realizado um último teste no qual o Simetbox fornecesse conexão de Internet para uma rede cabeada com mais 10 máquinas e conexão wifi para 2 máquinas. Em todas elas, usuários fizeram acesso normalmente à Internet, apenas acessando páginas *web*. O resultado é conforme a Figura 58, através da qual o mesmo padrão de latência é mantido em comparação aos testes anteriores. A única diferença é que ocorrem maiores picos em vista da grande quantidade de conexões.

A Figura 59 (pág. 158) atua apenas como registro fotográfico do equipamento

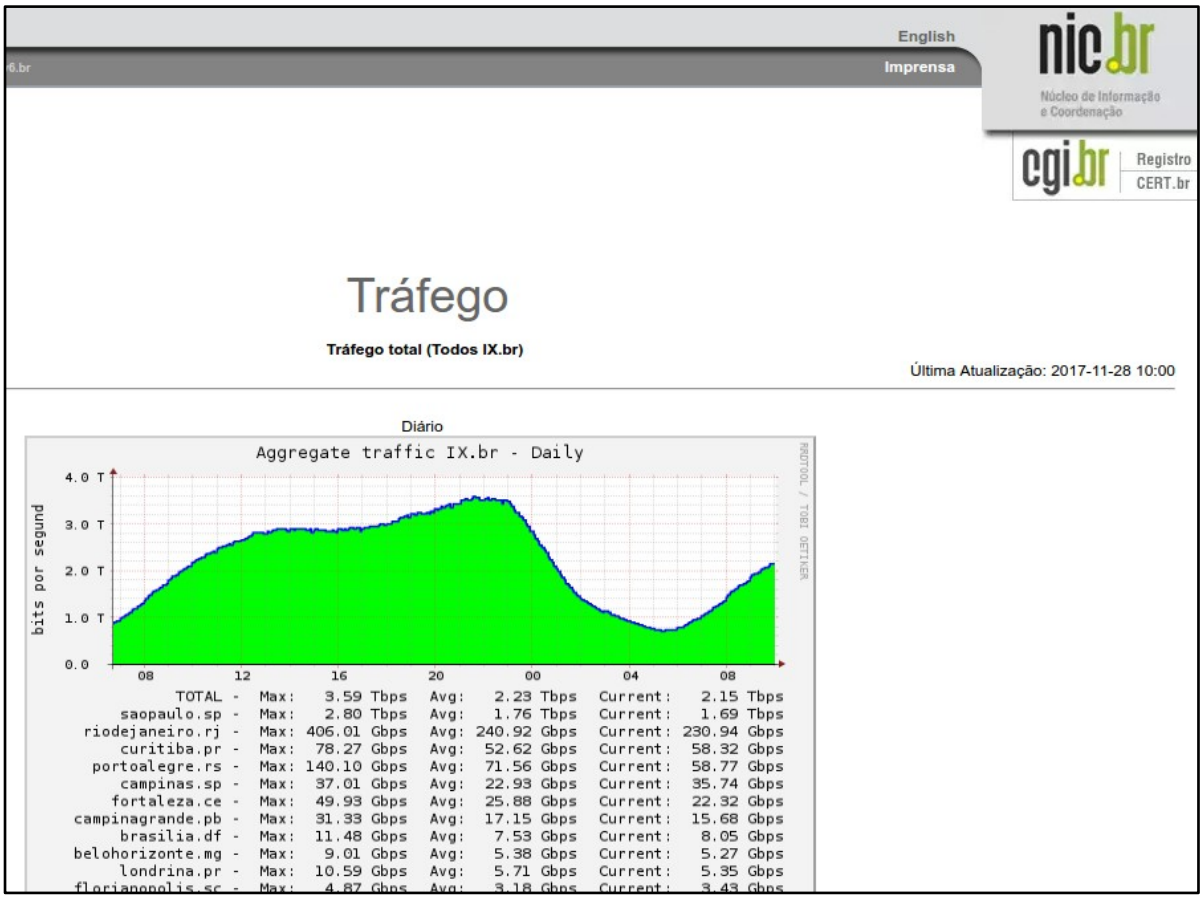


Figura 55: Tráfego total do PTT referente ao período de 07h00m do dia 27/11/2017 até 10h00 do dia 28/11/2017 conforme Nic.br (2017d).

utilizado localmente.

