UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
MBA EM GESTÃO DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

LEONARDO MASSAMI FUKUDA

SEGURANÇA DA INFORMAÇÃO EM IOT

MONOGRAFIA

CURITIBA
2019

LEONARDO MASSAMI FUKUDA

SEGURANÇA DA INFORMAÇÃO EM IOT

Monografia apresentada como requisito parcial para obtenção do título de Especialista em Gestão da Tecnologia da Informação e Comunicação da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. MSc.Alexandre Miziara

CURITIBA

2019

Folha destinada à inclusão da **Ficha Catalográfica** por meio de solicitação ao Departamento de Biblioteca da UTFPR e posteriormente inserida nesse espaço: verso da Folha de Rosto (folha anterior).

Espaço para a ficha catalográfica sob responsabilidade exclusiva do Departamento de Biblioteca da UTFPR.

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Campus Curitiba
Diretoria de Pesquisa e Pós-Graduação
CURSO DE ESPECIALIZAÇÃO EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

TERMO DE APROVAÇÃO

SEGURANÇA DA INFORMAÇÃO EM IOT

por

LEONARDO MASSAMI FUKUDA

Esta monografia foi apresentada às **19:30 h** do dia **27/06/2019** como requisito parcial para a obtenção do título de Especialista no CURSO DE ESPECIALIZAÇÃO EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, da Universidade Tecnológica Federal do Paraná, **Campus Curitiba**. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho:

1		Aprovado
2		Aprovado condicionado às correções Pós-banca, postagem da tarefa e liberação do Orientador.
3		Reprovado

_____

Prof. MSc. Bernadete M.V.F. Rosa
UTFPR - Examinador

_____

Prof. MSc. Alexandre Jorge Miziara
UTFPR – Orientador

_____

Prof. MSc. Alexandre Jorge Miziara
UTFPR – Coordenador do Curso

O documento original encontra-se arquivado no DAELN

AGRADECIMENTOS

Dedico este trabalho primeiramente a Deus, por ser essencial em minha vida, autor de meu destino, meu guia, e minha família com muito carinho e apoio, não mediram esforços para que eu chegasse até esta etapa da minha vida.

RESUMO

FUKUDA, Leonardo Massami. **Segurança da Informação em *IOT***. 2019. 41f. Monografia (MBA em Gestão da Tecnologia da Informação e Comunicação) - Universidade Tecnológica Federal do Paraná. CURITIBA, 2019.

Os avanços tecnológicos são inquestionáveis, cada vez mais presente no dia a dia, modificando o comportamento das pessoas, o modo de fazer compras, interagir, fazer amizades, ver filmes, ler notícias e principalmente a forma de se informar. Hoje a internet deixou de conectar apenas computadores, para conectar pessoas, a evolução das tecnologias permite essa conectividade em inúmeros tipos de dispositivos, a "Internet das Coisas", facilitando a interação e gerando enormes benefícios para a população. Esse presente estudo visa analisar pontos fundamentais sobre a Internet das Coisas internet, sua tecnologia, vantagens e desvantagens. Essa análise sobre Internet das Coisas, será mensurada pela Segurança da Informação, onde busca-se uma reflexão sobre a vulnerabilidade e critérios de segurança na Internet das Coisas. Em 60 segundos saber que resultou em 3.8 Milhões de pesquisas no Google, 3.3 Milhões de Posts no Facebook, 29 Milhões de mensagens enviadas via *Whatsapp*, 448.800 *Tweets* no *Twitter*, 65.972 *uploads* de fotos no *Instagram*, 149.513 e-mails enviados, 500 horas de *upload* de vídeos no *Youtube*, e 1.440 posts no *Wordpress*, com todas essas informações a motivação é clara em saber como a Segurança da Informação está preparada para a quantidade de informações de trafegam de entre os dispositivos e pessoas, se estamos seguros em produzir essa quantidade de conteúdo para a Internet. Analisar a eficiência da Segurança da Informação da Internet das Coisas, entendendo sobre a Segurança da Informação em dispositivos de conexão. Mapeando as vulnerabilidades da Segurança em *IoT*, conhecer os mecanismos de funcionamento sobre as formas e vantagens oferecidas pela *IoT*, refletindo sobre os indicadores de Segurança da Informação na infraestrutura que utilizam esta tecnologia. Será utilizado com instrumento norteador a pesquisa exploratória, para identificar os fatos pertinentes ao objetivo de estudo que será a base para futuros trabalhos, visando assim conciliar os conhecimentos científicos, da realidade praticada, buscando resultados. Considerando que a proposta deste estudo, não é apresentar soluções para o Segurança da Informação em *IoT* e sim realizar uma análise dos critérios de segurança da informação em ambientes de conexão *IoT*, assim recorremos a diversas referências bibliográficas, onde relevados autores com importantes contribuições literárias, foram analisados e nortearam o estudo em questão. A realização deste trabalho permitiu, analisar e mensurar o uso de novas tecnologias, compreendendo a origem, e a sua disseminação, bem como as vantagens, da internet das coisas, é possível conhecer em um nível mais aprofundado seus problemas e barreiras. Graças a contribuição de diversos autores e suas obras, observamos que a *IoT*, sem dúvida é o enorme salto das tecnologias e inovações. Seus resultados são de altíssimas relevância e melhoria para qualidade de vida das pessoas e corporações, também foi possível realizar uma ampla reflexão sobre o importante papel da Segurança da Informação, os benefícios que sua aplicação de modo corretor podem oferecer para os usuários da *IoT*. Dessa forma, o presente estudo finaliza-se, de modo satisfatório pela importância de investigar duas áreas com evolução e aplicação tão impactante, fundamentais no mundo contemporâneo, que são a Segurança da informação e a Internet das Coisas, pois essa junção de modo correto oferecerá cada vez mais benefícios e qualidade de vida nos setores pessoais e profissionais e sobretudo espera-se um grande crescimento da *IoT*, com total confiança oferecida pela Segurança da Informação.

Palavras Chave: *IoT*, Segurança da Informação, Vulnerabilidade, Conexão.

ABSTRACT

FUKUDA, Leonardo Massami. *Information Security in IOT*. 2019. 41 f. *Monograph* (MBA *in Management of Information Technology and Communication) - Federal Technological University of* Paraná, CURITIBA, 2019.

Technological advances are unquestionable, increasingly present day to day, modifying people's behavior, shopping, interacting, making friends, watching movies, reading news, and especially how to get informed. Today the Internet has stopped connecting only computers, to connect people, the evolution of technologies allows this connectivity in many types of devices, the "Internet of Things", facilitating interaction and generating huge benefits for the population. This present study aims to analyze fundamental points about the Internet of Things Internet, its technology, advantages and disadvantages. This analysis on IoT will be measured by Information Security, where it is sought a reflection on the vulnerability and safety criteria in the IOT. In 60 seconds you know it resulted in 3.8 Million searches on Google, 3.3 Million Facebook Posts, 29 Million messages sent via Whatsapp, 448,800 Twitter Tweets, 65,972 Instagram Photo uploads, 149,513 emails sent, 500 hours upload videos on Youtube, and 1,440 posts on Wordpress, with all this information the motivation is clear in knowing how Information Security is prepared for the amount of information to travel between devices and people if we are sure to produce that amount content to the Internet. Analyze the efficiency of Internet Information Security of Things, understanding about Information Security in connection devices. Mapping the security vulnerabilities in IoT, knowing the mechanisms of operation on the forms and advantages offered by IoT, reflecting on the indicators of Information Security in the infrastructure that use this technology. Exploratory research will be used as a guiding instrument to identify the pertinent facts of the study objective that will be the basis for future work, in order to reconcile the scientific knowledge, the reality practiced, seeking results. Considering that the proposal of this study is not to present solutions for Information Security in IoT, but to carry out an analysis of information security criteria in IoT connection environments, we have used several bibliographical references, where authors with important literary contributions have been surveyed, were analyzed and guided the study in question. The realization of this work allowed, analyze and measure the use of new technologies, understanding the origin, and their dissemination, as well as the advantages, of the internet of things, it is possible to know in a deeper level their problems and barriers. Thanks to the contribution of several authors and their works, we note that IoT is undoubtedly the great leap of technologies and innovations. Its results are of high relevance and improvement to the quality of life of individuals and corporations, it was also possible to carry out a broad reflection on the important role of Information Security, the benefits that its application can offer to IoT users. In this way, the present study is satisfactorily completed by the importance of investigating two areas with such a powerful evolution and application, fundamental in the contemporary world, which are Information Security and the Internet of Things. more and more benefits and quality of life in the personal and professional sectors, and above all, a great growth of IoT is expected, with full confidence offered by Information Security.

