**INTERNET DAS COISAS: IMPACTO DA INTERNET DAS COISAS NA SEGURANÇA DA INFORMAÇÃO**

Lenivaldo Dias Junior[[1]](#footnote-1)

**RESUMO**

Este artigo aborda como a Internet das Coisas vem causando um grande impacto na Segurança da Informação em função do surgimento acelerado de dispositivos que se conectam a internet e como estes colocam em risco os princípios básicos da Segurança da Informação. Observou-se as abordagens que devem ser tomadas como medida de proteção para evitar ataques através dos dispositivos da internet das coisas.

**Palavras Chave:** Internet Das Coisas. Segurança Da Informação. Vulnerabilidades.

**INTRODUÇÃO**

Novas tecnologias surgem através da criatividade e sagacidade de grandes cientistas, pesquisadores e estudiosos ao notarem uma deficiência, oportunidade ou necessidade de romper barreiras a fim de tornar cada vez mais prática a vida do ser humano e conectando-os, fazendo desta necessidade maior e principal motivador de dedicação para grandes descobertas, e em um desses momentos que surgiu o termo hoje conhecido como Internet das Coisas.

A ideia da Internet das Coisas de conectar vários dispositivos através da internet, como uma enorme teia acessível de qualquer parte do mundo, com o intuito de agilizar e facilitar o dia a dia do ser humano, entretanto tal benefício vem também acompanhado de um malefício e um desafio a altura para os profissionais de Segurança da Informação: manter a segurança e privacidade dos dados do usuário.

Este artigo intitulado Impacto da Internet das Coisas na Segurança da Informação, vem estabelecer a discussão sobre os problemas ocasionados devido a vulnerabilidades existentes nos dispositivos que fazem parte da internet das coisas.

O tema aborda como a grande quantidade de dispositivos que fazem parte da internet das coisas possuem problemas de vulnerabilidades que agravam a questão da segurança da informação colocando em risco os seus princípios básicos, além de proporcionar ataques cibernéticos capazes de derrubar ou causar instabilidades em serviços disponibilizados através da internet e métodos utilizados como forma de proteção afim de evitar estes tipos de ataques.

O objetivo principal deste artigo é entender como o grande crescimento do número de dispositivos da Internet das Coisas, principalmente dentro das organizações impactam na segurança da informação. Para ajudar a conduzir o trabalho tivemos os seguintes objetivos específicos:

- Conceituar a internet das coisas

- Explicar o que é a segurança da informação, seus valores e pilares;

- Abordar a vulnerabilidade do BYOD dentro das organizações;

- Por que a segurança da informação é um empecilho para a internet das coisas.

Esta artigo, trata-se de um estudo de abordagem qualitativa, para Oliveira (1999, p. 116), “[...] esta difere do quantitativo pelo fato de não empregar dados estatísticos como centro do processo de análise de um problema.”, exploratória quanto a finalidade que segundo Silveira e Cordova (2009, p. 35), “Este tipo de pesquisa tem como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito[...]” e de cunho bibliográfico, de acordo com Oliveira (1999, p. 119), “A pesquisa bibliográfica tem por finalidade conhecer as diferentes formas de contribuição cientifica que se realizaram sobre determinado assunto ou fenômeno.”.

**INTERNET DAS COISAS**

De acordo com Santos et. Al. E Tondin (2016), conceituar Internet das Coisas (também conhecida por **IoT**Internet of Things, em inglês), de uma forma tecnológica seria, que a Internet das Coisas é o cenário, que emergiu do avanço de várias áreas como, sistemas embarcados, microeletrônica, comunicação e tecnologia de informações, permitindo que todos os objetos da vida cotidiana, possam estar conectados à Internet e agindo de forma “inteligente”.

Nas décadas de 80 e 90, os estúdios de hollywood, nos apresentaram uma série de desenhos e filmes futurísticos, aonde vários de seus personagens viviam em ambientes totalmente automatizados, como exemplo pode-se citar um clássico como Os Jetsons (Transmissão original 1962, 1963), que acionavam a maioria das funcionalidades da casa através de comando de voz ou ao simples toque de um botão.

Na época em questão, isso parecia ser impossível, mas esta realidade já não está tão distante assim. Com a chegada da Internet das Coisas, o sonho Hollywoodiano está se tornando realidade.