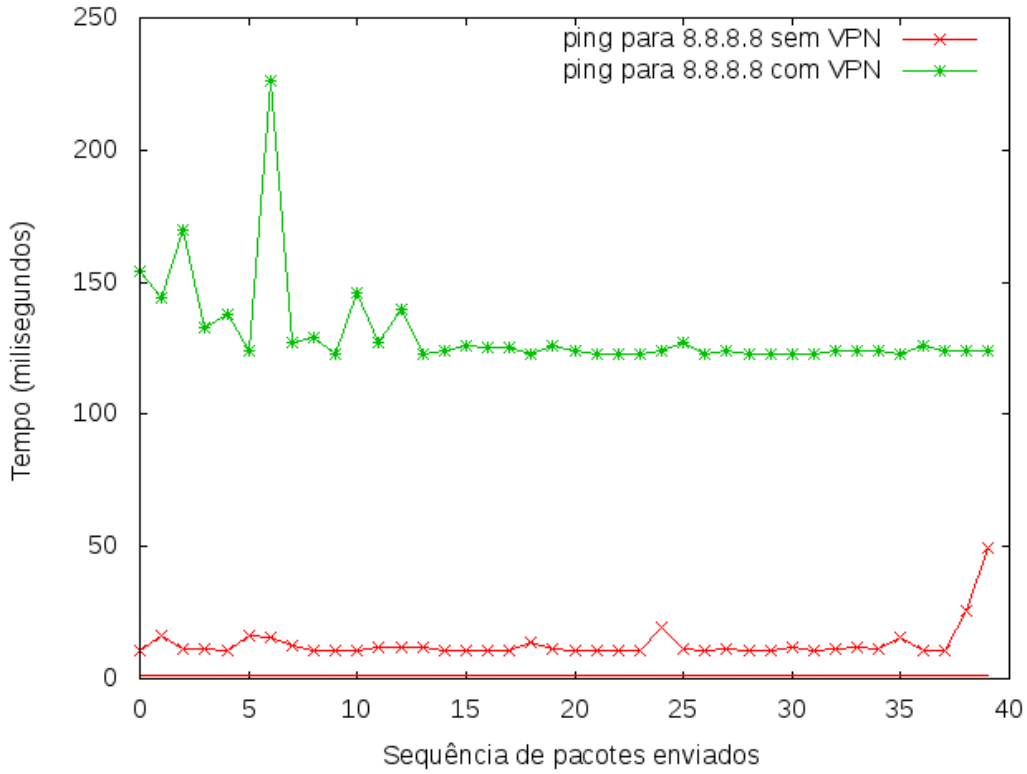


Figura 56: Comparativo de conexão (rede local wifi) com uso de VPN e sem uso de VPN.