Keywords: IoT, Information Security, Vulnerability, Connection.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

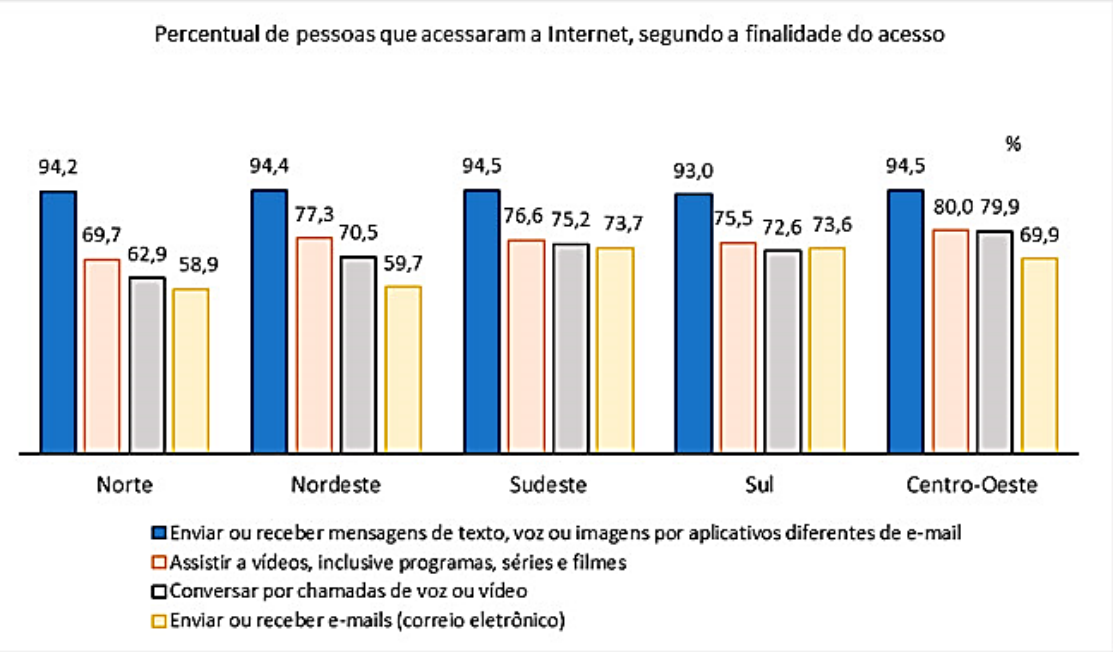
1 INTRODUÇÃO

O que hoje é chamado de internet das coisas (*internet of things*) é um conjunto de tecnologias, protocolos e sensores que permitem que objetos se conectem a uma rede de comunicações e são capazes de coletar e transmitir dados. É uma extensão da internet atual que possibilita que objetos do dia-a-dia quaisquer que sejam, com capacidade computacional e de comunicação que se conectem à Internet. Assim unificando a necessidade de garantir a privacidade das informações e a facilidade de conexão. De acordo com (TAURION 2017), "talvez estejamos às portas de uma nova revolução de tanto impacto na sociedade como foi a industrial no século XIX". Cada vez mais as pessoas estão conectadas com seus celulares e demais dispositivos gerando informações na internet. Através do avanço das tecnologias nos últimos anos, a oferta de serviços através da *Web* tem aumentado de forma expressiva e evoluindo diariamente, facilitando cada vez mais nosso dia a dia. Com esta evolução surgiu a ideia de se conectar o meio físico ao virtual, o que recebeu o nome de Internet das Coisas, que segundo (VALENTE 2011), é um paradigma que tem por objetivo criar uma ponte entre acontecimentos do mundo real e as suas representações no mundo digital, por meio da conexão de objetos.

Segundo o Instituto Brasileiro de Geografia e Estatística – IBGE, apresentou no PNAD Contínua TIC 2016 a análise dos resultados obtidos pode-se observar na Figura 1, que 94,2% das pessoas que utilizaram a Internet o fizeram para trocar mensagens de texto, voz ou imagens por diversos tipos de aplicativos, além de assistir a vídeos, programas, séries e filmes 76,4%, as conversar por chamada de voz ou vídeo, representa 73,3% e enviar ou receber e-mail, com um total de 69,3%.

Os aparelhos de telefonia móvel fazem parte de 92,6% dos 69,3 milhões de domicílios. No segundo, o computador, como o único meio de acesso em apenas 2,3% das residências com Internet. As Televisões com conversor digital, representa 48,2 milhões 71,5% e restante somente com o conversor de sinal para a TV aberta. A idade que mais acessou a Internet, está representada na faixa etária de 18 a 24 anos de idade, já as pessoas acima de 60 anos (ou mais), apenas 24,7% acessaram. Os números da conectividade, apontado pelo IBGE, revelou acima de tudo o poder de interação e comunicação entre os meios digitais, cabe ressaltar que a pesquisa foi divulgada no ano de 2017, com dados referentes ao ano anterior.

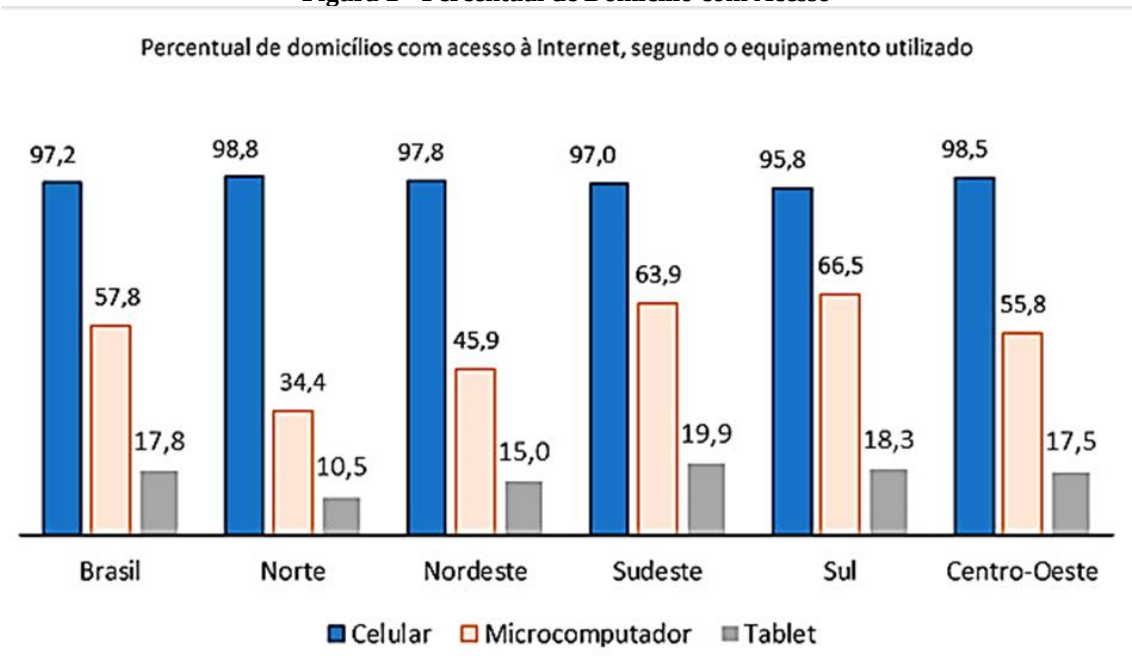
Figura 1 - Percentual de acesso à Internet



Fonte: IBGE/2017.
Disponível em:<https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/20073-pnad-continua-tic-2016-94-2-das-pessoas-que-utilizaram-a-internet-o-fizeram-para-trocar-mensagens> Acesso em: Jan.2019.

Pode-se observar na Figura 2, que outro fato de extrema relevância é o crescimento contínuo ano após anos, estimando que para o ano de 2020, 70% da população mundial estará conectada por dispositivos móveis.

Figura 2 - Percentual de Domicílio com Acesso



Fonte: IBGE/2017.
Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/20073-pnad-continua-tic-2016-94-2-das-pessoas-que-utilizaram-a-internet-o-fizeram-para-trocar-mensagens> Acesso em: Jan.2019.

O dispositivo mais utilizado para acessar a internet é o celular, com 95% dos usuários, 63,7% pelo microcomputador, 16,4% via *tablet*, 11,3% pela televisão e menos de 1% por outro equipamento eletrônico. A grande maioria de acesso foi realizado pela Banda larga 99,6%.

Nos domicílios em que não se usava a Internet, os principais motivos foram: falta de interesse (34,8%), serviço era caro (29,6%) e nenhum morador sabia usar (20,7%). Entre as residências que não utilizaram a Internet, a não disponibilidade do acesso à Internet abrangeu 8,1% e o custo do equipamento, 3,5%.

Regionalmente, o principal motivo para não uso da Internet foi a falta de interesse, exceto no Nordeste, onde ficou atrás de o serviço de acesso ser caro (34,8%). No Norte, o segundo motivo foi a não disponibilidade de acesso à Rede na área (24,4%), percentual mais elevado que nas outras grandes regiões, em que variaram de 9,8% (Centro-Oeste) a 4,2% (Sudeste). Com exceção do Norte, a falta de quem soubesse usar a Internet foi a terceira razão mais citada, variando de 20,3% (Sudeste) a 22,5% (Centro-Oeste).

Na comparação por grupamentos das atividades, o acesso à Internet foi mais elevado, comunicação e atividades financeiras, imobiliárias, profissionais e administrativas (92,0%), da educação, saúde humana e serviços sociais (91,2%), da administração pública, defesa e seguridade social (88,3%) e de outros serviços (87,6%). Agricultura, pecuária, produção florestal, pesca e aquicultura (28,3%) foi o grupamento de atividade com menos uso da Internet.

1.2 Objetivos

Este trabalho tem como principal objetivo analisar a eficiência da Segurança da Informação da Internet das Coisas, entendendo sobre a Segurança da Informação em dispositivos de conexão. Mapeando as vulnerabilidades da Segurança em internet das coisas, conhecer os mecanismos de funcionamento sobre as formas e vantagens oferecidas pela internet das coisas, refletindo sobre os indicadores de Segurança da Informação na infraestrutura que utilizam esta tecnologia.