O termo Internet de Coisas, surgiu em meados de 1999 a partir de ideias do pesquisador britânico, Kevin Ashton, do Instituto de Tecnologia de Massachusetts, mas, inicialmente, apenas com a possibilidade de se etiquetar eletronicamente os produtos da linha de produção de uma empresa, para facilitar a logística, utilizando identificadores de radiofrequência.

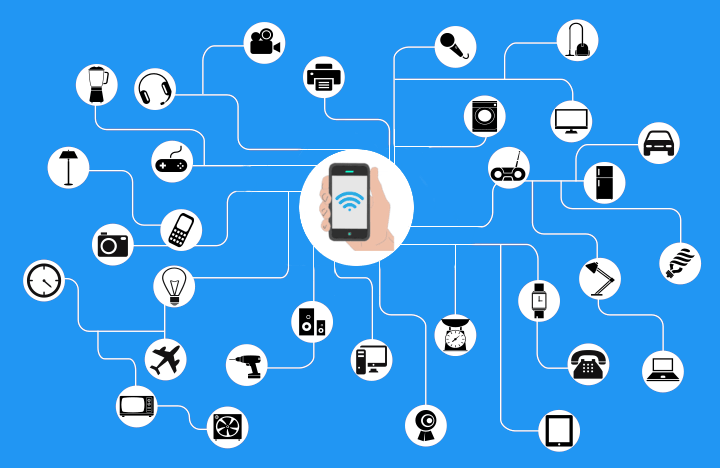
Pode-se dizer ainda que a Internet das Coisas é um conceito extremamente novo, segundo o Cisco *Internet Business Solutions Group* (IBSG), estima-se que a Internet das Coisas, tenha nascido entre 2008 e 2009, já que foi justamente nesse período que foram conectados à Internet mais dispositivos do que pessoas. (Evans, 2011).

Apesar de a Internet das Coisas, ser um conceito relativamente novo, Silva Neto, em seu livro Privacidade na Internet Um Enfoque Jurídico, traz um pensando de Tesla, que no final do século XIX, pensava em comercializar em Nova Iorque, uma combinação de suas descobertas, que tornaria possível, de modo preciso e instantâneo, a transmissão, sem fios, de qualquer tipo de sinais, mensagens ou caracteres, para todas as partes do mundo, assim como também, Um receptor barato, não maior que um relógio, que permitiria escutar, em qualquer lugar, na terra ou no mar, a palavra falada ou a música executada em algum outro lugar, mesmo que distante.

Hoje em dia a Internet das Coisas, já deixou de ser uma tendência para ser realidade, a cada dia que passa existem mais e mais equipamentos conectados à Internet. À medida que grandes empresas, não só do ramo da tecnologia, procuram integrar ainda mais dispositivos a rede, como por exemplo: os carros autônomos da Google, Tesla e da Udacity, geladeiras inteligentes da Samsung, inúmeras Smart TV que se encontram no mercado, ou seja, cada dia mais o mundo real está estreitando as relações com o mundo digital tendendo a se unificarem em um futuro, permitindo desta forma que ambos os mundos (real e digital) mantenham uma constante interação, seja com outras pessoas ou com outros equipamentos.

Pensando em todo o potencial que a Internet das Coisas tem, surgiram iniciativas para unifica-la, envolvendo a indústria, com os fabricantes de dispositivos, órgãos reguladores e de padronização, no Brasil fica a cargo da ABINC (Associação Brasileira de Internet das Coisas), além é logico de entidades acadêmicas e de pesquisa de todo o mundo.

Embora ainda não se tenha um consenso, e cada fabricante de dispositivo conecte seus equipamentos de diferentes formas, como por exemplo Bluetooth, Wi-Fi, Infra Vermelho, a tendência é que em breve todos estejam usando a internet como principal meio de comunicação para transferir suas informações, e é justamente nesse ponto que se tem que ter mais atenção. Já que equipamentos conectados à internet tendem a ser mais suscetíveis a ataques.



Fonte: Bluelux, 2016

Segundo Santos et. Al (2016):

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 viabilizará, 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. (SANTOS ET. AL, 2016, P. 2)

Com relação ao pensamento de Santos et. Al transcrito a cima, pode se observar que a Internet das Coisas nada mais é do que a evolução da própria internet, então é necessário entender as diferenças entre a Internet e a Web (World Wide Web), termos esses que na maioria das vezes são utilizados de forma errônea.