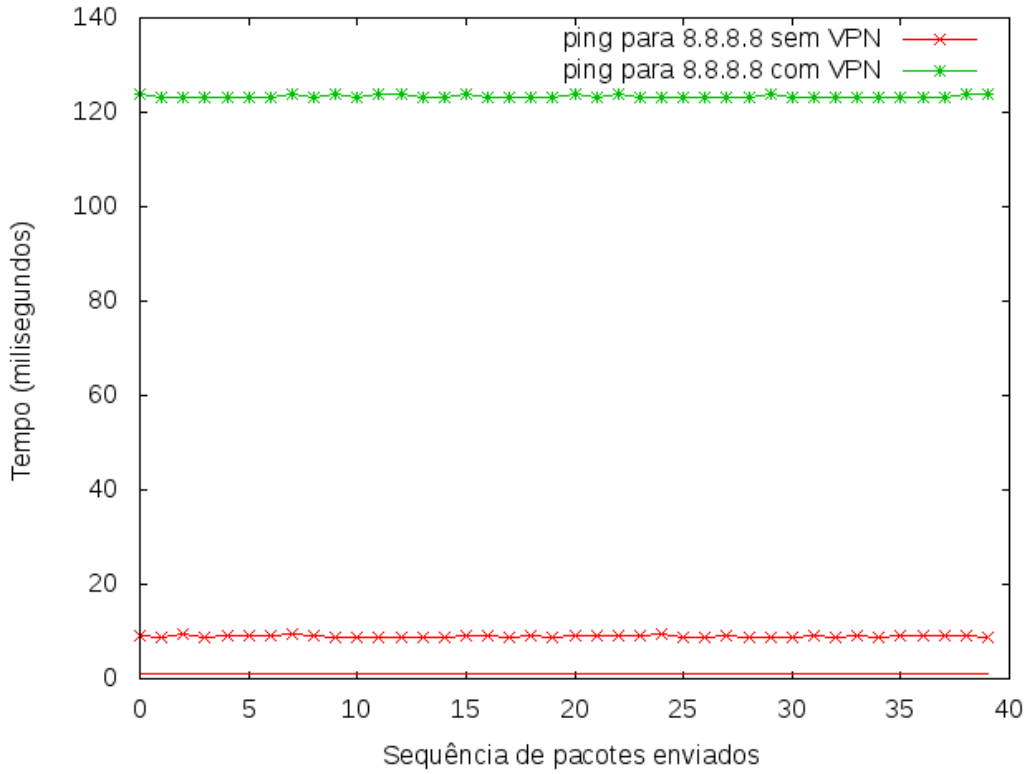


Figura 57: Comparativo de conexão (rede local ethernet) com uso de VPN e sem uso de VPN.

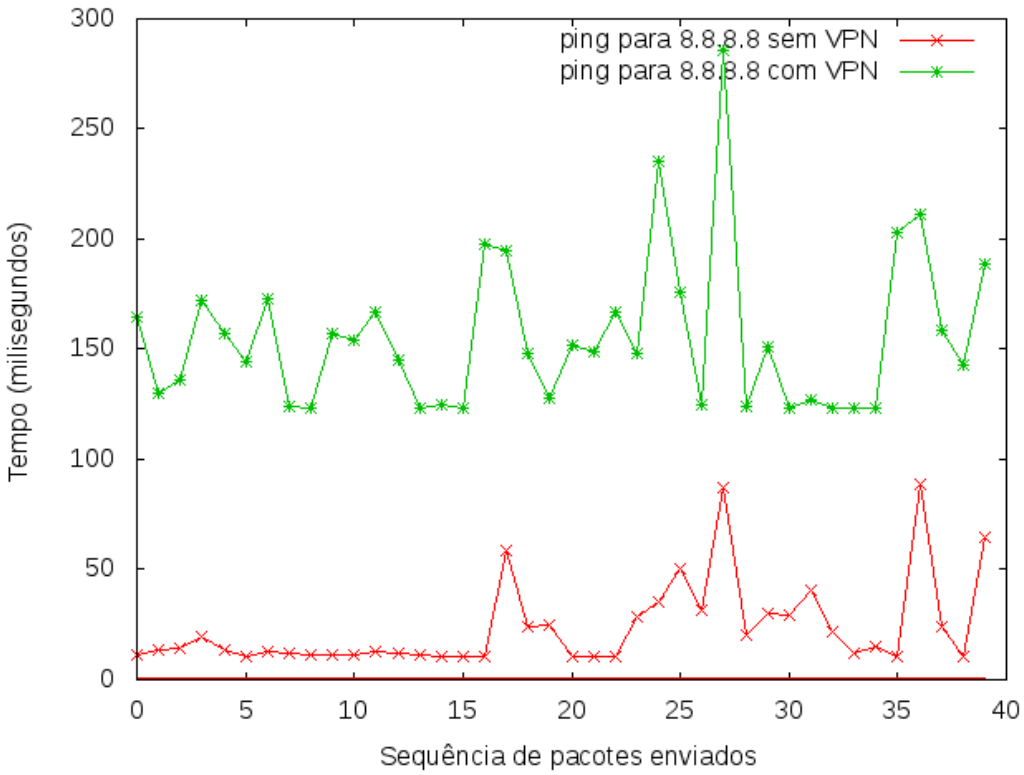


Figura 58: Comparativo de conexão (rede local ethernet e wifi com vários clientes) com uso de VPN e sem uso de VPN.

Figura 59: Equipamento utilizado na rede local.