Para atingir o objetivo principal da pesquisa, foram necessários os seguintes objetivos específicos:

- Entender os dispositivos de Segurança da Informação em dispositivos de conexão;

- Mapear a vulnerabilidade da Segurança da Informação em Internet das coisas;
- Conhecer os mecanismos de funcionamento da internet das coisas;
- Estudar sobre as formas e vantagens oferecidas pela Internet das coisas;
- Refletir sobre os indicadores de Segurança da Informação na infraestrutura que utilizam Internet das coisas, realizando uma análise dos critérios de segurança da informação em ambientes de conexão *IoT*,

1.3 Justificativa

Em virtude da crescente demanda e utilização da internet este trabalho justifica-se pela necessidade de verificar de que forma as empresas e as pessoas na sociedade atual, estão preparadas para internet das coisas, na qual cada vez mais dados circulam pelas redes que conectam indivíduos, empresas e governos em todo o mundo. Essas tecnologias permitem que estudos, trabalho, negócios e lazer sejam conduzidos de forma simples, prática e facilitada, porém, não se pode afirmar que não existam riscos e vulnerabilidades. Pensar em inovação tecnológica é olhar para o futuro, pois hoje a internet deixou de conectar apenas computadores, para conectar pessoas, a evolução das tecnologias permite essa conectividade em inúmeros tipos de dispositivos, a Internet das coisas.

Diante disso, é preciso analisar de que forma a relevância da segurança da informação é vista por empresas e indivíduos, quais as ferramentas utilizadas por eles para que os dados que trafegam na rede sejam mantidos em sigilo e seguro, de que forma buscam melhorar essa segurança diariamente em suas atividades. Com isso, torna- se possível destacar quais são os desafios do setor e as perspectivas na área para os próximos anos.

1.4 Procedimentos metodológicos

Foi realizada uma pesquisa bibliográfica sobre Segurança da Informação em *IoT*. Foram utilizados como fontes de pesquisa, livros, artigos científicos, bibliotecas digitais e repositórios acadêmicos que foram analisados e nortearam o estudo em questão.

As Palavras-chave para a pesquisa em meios eletrônicos: *IoT,* Internet das Coisas, Segurança da Informação, Vulnerabilidade e Conexão.

2 SEGURANÇA DA INFORMAÇÃO

O conceito da Segurança da Informação - SI, ligado com proteção de um grupo de informações, com o vínculo de defender o valor, que essas representam para uma pessoa ou empresa, os critérios da Segurança da Informação, temos a confidencialidade, integridade, disponibilidade e autenticidade. De acordo com (FONTES 2010), o conceito de SI, são:

> Segurança da Informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada.

O conceito de SI é normatizado pelo NBR ISO/IEC 17799, Segundo (CAMPOS 2007), Confidencialidade é:

> Propriedade que limita o acesso à informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação, ou seja a informação somente pode ser acessada por pessoas explicitamente autorizadas.

Sobre a Integridade, Campos, afirma:

> Quando uma informação é indevidamente alterada, intencionalmente ou não, tal como pela falsificação de um documento, da alteração de registros em um banco de dados, ou qualquer coisa que altere a informação original de maneira indevida, configura um incidente de Segurança da Informação por quebra de integridade.

A explicação de (CAMPOS 2007) sobre a Disponibilidade é:

> Quando a informação não é acessível nem mesmo por quem é de direito, como no caso da perda de documentos, quando há sistemas de computador “fora do ar” ou, ainda, em função de ataques de negação de serviço a servidores de rede ou servidores *Web*, ou seja, quando esses servidores estão inoperantes em resultado de ataques e invasões, então isto é um incidente de Segurança da Informação por quebra de

> disponibilidade. Mesmo as “quedas” de sistemas não provocadas, ou seja, não intencionais, configuram quebra de disponibilidade.

(CAMPOS 2007), ainda ressalta a importância da Autenticidade:

> A autenticidade, consiste na veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações.

Para (FERREIRA e ARAÚJO 2006), ainda adicionam os seguintes conceitos de Segurança da Informação:

> Legalidade: o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos;
>
> Auditabilidade: o acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação;
>
> Não repúdio: o usuário que gerou ou alterou a informação (arquivo ou e-mail) não pode negar o fato, pois existem mecanismos que garantem sua autoria.

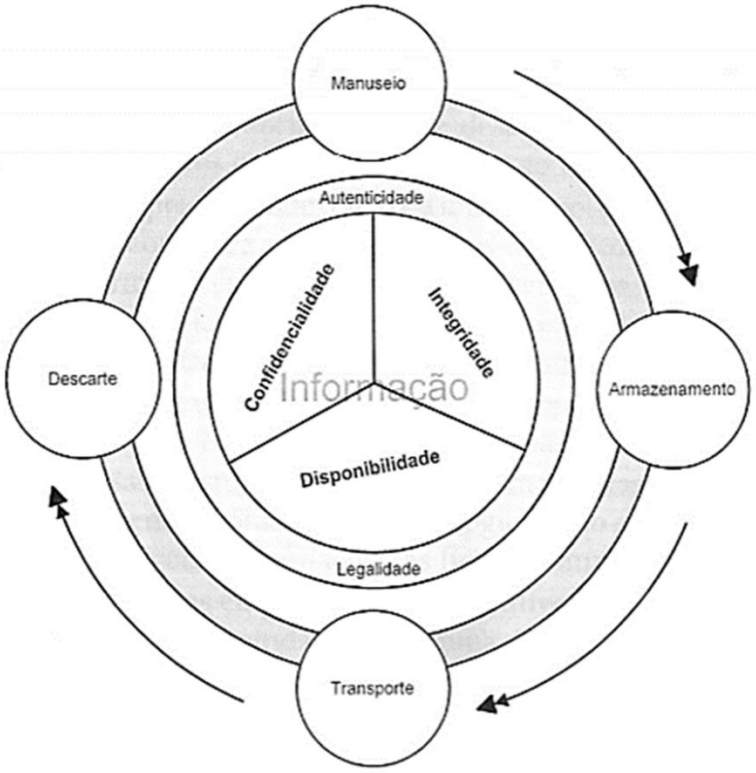
(SÊMOLA 2003), retrata o ciclo de vida da informação e sua interação com os conceitos de segurança, conforme é apresentado na Figura 3.

A importância de se estabelecer e cumprir políticas de segurança, é fundamental para garantir o sucesso com a tramitação de dados, preservando todos os conceitos necessários para as informações, bem como para a empresa. A política de segurança define as medidas que a organização precisa tomar para poder proteger suas informações e refletem o comprometimento da empresa com a segurança.

Para (CAMPOS 2007, p.31):

> As ações de segurança não podem ser apenas alguns procedimentos formais e escritos unicamente para mostrar aos executivos ou para evidenciar em uma auditoria. Devem ser uma filosofia de trabalho, de fato, algo sustentável e de cunho prático. Escrever algumas normas e pendurá-las nos murais, unicamente, não vai garantir a segurança da informação.

Figura 3 - Os quatro momentos do ciclo de vida da informação.



Fonte: SÊMOLA 2003, pag.11.

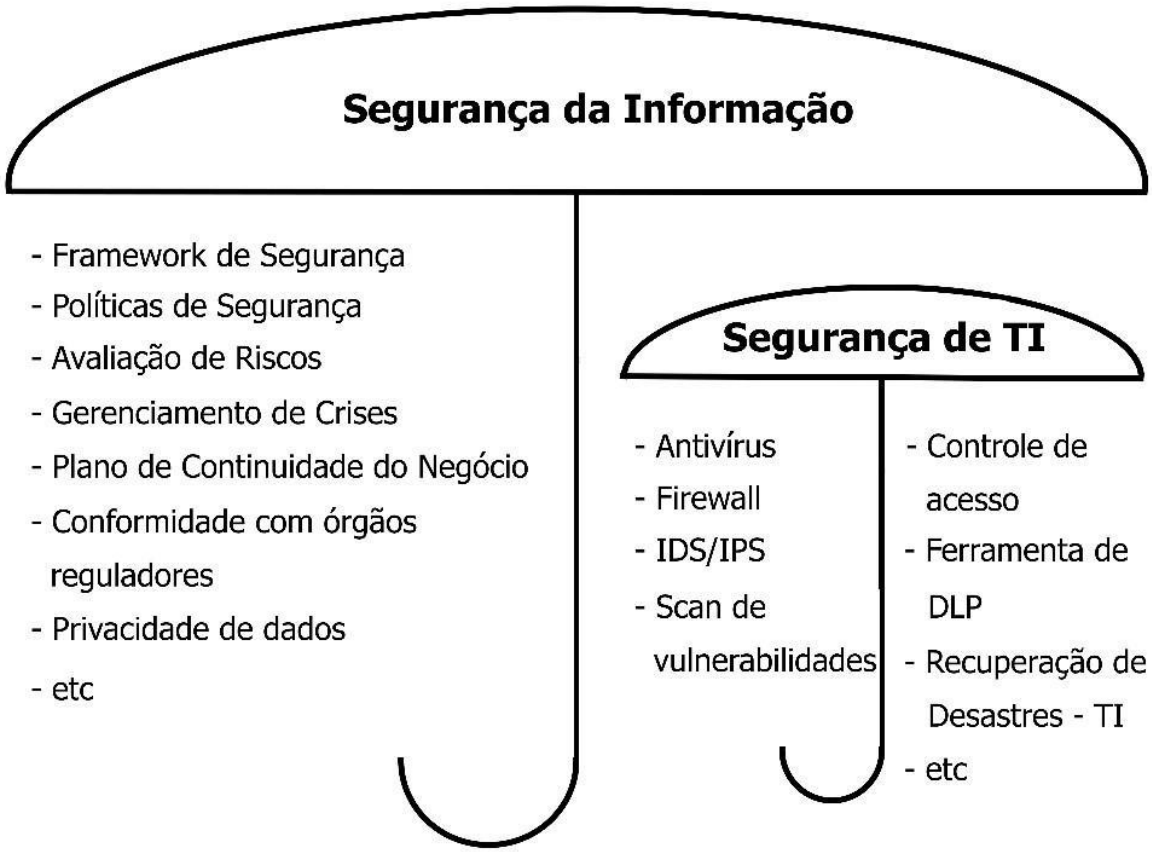
Para (FONTES 2010), uma política de segurança tem como objetivo definir o tratamento que deve ser dado às informações armazenadas, processadas ou transmitidas no ambiente convencional ou no ambiente de tecnologia da organização e que são os princípios fundamentais de como a organização exige que a informação seja utilizada, além de que se aplica a todos os usuários que utilizam as informações da organização. Na Figura 4, é apresentado algumas das responsabilidades corporativas e técnicas da segurança da informação.