Segundo Evans (2011) :

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 transforme as informações que fluem pela Internet em algo utilizável. (EVANS, 2011)

Deste o seu surgimento ainda na época da guerra fria, no final dos anos 60, a Internet não evoluiu muito, enquanto a Web passou por várias mudanças como pode se ver no quadro 1, logo abaixo:

Quadro 1 – Evolução da WEB

|  |  |
| --- | --- |
| ETAPA | MOMENTO |
| 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 "panfletoware". 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". |

|  |  |
| --- | --- |
| ETAPA | MOMENTO |
| Etapa 4 | A quarta etapa, 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: Autoria própria.

Em comparação com a Web, a Internet não mudou muito, ela continua fazendo essencialmente o mesmo que foi planejada para fazer, ainda na época da ARPANET, uma das únicas mudanças significativas que houve, foi que no início eram usados inúmeros tipos de protocolos, como por exemplo, Apple Talk e Token Ring, e hoje em dia a Internet tem como padrão o protocolo IP.

Segundo Santos et. Al, “A Internet das Coisas tem alterado aos poucos o conceito de redes de computadores. ” (SANTOS, 2016, p. 2).

Isso exposto pode se observar, que a Internet das Coisas se torna imensamente importante, pois ela é a primeira grande transformação real que a Internet está passando, segundo Evans “um salto que levará a aplicações revolucionarias com potencial para melhorar consideravelmente a forma como as pessoas vivem, aprendem, trabalham e se divertem. ” P.6

**Segurança da Informação**

Antes de falar especificamente sobre Segurança da Informação, é necessário discorrer sobre o conceito do termo informação.

Informação tem uma definição deveras demasiada ambígua e incerta, pois varia muito de acordo com o ponto de vista de cada área e a forma como é abordada, contudo existe um consenso dentre tantos olhares sobre o termo e sua definição; a informação, por unanimidade de pontos de vista, é construída com três componentes básicos e na mesma intensidade essenciais, são eles: dados, informação e conhecimento.

Esclarecendo que a informação consiste em diferenças que fazem diferença, ou seja, a informação é constituída por um conjunto de dados explicitando um ponto de vista diferente sobre o mesmo assunto, assim trazendo um significado novo e relações desconhecidas sobre eventos e objetos (CAMPOS, 2007).

A informação pode possuir significado e causar impacto, se tornando o elemento essencial para a criação do conhecimento. Sendo assim, conclui-se que só se pode formar o conhecimento através do contato com a informação.

Isto exposto, pode-se dizer que a informação é de interesse vital para qualquer pessoa ou organização, já que essa informação bem utilizada por seus colaboradores, no caso de uma organização, poderá gerar grande valor para a mesma.

Sabido o quão importante é a informação para uma organização, é necessário entender o que é a Segurança da Informação e qual a sua importância para a sobrevivência das organizações.

Segundo Fontes (2010), uma definição simples e objetiva do que vem a ser a Segurança da Informação é:

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. (FONTES, 2010, p.11)

Para se falar de Segurança da Informação temos que entender seus três principais pilares: Confidencialidade, Integridade e Disponibilidade, conhecidos como CID.

Quadro 2 – Pilares da Segurança da Informação.

|  |  |  |
| --- | --- | --- |
| Confidencialidade | Integridade | Disponibilidade |
| A informação deve ser acessada e utilizada exclusivamente pelos que necessitam dela para a realização de suas atividades profissionais na organização; para tanto, deve existir uma autorização prévia. | A informação deve estar correta, ser verdadeira e não estar corrompida. | A informação deve estar acessível para o funcionamento da organização e para o alcance de seus objetivos e missão. |

Fonte: Autoria Própria.

Segundo o quadro 2, percebe-se que se um ou mais desses pilares não forem seguidos em algum momento, ocorrerá um incidente da Segurança da Informação, que nada mais é que a quebra dessa Segurança.

Campos (2007) diz que a quebra da Confidencialidade é:

Quando uma informação é acessada por pessoa não autorizada, intencionalmente ou não, seja pela descoberta de uma senha, pelo acesso a documentos ou de qualquer outro modo, então isto é um incidente de Segurança da Informação por quebra de confidencialidade. (CAMPOS, 2007, P.18)

O tipo de ataque mais utilizado para a quebra desse pilar é a engenharia social, que nada mais é que um ataque as pessoas da organização e não ao seu sistema, nesse caso, o atacante utiliza-se de métodos de sugestão e convencimento para induzir uma pessoa a quebrar um protocolo ou procedimento.