O grande impasse que mais ameaça à segurança da informação, são os ataques, acidentais ou intencionais, onde do tipo intencionais alterna entre a observação de dados, através das ferramentas de monitoramento de redes, aos mais complexos e sofisticados com base no funcionamento do sistema. Segundo (NETO 2001), O ataque define-se por usuários que utilizam recursos computacionais de maneira ilícita". O autor classifica alguns tipos de ataques:

- Ataques *DoS* (*Denial of Service*) – O ataque de negação de serviço torna um servidor inoperante sobrecarregando-o excessivamente com solicitações de serviço.

Nesse tipo de ataque é feita uma sobrecarga de pacotes, formando uma quantidade de dados maior que uma rede ou host possa aguentar tornando a rede instável.

Figura 4 - Responsabilidade Corporativas e Técnicas da Segurança da Informação.



Fonte: cryptoid.com.br

Disponível em: < https://cryptoid.com.br/ciberseguranca-seguranca-da-informacao/governanca-de-seguranca-da-informacao-seguranca-de-ti-x-seguranca-da-informacao/ > Acesso Jan.2019.

- Ataques *DoS* (*Denial of Service*) – O ataque de negação de serviço torna um servidor inoperante sobrecarregando-o excessivamente com solicitações de serviço. Nesse tipo de ataque é feita uma sobrecarga de pacotes, formando uma quantidade de dados maior que uma rede ou host possa aguentar tornando a rede instável.
- Ataques *DDoS* - São ataques semelhantes ao *DoS*, tendo como origem diversos e até milhares de pontos disparando ataque, *DoS* para um ou mais sites determinados. Para isto, o invasor coloca agentes para dispararem o ataque em uma ou mais vítimas. As vítimas são máquinas escolhidas pelo invasor por possuírem alguma

vulnerabilidade. Estes agentes, ao serem executados, se transformam em um ataque *DoS* de grande escala.

- Cavalos de Tróia – "é um programa que aparenta ter uma função útil, mas possui alguma função maliciosa que burla os mecanismos de segurança. Não possui a capacidade de se auto replicar. Como exemplo pode-se citar um jogo puxado pela Internet, que na verdade, ao ser executado, tira a atenção do usuário enquanto executa algum dano ao computador ou seus dados em segundo plano"
- Quebra de Senhas - Para obter o acesso é necessário uma senha muitos invasores tentam quebrar estas senhas através de técnicas de quebras de senhas, como tentar as senhas padrões de sistemas ou as senhas simples como nomes pessoais, nome da empresa, datas, entre outros. Mas para facilitar a descoberta da senha, existem diversos programas, como dicionários de senhas e programas que tentam todas as combinações possíveis de caracteres para descobrir a senha.
- *Spoofing* - Nesta técnica, o invasor convence alguém de que ele é algo ou alguém que não é, sem ter permissão para isso, conseguindo autenticação para acessar o que não deveria ter acesso, falsificando seu endereço de origem. É uma técnica de ataque contra a autenticidade, onde um usuário externo se faz passar por um usuário ou computador interno.
- *Sniffer* - é um programa de computador que monitora passivamente o tráfego de rede, ele pode ser utilizado legitimamente, pelo administrador do sistema para verificar problemas de rede ou pode ser usado ilegitimamente por um intruso, para roubar nomes de usuários e senhas. Este tipo de programa explora o fato dos pacotes das aplicações *TCP/IP* não serem criptografados. Entretanto, para utilizar o *sniffer*, é necessário que ele esteja instalado em um ponto da rede, onde passe tráfego de pacotes de interesse para o invasor ou administrador.

Falar em segurança da informação, é pertinente pensar em "Vírus", que são códigos, construídos através de uma linguagem de programação, com objetivos causar danos ao sistema, roubar dados ou alterar o funcionamento normal do sistema. O Vírus tem capacidade de se multiplicar, contaminado outros softwares, instalados nos computadores, por que ele não pode auto executar, precisando de um programa hospedeiro, como exemplos o "*worm*" (verme), ou o "Vírus polimórfico", ele tem a capacidade de se transformar (mutação), confundindo a sua identificação. A Segurança da Informação prevê métodos de Proteção, para prevenir os ataques, invasões e a vulnerabilidade das informações, recursos como o *Firewall*, que tem o objetivo de

proteger a rede local, contra os acessos não indevidos. Estrategicamente está localizado entre a rede local e a internet, controlando o tráfico de informações. Outra importante medida de segurança é a Criptografia, que garante o absoluto segredo e a probidade da informação, normalmente o processo de criptografia é realizado quando a remetente cifra (protege) a mensagem original utilizando um algoritmo de ciframento, com chave privada, reconhecida apenas pelo algoritmo (deciframento) do destinatário (ABNT, 2001).

A questão da segurança da informação deve ser levada muito a sério, sempre tratada como prioridade, em ações preventivas e não apenas em ações corretivas, para isso a organização deve elaborar um plano de contingência definindo claramente suas políticas e metas de segurança, conforme é representado na Figura 5.

Figura 5 - Políticas de Segurança.

Estrutura Baseada na Norma Internacional ISO/IEC 27002

Fonte: Livro Praticando a segurança da informação, Edison Fontes, Editora BRASPORT, 2008.

A questão da Segurança, vai bem além de invasão, roubo, ameaças de terceiros entre outros. Pensar, planejar e proteger as informações de uma organização, é pensar também em falhas humanas, acidentais, defeitos em equipamentos e fenômenos naturais como um incêndio, que poderá destruir a base de dados, danificado os equipamentos. Neste caso a inclusão de um plano para as cópias de segurança "*Backups*", são de extrema relevância na abrangência da proteção dos dados. A cópia de segurança (*Backup*) certifica a disponibilidade dos dados da empresa, sendo necessário planejá-lo, e esse planejamento inclui desde o tipo de mídia para o

armazenamento de dados (fitas magnéticas, discos óticos e web backup), os tipos de *backup*, entre eles o "*Backup Full*", que é o backup de todos os arquivos. Outro tipo é o "*Backup* Incremental", onde primeiramente verificasse o horário das alterações do arquivo, e realiza-se a cópia do mais recente, desde o horário da sua última alteração.

Ainda como critério de segurança da informação, teremos que ter um perfeito controle de acesso, tanto fisicamente como logicamente, ou seja, na parte física, quem poderá utilizar os computadores da empresa, ter acesso às informações privilegiadas, acesso aos códigos do sistema, backups e privilégios. Já na parte lógica, quem usará o sistema, os níveis de permissão, para poder alterar e excluir dados, bem como um forte controle de *Login* e Senha, utilização de assinatura digital e certificação digital expedida pelo uma certificadora autorizada (ABNT, 2001).

Em geral recomenda-se uma série de cuidados, como instalação de antivírus, instalação física como portas corta fogo, *nobreaks*, salas refrigeradas com aparelhos de ar-condicionado, câmeras de Vigilância, entre outros. Neste cenário retrata-se a importância da segurança da informação, proteger o maior patrimônio de uma corporação, não representa apenas um dever e sim uma questão de qualidade na busca de melhorias contínuas e sabedoria na aplicação dos recursos tecnológicos (ABNT, 2001).

3 INTERNET DAS COISAS

Após o surgimento da grande rede mundial de computadores a "Internet" e sua consolidação, e juntamente com o enorme crescimento da telecomunicação, principalmente com a conexão *TCP/IP*, surge no ano de 1999, o termo "Internet das Coisas" - *Internet of Things (IoT),* sua proposta é de conectar diversos dispositivos (em diferentes plataformas) através do ambiente web, num panorama em que várias coisas estão conectadas e se comunicam. (ASHTON 2009) utilizou o termo "*Internet of Things*" (*IoT*) pela primeira vez em uma apresentação que ele fez na *Procter & Gamble* (*P&G*) para relacionar a ideia de *RFID* (*Radio Frequency Identification*) com a cadeia de suprimentos da *P&G*. Para (ASHTON 2009), seria necessário "empoderar" os computadores para que eles mesmos pudessem coletar e lidar com as informações, fosse por *RFID* ou por demais tecnologias de sensores, sem as limitações do homem. De modo geral, *IoT* passou a ser identificada como a possibilidade de conexão do mundo físico com o mundo digital.

A evolução desse conceito (*IoT*), começou a conectar qualquer meio físico ao virtual, de acordo com (VALENTE 2011), "é um paradigma que tem por objetivo criar uma ponte entre acontecimentos do mundo real e as suas representações no mundo digital, por meio da conexão de objetos". A ideia de "tudo" poder se conectado a "tudo", remete-se a sistemas embarcados adicionados a computação nas nuvens, aos grandes armazenamentos de dados em *Big Data* e a própria Internet, essa inovação tecnológica, embora muito recente, ganhou o mundo e está aplicada em todos os segmentos e produtos. Para muitos, a *IoT*, é coisa futurísticas, com nos desenhos animados, especialmente "*The Jetsons*", apresentados nos anos de 1985, onde os personagens *George*, *Jane*, *Judy*, *Elroy*, *Rosie* e *Astro*, viviam no futuro (precisamente no ano de 2062), a sua tecnologia era aplicada em Carros voadores, videofones (com chamadas feitas até pelo relógio de pulso) e eletrodomésticos inteligentes, empregada-robô e outros, como pode relembrar a Figura 6. Porém em uma análise bem simplificada, através da internet das coisas, já se começou a viver esse futuro, ou seja, se examinarmos a tecnologia ao nosso redor teremos, como exemplo, câmeras e sensores nos automóveis, geladeiras capazes de detectar um produto com data próxima ao vencimento, ou até mesmo se precisa ser reposto. A pulseira inteligente que auxiliam monitoramento da saúde, registrando os movimentos, é armazenado em um aplicativo de celular, posteriormente os dados coletados são analisados e assim podemos efetuar avaliações das atividades físicas praticadas. Vários dispositivos criados que podem se integrar ao smartphone.

Figura 6 – ANO 1960 *SMARTWATCH*.

Fonte: screenrant.com
Disponível em: <https://screenrant.com/times-the-jetsons-predicted-the-future/> Acesso Jan.2019.

Carros elétricos e autônomos, que oferecem um completo *check-up* e dados de geolocalização, Meios de Pagamento, através do uso do celular ou de relógios e pulseiras, com a tecnologia de *NFC*, (*Google Pay*), que efetua a unificação de diversas formas de pagamento em um só ambiente, como no exemplo da Figura 7, o *smartwatch*, seguem na lista dos exemplos.

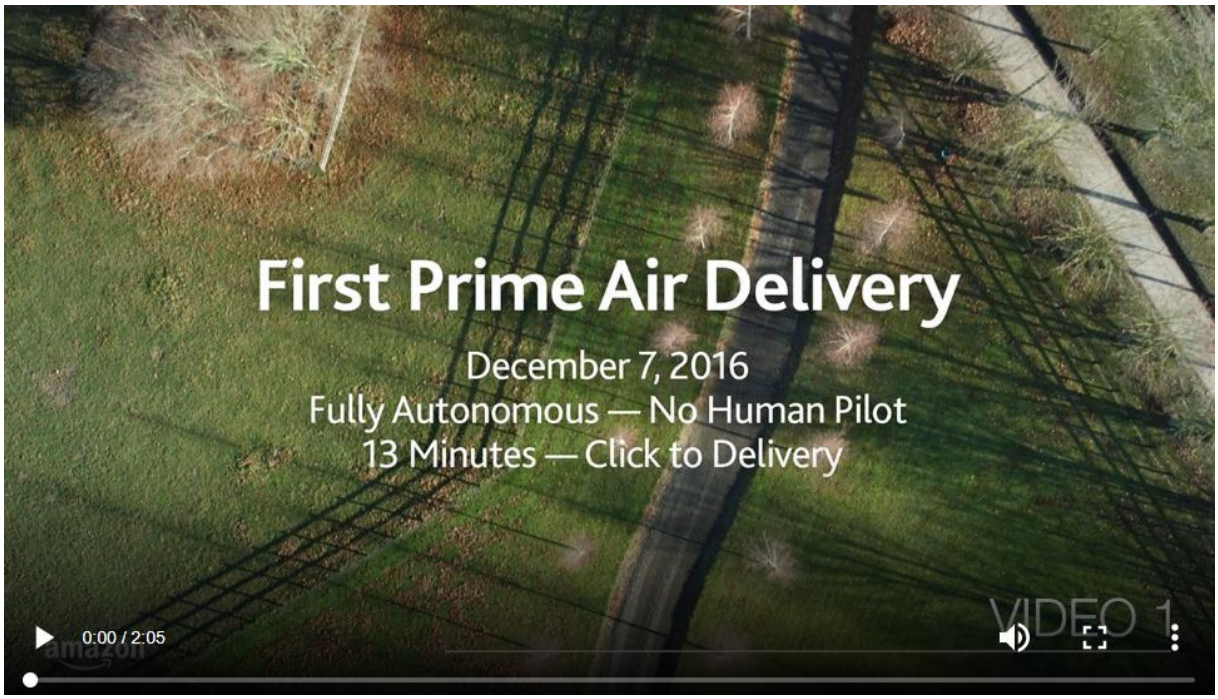
Figura 7 - Aplicação da Internet das Coisas – *Smartwatchs*

Fonte:betakit.com

Disponível em: <https://betakit.com/ww-the-wearable-weekly-2017-is-the-year-of-the-smartwatch/> Acesso Jan.2019.

Drones, que por muitos são considerados como um brinquedo, porém sua aplicação vai muito mais além, atuando nas áreas de negócio, podem ser usados para filmagens, monitoração, fotos aéreas para composição de imagens, entregas de produtos, como o caso da *Amazon*, no dia 7/12/2016 realizou a sua primeira entrega de produtos usando um drone conforme demostra no link do vídeo na Figura 8.

Figura 8 - *First Prime Air Delivery*



Fonte: Youtube.com

Disponível em: < https://www.youtube.com/watch?v=vNySOrI2Ny8> Acesso Jan.2019.

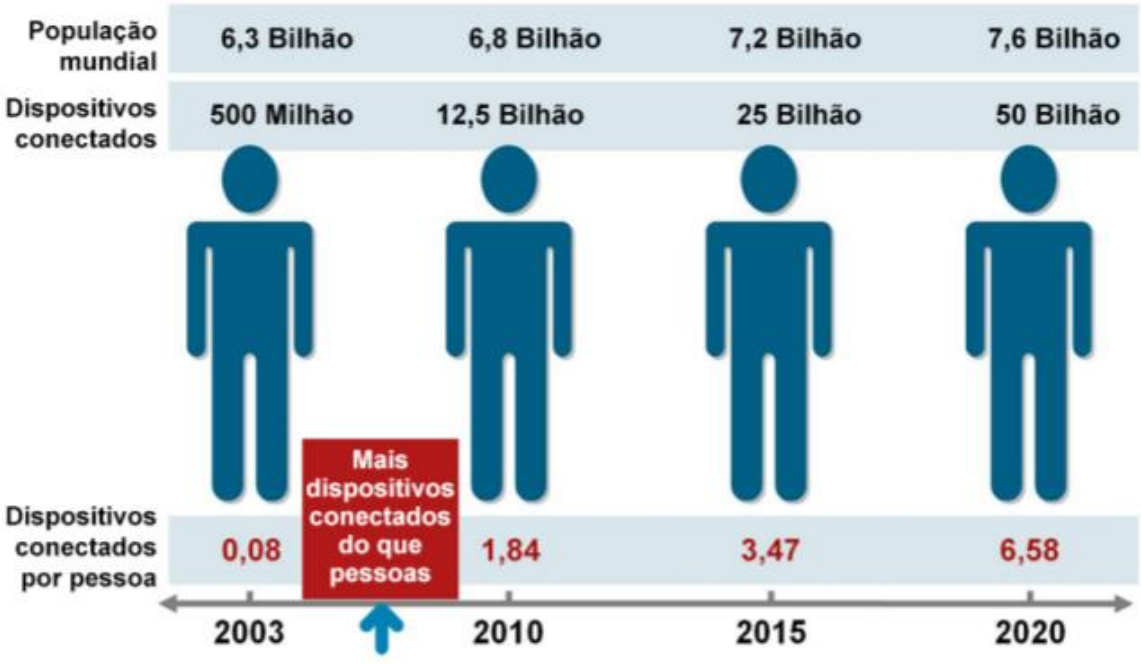
Comprovadamente a Internet das Coisas, é uma tecnologia inovadora em amplo desenvolvimento, em todos os setores e segmento, aplicações e entendimentos, de acordo com a projeção da *Gartner*, até o ano de 2022, teremos 21 bilhões de "coisas" conectadas com internet, já para empresa de tecnologia CISCO, a estimativa é bem maior, sua aposta é que em 2020, teremos 50 Bilhões de coisas conectadas, ultrapassando o número de habitantes do planeta, como pode ser observado na Figura 9.

O Brasil está presente no cenário mundial, entre os países que utilizam a IoT, é gerenciado pela ABINC (Associação Brasileira de Internet das Coisas), e se prepara para transformações que possam permitir, sua aplicação em diversas áreas, entre elas a da saúde, educação, segurança pública, energia, logística e varejo, sempre objetivando uma melhoria

relacionamento com cliente e na qualidade do atendimento e serviços prestados. (SANTOS et. Al 2016), define a IoT, como:

> A Internet das Coisas, em poucas palavras, nada mais é que uma extensão da Internet atual. Esta extensão é feita ao proporcionar que objetos do dia-a-dia (quaisquer que sejam) se conectem à Internet. A conexão com a rede mundial de computadores viabiliza, primeiro, controlar remotamente os objetos e, segundo permitir que os próprios objetos sejam acessados como provedores de serviços. Estas novas habilidades, dos objetos comuns, geram um grande número de oportunidades tanto no âmbito acadêmico quanto no industrial. Todavia, estas possibilidades apresentam riscos e acarretam amplos desafios técnicos e sociais.

Figura 9 - Número de Dispositivos X Número de Pessoas



Fonte: Cisco IBSG, 2011.

Conforme o pensamento do autor, a Internet das Coisas, é a própria evolução natural da internet, (EVANS 2011), apresenta a diferenciação entre a Internet tradicional e o *IoT*:

> A Internet é a camada ou rede física composta por switches, roteadores e outros equipamentos. Sua função primária é transportar informações de um ponto a outro de forma rápida, confiável e segura. Por outro lado, a Web é uma camada de aplicativos que opera sobre a

> Internet. Sua função primária é oferecer uma interface que transforma as informações que fluem pela Internet em algo utilizável.

Ainda segundo (EVANS 2011), é preciso conhecer e entender a evolução da Internet, como pode ser acompanhado pela Tabela 1, para se ter uma melhor compreensão do momento atual da nova conectividade.

Tabela 1 - Evolução da Internet

FASE	PERÍODO
1	Primeiro veio a fase de pesquisa, quando a *Web* foi chamada de *ARPANET* (*Advanced Research Projects Agency Network*). Nesse período, a *Web* foi usada principalmente pelo meio acadêmico para pesquisas.
2	A segunda fase da Web pode ser chamada de "panfleto *ware*". Caracterizada pela "corrida do ouro" dos nomes de domínio, essa etapa se concentrou na necessidade de quase todas as empresas de compartilharem informações na Internet para que as pessoas pudessem saber sobre seus produtos e serviços.
3	A terceira evolução mudou a *Web* de um patamar de dados estáticos para um de informações transacionais, nas quais produtos e serviços podem ser comprados e vendidos, assim como era possível oferecer serviços. Nessa fase, as empresas como o eBay e a Amazon.com explodiram no cenário. Essa fase também será lembrada como o crescimento e a explosão da bolha "ponto com".
4	A quarta fase, onde estamos agora, é a *Web* "social" ou de "experiência", na qual as empresas como *Facebook*, *Twitter* e *Groupon* se tornaram famosas e rentáveis (uma distinção notável da terceira etapa da *Web*) ao permitir que pessoas se comuniquem, conectem e compartilhem informações (textos, fotos e vídeos) sobre si mesmos com amigos, família e colegas.

Fonte: Cisco IBSG, 2011.

4 COMO FUNCIONA A INTERNET DAS COISAS

A diversidade dos recursos tecnológicos, integra e viabiliza a utilização da *IoT*, em diversos espaços físicos, assim a classe é composta por blocos, que são, Identificação, primordial para detectar os objetos que serão utilizados para conectá-los à Internet. Entre esses identificadores destaca-se *RFID, NFC* (*Near Field Communication*) e endereçamento *IP*. Os sensores (Atuadores), ficam com a responsabilidade de coletam informações, e armazenar e/ou encaminhar os dados para as bases de dados, *clouds* ou *data centers*. Assim os agentes controlam o cenário segundo o recebimento das informações. O crivo da Comunicação, é referente às técnicas de conexão dos objetos, com o importante papel no consumo de energia, normalmente são utilizadas *WiFi*, *Bluetooth*, *IEEE* 802.15.4 e *RFID*. Referente a configuração da computação, está incluído a unidade de processamento, (microcontroladores, processadores e *FPGAs*), responsáveis por executar algoritmos locais nos dispositivos. De acordo com (MAXFIELD 2004). Um *FPGA* é um dispositivo lógico programável, apresentado como circuito integrado, que contém matrizes de blocos lógicos, com interconexões configuráveis, chamados *CLBs* (*Configurable Logic Blocks*), organizados de tal maneira que um desenvolvedor possa programá-los para executar uma ampla gama de tarefas.

O segundo bloco, é o de Serviços, com a missão de prover diversas classes de serviços, desde Serviços de Identificação, que são responsáveis por mapear as Entidades Físicas (EF) nas Entidades Virtuais (EV), controle como a temperatura, coordenadas geográficas; Assim todos os serviços de Agregação de Dados, utilizados para coletar e totalizar dados (homogêneos/heterogêneos), obtidos a partir dos Dispositivos ; Serviços de Colaboração e Inteligência, cuja a ação é sobre os serviços de agregação de dados, possibilitando a tomada de tomar decisões e reagir de modo adequado, conforme determinado cenário; Serviços de Ubiquidade, tem a finalidade específica de prover serviços de colaboração e inteligência há todo momento, independente do lugar. A conclusão da Semântica, é habilidade de extração de conhecimento dos dispositivos da Internet das Coisas, irá cuidar das descoberta e conhecimento, bem como o uso eficiente dos recursos inerentes na Internet das Coisas, são aplicadas diversas técnicas, em destaque o *Resource Description Framework* (*RDF*), *Web Ontology Language* (*OWL*) e *Efficient XML Interchange* (*EXI*), (ZAIDAN 2014).

Especificamente falando sobre as tecnologias de comunicações e suas características mais relevantes. Como o Ethernet. O padrão Ethernet (*IEEE* 802.3), *Wi-Fi*, essa tecnologia permite a solução para a comunicação sem fio, o *ZigBee*. Baseado na especificação do protocolo *IEEE* 802.15.4 para a camada de enlace, suas características são a baixa vazão,

reduzido consumo energético e baixo custo. O *Bluetooth Special Interest Group* tecnologias de rede sem fio para *PANs – Personal Area Networks*, aplicada para os *smartphones*, *headsets*, Pcs entre outros. Cabe destaque especial para os padrões tecnológicos da telefonia celular 3G/4G, muito utilizado na *IoT*, podem alcançar grandes distâncias, aproveitando a infraestrutura das redes de telefonia celular 3G/4G. Conforme Tabela 2, pode se observar a tecnologia e suas características.

Tabela 2 - Comparação das Tecnologias de Comunicação

Protocolo	Alcance	Frequência	Taxa	IPv6	Topologia
Ethernet	100/2000 m	N/A	10 Gbps	Sim	Variada
Wi-Fi	50 m	2.4/5 GHz	1300 Mbps	Sim	Estrela
BLE	80 m	2.4 GHz	1 Mbps	Sim*	Estrela/Mesh
ZigBee	100 m	915 MHz/2.4 GHz	250 kbps	Sim	Estrela/Mesh
3G/4G	35/200 km	1900/2100/2500 MHz	1/10 Mbps	Sim	Estrela
SigFox	10/50 km	868/902 MHz	10–1000 bps	–	–
LoraWan	2/5 km	Sub-GHz	0.3-50 kbps	Sim	Estrela

Fonte:homepages.dcc.ufmg.br
Disponível em: <https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/internet-das-coisas.pdf> Acesso em 10 Fev.2019.

A Modelagem de dados, coletados por sensores, raramente possuem uma padronização hierárquica, (relacionamentos ou mesmo um formato padrão), para sua utilização, assim os softwares de modelagem, permitem utilizar esses dados, de forma compatível e interoperabilidade, ajustando-os para formatos de padrões interpretáveis. O real objetivo da modelagem é definir um padrão unificando atributos, características as conforme o domínio da aplicação, suas representações são *key-value*, *markup scheme*, *graphical*, *object based*, *logic based* e *ontology based modeling*. Sua aplicabilidade tem uma variação de acordo com o domínio da aplicação, “A representação os dados são modelados como um conjunto de chaves e valores em arquivos de texto, representação da informação, que, ela possui complexidade de organizar e recuperar quando o volume de dados aumenta” (BETTINI 2010).

5 A SEGURANÇA DA INFORMAÇÃO EM IOT

Com a ampla possibilidade de ter conexão em qualquer ambiente, aumenta consideravelmente as possibilidades de comunicação, interação, serviços e recursos provindos da *Web*, porém do outro lado da moeda, também existe o aumento da vulnerável a um ataque, próprio Departamento Federal de Investigação, o "*FBI*", com sede *Washington – EUA*, com a missão de investigação de crimes de âmbito federal, em nota oficial, faz esse alerta a população, orientando sobre as possibilidades de ataque de hackers em ambientes *IoT*. A falta de privacidade, sendo que todas as coisas tem (ou terão), acesso à Internet, como por exemplo as TV's, geladeiras, automóveis, entre outros, fará com que se produza uma quantidade enorme de dados, que consequentemente serão armazenados em banco de dados e de acordo com as políticas de segurança aplicadas poderão deixar portas abertas para ataques. Conforme explica (BALAGUER 2015):

> Com a rápida expansão da utilização da Internet das Coisas em todo o mundo, além da crescente disseminação de malwares para todo tipo de hardware e software (sejam sistemas operacionais ou aplicativos), a preocupação com a Segurança da Informação (dados pessoais e corporativos) também deve seguir entre as principais prioridades da indústria de Tecnologia da Informação.

A gravidade dessa situação é potencializada quando se trata de pessoas físicas, usando equipamentos pessoais, (JUNIOR 2016), analisa esse risco.

> Como milhões de novos dispositivos passam a estar conectados, é inevitável que algumas pessoas levem seu gadgets para o ambiente de trabalho. Caso se conectem à rede da empresa, é natural que aquele objeto passe a ser mais um *endpoint*, ou seja, mais uma porta de entrada para vírus e malwares.

Se para as pessoas físicas a probabilidade de riscos, são maiores, no caso corporativo os prejuízos são incalculáveis, conforme (AYOYAN 2015), orienta:

> Um dos problemas levantados em discussões dessa natureza tem a ver com a forma como esses objetos serão gerenciados dentro da crescente infraestrutura de TI do futuro não muito distante. Há algum tempo, as infraestruturas empresariais móveis eram bastante simples – dispositivos *Blackberry* eram a novidade. Em seguida, graças ao

> lançamento de smartphones populares e da "consumerização de TI", alguns funcionários iniciantes começaram a utilizar seus próprios smartphones, tablets e outros dispositivos pessoais no trabalho. Logo, todo mundo aderiu à prática. O *BYOD* tornou-se generalizado, apesar de uma série de novas dores de cabeça para as empresas antes de finalmente chegarem a um consenso.

Analisando os inúmeros riscos e as vulnerabilidades em dispositivos *IoT*, torna-se cada vez mais comum, e ameaçador principalmente porque erros cometidos por fabricantes de dispositivos que ainda não estão familiarizados com as práticas de segurança, conforme relata (ZANI 2016):

> Os dispositivos de Internet das Coisas muitas vezes não são projetados para a segurança. A maioria dos dispositivos não tem uma abordagem coordenada de segurança de rede, não exigem senha ou não se preocupam com complexidade das mesmas, armazenam informações pessoais e contém diversas vulnerabilidades. A proliferação de novos dispositivos, a baixíssima preocupação com segurança e alto valor dos dados contidos nesses objetos farão com que os ataques cibernéticos visando esses dispositivos cresçam de forma abundante.

Os erros de fabricantes, no sentido de não acompanhar a rapidíssima evolução da Internet das Coisas, como por exemplo adicionar as funcionalidades IP a seus dispositivos, com o objetivo de obter maiores informações sobre o dispositivo, ou no caso dos níveis de privilégios, estabelecer senhas padrões. Tratando desses dispositivos, podemos cauteriza-los em três agrupamentos conforme as funções exercidas:

1º) Dispositivos para coleta de informações, via sensores, transmitindo essas informações constantemente.

2º) Dispositivos para receber informações coletadas, pelo primeiro grupo via internet.

3º) Dispositivos específicos, que representa a junção dos demais grupos, coleta e recebe informações.

Nesses grupos, a reflexão é focada na prerrogativa da segurança da informação, pois como descrito anteriormente, a grande maioria dos fabricantes, preocupam se primordialmente

com a questão da funcionalidade do próprio dispositivo, deixando em segundo plano ou de forma inexistente a segurança da informação (GOMES 2016).

Como por exemplo um fabricante de dispositivo para rastreamento veicular, cuja o foco é fornecer informações em tempo real sobre a localização do veículo, roteiro, velocidade e demais indicadores, dentro do conceito para atender as necessidades específicas do produto. Não considerando a possibilidade que um terceiro também possa ter interesse em rastrear essas informações, coletadas e armazenadas. Observa-se que em geral os dispositivos para *IoT*, são possíveis alvos de ataques de negação e serviço *DDoS*, causando danos seríssimos aos dispositivos e em certos casos até parando o funcionamento do serviço realizado pelo dispositivo. Um exemplo dessa situação ocorreu no final do ano de 2017, onde a *Spotify*, *Netflix*, *Twitter*, *Tumblr*, *CNN* e *Reddit*, tiveram seu site temporariamente fora do ar, devido ao "*Dyn*", um provedor de internet, ter sido invadido por *hackers*, durante a investigação do problema, verificou-se eles utilizaram os sistemas de câmeras de segurança, conectados à internet, forçando o acesso ao site do *Dyn*, o ataque *Distributed Denial of Service* (*DDoS*) em português, Distribuído de Negação de Serviço, congestionou o sistema e o serviço saiu fora do ar (KURTZ 2016).

Todo a problemática gira em torno de novas formas de conexão de dispositivos, que efetua a coleta e recebimento de dados pessoais dos usuários para as empresas, que oferecem diversos serviços, entre eles a vigilância, de acordo o exemplo citado, esse serviço de vigilância também pode ser residencial, por isso a administração dos dados pessoais, se torna o fator mais crítico, a situação piora no Brasil, pois não há uma legislação específica para proteção de dados pessoais. No ano de 2016, foi criado pela Câmara dos Deputados, uma PL 5.276/2016, que dispõe sobre o tratamento de dados pessoais, porém os trabalhos não avançaram e segundo a própria Câmara dos Deputados:

> "O documento é muito claro ao dizer que, se não houver a edição de uma lei de proteção de dados no Brasil, permanecerá no país uma insegurança jurídica, diante de uma diversidade de interpretações que se possa ter sobre a proteção de dados, a partir de um conjunto de legislações",

A ação de órgãos regulatórios, vem trabalhando nesse sentindo em busca de soluções plausíveis, como é o caso da ABINC, porém diante de diversos conflitos existentes a solução está longe de ter um consenso, relação às especificações de segurança dos dispositivos da Internet das Coisas. Em outros países como na Europa, a legislação trabalha com essa situação

há mais de 20 anos. Incontáveis ameaças cercam o desenvolvimento da *IoT,* como a utilização de Interface web insegura, mecanismo de autenticação fraca ou em certos casos até insuficiente, falta de criptografia, interface móvel e em nuvem com configurações de segurança que deixem os softwares vulneráveis. Outra porta aberta para os ataques, são os próprios usuários, que por inexperiência ou descuido não utiliza os devidos padrões de segurança para sua proteção, na maioria dos casos são atitudes simples, tanto on e off-line que os tornam vulneráveis.

Segundo (*BUSINESS INSIDER* 2017), é preciso considerar 3 abordagens:

- Visibilidade: as imagens de ameaças, dispositivos, aplicações e dados, bem como a relação entre esses elementos, devem ser visualizadas em tempo real para que o processo seja inteligente. Essa medida requer controles dinâmicos, que realizem a automação e a análises para a tomada de decisões;
- Consciência da ameaça: a capacidade de identificar malwares e vulnerabilidades deve ser aprimorada e tomar por base o comportamento anormal ou normal. Além disso, deve ser feito o mapeamento dos indicadores e tomar decisões rapidamente. Assim, é possível ir além da complexidade e da fragmentação dos ambientes;
- ação: a presença de ameaças e comportamentos anormais exigem alguma ação. Para isso, é necessário contar com tecnologias, pessoas e processos que atuem em conjunto.

O excesso de dados gerados na tecnologia *IoT,* sem a menor margem de dúvida é enorme, foi apresentado na (*BUSINESS INSIDER* 2017), através de um relatório da *Federal Trade Comission,* os indicadores mensurando que a cada 10.000 é produzido 150 milhões de *Data Points* diariamente. O significado real dessa informação é que cada um desses pontos de dados, pode ser transformar em uma forma de acesso aos *hackers*, aumentando ainda mais vulnerabilidade às informações.

O recorde apresentou como a espionagem, via dispositivos inteligentes, utilizados na *IoT,* ficam mais vulneráveis e fáceis de serem invadidos por hackers, alguns exemplos desta realidade, pode ser sua própria *smart TV,* imagine que exista outra conexão em sua casa, e que você realiza algumas tarefas do seu dia a dia, como em sua moradia, assim quanto mais *Data Points*, existirem maior será o seu risco de espionagem. A princípio não existe uma solução mágica ou estratégica para acabar com o risco eminente, somente a utilização de condutas corretas das práticas de políticas de segurança da informação, serão eficientes para reduzir os riscos e proteger o bem mais valioso das pessoas e empresas, que são as informações. Adotar

as políticas em sua totalidade, e conscientizar que a segurança é uma responsabilidade de todos, melhora significativamente a quantidade e qualidade de dados, dando margens para privacidade e criando um cenário ideal para a utilização da Internet das Coisas, que muito tem que evoluir nesta questão tão prioritária. Pode-se observar na Figura 10 a variedade de *data points* em um mesmo ambiente.

Figura 10 – Smart House

Fonte: energiainteligenteufjf.com
Disponível em: <http://energiainteligenteufjf.com/como-funciona/como-funciona-internet-das-coisas/> Acesso em 10 Fev.2019.

6 DESAFIOS E BARREIRAS DA IOT

A cada momento uma inovação tecnológica, surpreende o mundo. Porém, para perfeita utilização das tecnologias modernas, um arcabouço de infraestruturas, pesquisas, interconexão, recursos tecnológicos, segurança e investimentos, tem que ser disponibilizados, acompanhando e oferecendo condições ideais para o seu perfeito funcionamento. Recursos responsivos, sensoriais, inteligentes e eficientes, que representam, na sua maioria, grandes desafios e barreiras quase intransponíveis. No caso da Internet das Coisas, a situação não é nada diferente, como descrito durante o presente estudo. Sua maior fragilidade é a questão da vulnerabilidade, afetando diretamente sua segurança, entretanto, infelizmente essa modernidade não tem apenas esse problema. (FREDERIC 2019) comenta sobre os vários desafios da *IoT*, e destaca que dentre as principais vulnerabilidades da Internet das Coisas, pode-se ter:

- A Privacidade do consumidor – Os equipamentos de medição inteligente totalmente digitais, gera um enorme volume de dados, fornecendo praticamente todos os tipos de informações pessoais nos dispositivos, expondo de maneira ampla a privacidade pessoal do seu usuário.
- Dados - A *IoT*, gera profundos impactos no armazenamento de dados, tanto aos dados que serão armazenados (de consumidores), como os dados que serão processados, analisados e distribuídos pelas empresas através de sistemas de mineração de dados (*Big Data*), normalmente esses dados serão gerados, em tempo real , na medida em que os consumidores utilizam seus *Apps* e os dispositivos. Neste contexto os desafios de segurança, permanece sendo o principal desafio, pois partir da utilização de inumeráveis dispositivos, maximizará o aumentará da dificuldade de segurança.
- Gestão de armazenamento – A infraestrutura de armazenamento, representa outro dificultador, que necessita de uma crescente capacidade, pois o negócio é capaz de coletar e usar cada mais dados, oriundos da *IoT*.
- Tecnologias de servidores – Como ressaltado grandes tecnologias necessitam de grandes recursos com a impacto da Internet das Coisas, os servidores devem acompanhar seu crescimento, em todos os seus segmentos chave.
- Rede de *Data Center* - Os *links WAN* nos data centers são dimensionados para as necessidades de largura de banda moderada, geradas por interações humanas com aplicações. A Internet das Coisas deve mudar esses padrões ao transferir grandes volumes de dados de sensores de mensagens pequenas ao data center para

processamento, aumentando as necessidades por largura de banda de entrada no data center.

A Figura 11, reporta uma importante informação, sobre a produção de informações online, no mundo a cada 60 segundos, ou seja, isso representa a quantidade de informação produzida, compartilhada e armazenada por aplicativos. O que reforça ainda mais a questão da infraestrutura e principalmente a importância da Segurança da Informação.

Figura 11 - O que acontece online em 60 segundos

Fonte: Página smartinsights.com.
Disponível em: http://www.smartinsights.com/internet-marketing-statistics/happens-online-60-seconds/ Acesso Jan.2019.

CONCLUSÃO

Graças a contribuição de diversos autores e suas obras, observamos que a *IoT*, sem dúvida é um enorme salto das tecnologias e inovações. Seus resultados são de grande relevância e melhoria para qualidade de vida das pessoas e corporações. Também foi possível realizar uma ampla reflexão sobre o importante papel da Segurança da Informação, os benefícios que sua aplicação de modo corretor podem oferecer para os usuários da *IoT*. As políticas de Segurança da Informação, devem ser respeitadas, pois conforme demonstrado no presente estudo o alto risco de vulnerabilidade existentes nos dispositivos utilizados para realizar conexões na *IoT*, deixando fragilizados os dados pessoais, para possíveis ataques de *Hackers* e outros tipos de criminosos virtuais. Um exemplo é a Lei dos Crimes Cibernéticos (Lei 12.737/2012), conhecida como Lei Carolina Dieckmann, que tipifica atos como invadir computadores (*hacking*), roubar senhas, violar dados de usuários e divulgar informações privadas como fotos, mensagens etc.

Essa tecnologia transforma-se em uma parceria e lucrativa para todos os setores, tanto na área profissional como pessoas, pois durante esse estudo foi apresentado indicadores que comprovam o número cada vez maior de usuários da internet, que utilizam os serviços *Web*, principalmente através de dispositivos, como o celular. Assim enxergamos a *IoT*, com a tecnologia do século e cada vez mais, está em fase de expansão, pois mesmo com todos os problemas relatados, a resolução proposta por estruturas de segurança da informação.

Observa-se que, para a Internet das Coisas, caminhar com o menor número de dificuldades e vulnerabilidades possíveis, é necessária uma conscientização coletiva, os fabricantes de dispositivos, até o usuário final, que a Segurança da Informação é um o fator principal a ser considerado. Cientes que ainda existe uma longa estrada para se percorrer, melhorando critérios de infraestrutura, gerenciamento de dados coletados através dos dispositivos de conexão, os próprios dispositivos de conexão, os softwares, os mecanismos da segurança da informação e a legislação brasileira sobre os crimes virtuais.

Os avanços tecnológicos são inquestionáveis, cada vez mais presente no dia a dia, modificando o comportamento das pessoas, o modo de fazer compras, interagir, fazer amizades, ver filmes, ler notícias e principalmente a forma de se informar. Os dois lados da moeda, todos os seguimentos comerciais estão na era digital, empresas de todas as naturezas e portes, utilização os recursos da tecnologia para conquistar novos clientes, e melhorar a qualidade de seus serviços e produtos. Pensar em inovação tecnológica é olhar para o futuro, pois hoje a internet deixou de conectar apenas computadores, para conectar pessoas, a evolução das tecnologias permite essa conectividade em inúmeros tipos de dispositivos, a “Internet das

Coisas", facilitando a interação e gerando enormes benefícios para a população. Esse presente estudo visa analisar pontos fundamentais sobre a Internet das Coisas internet, sua tecnologia, vantagens e desvantagens. Essa análise sobre *IoT*, será mensurada pela Segurança da Informação, onde busca-se uma reflexão sobre a vulnerabilidade e critérios de segurança na *IoT*.

REFERÊNCIAS

ABNT. NBR ISO/IEC 17799 - Tecnologia da informação: código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2001.

ABNT. NBR ISO/IEC 27002 - Tecnologia da informação: código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2001.

AMAZON PRIME AIR'S FIRST CUSTOMER DELIVERY Amazon. Youtube. 14 dez. 2016. 3min54s. Disponível em: < https://www.youtube.com/watch?v=vNySOrI2Ny8> Acesso em 10 Fev.2019.

ASHTON, Kevin. That 'Internet of Things' Thing. 2009. Disponível em: <http://www.rfidjournal.com/articles/view?4986> Acesso em 10 Fev.2019.

AVOYAN, Hovhannes. Por que a Internet das Coisas vai transformar a gestão de dispositivos móveis. Disponível em:<https://www.monitis.com/blog/why-internet-of-things-will-transform-mobile-device-management/>. Acesso em 10 Fev. 2019.

BALAGUER, Adriano. Segurança da Informação no mundo da Internet das Coisas, Disponível em: < https://computerworld.com.br/2015/02/25/seguranca-da-informacao-no-mundo-da-internet-das-coisas/> Acesso em 05 Fev. 2019.

BUSINESS Insider Disponível em: < https://www.businessinsider.com/internet-of-things-security-privacy-2016-8?u> Acesso em 05 Fev. 2019.

CAMPOS, André. Sistemas de Segurança da Informação: Controlando os riscos. 2 ed. Florianópolis: Visual Books, 2007.

CISCO, Número de Dispositivos X Número de Pessoas disponível em: <https://www.cisco.com/c/dam/global/pt_br/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf> Acessado em 10-02-2019.

EVANS, Dave. Internet das Coisas: Como a próxima evolução da Internet está mudando tudo. Disponível em: < https://www.coeforict.org/wp-content/uploads/2013/10/Internet-of-Things-author-Michele-Royer-Phd-September-2013.pdf>. Acesso em 11 Fev. 2019.

FERREIRA, F. N. F.; ARAÚJO, M. T. Política da Segurança da Informação: Guia Prático para Elaboração e Implementação. 1. ed. Rio de Janeiro: Ciência Moderna, 2006.

FONTES, Edison. Segurança da Informação: O usuário faz a diferença. São Paulo: Saraiva, 2010.

FREDRIC, Paul 10 principais vulnerabilidades da Internet das Coisas 2019. Disponível em: < https://cio.com.br/10-principais-vulnerabilidades-da-internet-das-coisas/> Acesso em 10 Fev.2019.

GIL, A. C. Como elaborar projetos de pesquisa. 4. ed. São Paulo: Atlas, 2007.

IBGE – Disponível em <https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/20073-pnad-continua-tic-2016-94-2-das-pessoas-que-utilizaram-a-internet-o-fizeram-para-trocar-mensagens acessado em 11-02-2019.

GOMES, Tebaldi. Exemplos e Aplicações de Intert das Coisas (IOT). 02/03/2016. Disponível em: <https://www.opservices.com.br/exemplos-de-internet-das-coisas/> Acesso em 29 Jun.2019.

KURTZ, João Netflix, Twitter, Spotify e Tumblr ficam fora do ar; entenda o caso TECMUNDO. 21/10/2016. Disponível em: <https://www.techtudo.com.br/noticias/noticia/2016/10/netflix-twitter-spotify-e-tumblr focam-fora-do-ar-entenda-o-caso.html> Acesso em 10 Fev.2019.

MALHOTRA, Naresh K. Pesquisa de marketing: uma orientação aplicada. 4ª Ed. Porto Alegre: Bookman, 2004.

MAXFIELD. Clive, Max. The Design Warrior's Guide to FPGAs. Elsevier, 2004. Disponível em: <http://blog.aku.edu.tr/ismailkoyuncu/files/2017/04/01_ebook.pdf> Acesso em 10 Fev.2019.

NETO, Amaro Moraes e Silva. Privacidade na internet um enfoque jurídico Edi pro, 2001

PRODANOV, C. C.; FREITAS, E. C. D. Metodologia do trabalho científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico. 2ª. ed. Novo Hamburgo: Universidade Freevale, 2013.

SANTOS ET AL. SANTOS, B. P., M. VIEIRA: A centrality-based and energy efficient collection protocol for low power and lossy networks. In Computer Networks and Distributed Systems (SBRC), 2015 XXXIII Brazilian Symposium on, pages 159–170. IEEE.

SÊMOLA, M. Gestão da Segurança da Informação, Uma visão executiva. 7. ed. Rio de Janeiro: Elsevier, 2003.

TAURION, Cezar. Tecnologias emergentes: Mudança de atitude e diferenciais competitivos nas empresas. Évora, 30 de agosto de 2017

VALENTE, Bruno Alexandre Loureiro. Um middleware para a Internet das coisas. 2011.

VERGARA, Sylvia C. Projetos e relatórios de pesquisa em administração. 3.ed. Rio de Janeiro: Atlas, 2000.

ZANI, Bruno. As vulnerabilidades e necessidades de segurança em IoT. 29/09/2016. Disponível em: <http://www.securityreport.com.br/overview/mercado/vulnerabilidades-necessidades-seguranca-iot/#.XOSDjMhKjIU> Acesso em 10 Fev.2019.

ZAIDAN. Fernando. XML, RDF e OWL (Para saber um pouco mais sobre a Web Semântica), 2014 Disponível em: < http://www.techoje.com.br/site/techoje/categoria/detalhe_artigo/1973> Acesso em 10 Fev.2019.