Campos (2007) diz que a quebra da Integridade é:

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. (CAMPOS, 2007, P.18)

Ocorre normalmente pela falta de validação de arquivos migrados de um sistema para outro, aonde os resultados da migração não são devidamente verificados, e após meses e até anos depois se descobre que os dados que ali estão não são mais confiáveis.

Campos (2007) diz que a quebra da 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, P.19)

Outro bom exemplo que pode se observar com relação a esse fator, é a falta de disponibilidade da informação por fatores naturais: enchentes, tempestades, terremotos. Ou ainda incidentes gerados por ação humana intencionalmente, como, incêndios, ataques com bombas, sabotagens e vandalismo.

**BYOD e Internet das Coisas**

A Internet das Coisas é um novo mundo de oportunidades, mas também é um desafio, este desafio requer atenção e uma nova mentalidade, além de uma intensa busca por soluções de segurança.

O fato é que ter uma conexão com a Internet torna qualquer objeto vulnerável a um ataque. Exemplos disso já começaram a deixar a ficção e tornaram-se realidade, em relatos de ataques contra carros autônomos, como pode ser observada na preocupação do FBI, que juntamente com dois órgãos de transito norte-americano, lançaram uma nota alertando a população e construtoras, sobre ataque de hackers a carros inteligentes (Mognon, 2016), e até mesmo contra aviões, como pode ser observado pela iniciativa lançada em 2015 pelos EUA para proteger aviões de ataque Hackers (Pasztor, 2015). Com a chegada dessas novas tecnologias de forma acelerada ao consumidor, ainda não se sabe ao certo o real impacto da Internet das Coisas na Segurança da Informação.

Para a Segurança da Informação a principal desvantagem para é a falta de privacidade, já que todas as coisas terão acesso à Internet, tais como, TV’s, geladeiras e até mesmo os automóveis. Com isso, haverá um enorme banco de dados funcionando *in-memory*, armazenando dados destes objetos. Isso proporcionará a uma seguradora de carros, por exemplo, a possibilidade de rastrear os locais por onde se passa, o modo como se dirige o carro e, com base nessas informações, aumentar ou diminuir o preço do seguro.

Segundo 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.(BALAGUER, 2015)

Para pessoas físicas, ou seja, o uso pessoal, se tem o risco envolvendo a segurança e a privacidade, mais para empresas o problema é ainda maior, já que há questões relacionadas não apenas a esses fatores, mas também a lucros e vantagens competitivas.

Segundo Junior (2016):

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 (JUNIOR, 2016).

Uma empresa que tem suas informações vazadas devido a uma falha proporcionada pela Internet das Coisas, pode até vim a perder espaço no mercado. Por isso o aumento da vulnerabilidade é o principal risco para a Segurança da Informação, e o que exige uma atuação mais contundente. É somente ao mitigar o risco de que dados sejam vazados que a pessoa ou empresa pode usufruir livremente dos benefícios da integração oferecidos pela Internet das Coisas.

Conhecer a fundo sua infraestrutura de segurança e ter controle sobre os dispositivos que se conectam ao ambiente de TI corporativo é o primeiro passo para que a empresa não corra riscos maiores na era da Internet das Coisas. (Junior, 2016)

O aumento dessa vulnerabilidade, é o que faz com que haja um aumento significativo da estrutura da Segurança da Informação para proteger os dados, nesse sentido os analistas precisam pensar em formas de construir e implantar uma estrutura de segurança mais robustas que contemple a integração da empresa, sem esquecer a necessidade de treinar os usuários, ou seja principalmente seus funcionários, para o uso correto e adequado de soluções de Internet das Coisas.

Para Gomes (2016) funcionários devem tomar o cuidado de não compartilharem informações em redes públicas de acesso, por exemplo, de modo a dificultar a invasão e o vazamento dos dados em qualquer ponto. Outro conselho para o ambiente corporativo, é isolar o trafego dos dispositivos e usuários que se encaixam no campo da Internet das Coisas em uma rede wi-fi exclusiva, isso faz com que o controle do pessoal de TI fique mais preciso, além de ajudar na garantia de que as operações da empresa não serão prejudicadas com a enorme quantidade de coisas conectadas.

De acordo com Avoyan (2015):

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. (AVOYAN, 2015)

Junto com a Internet das Coisas outro termo que vem se popularizando é o BYOD do inglês *Bring Your Own Device* que em tradução livre quer dizer “traga o seu próprio dispositivos”, que é um termo criado para expressar o uso de dispositivos pessoas no ambiente de trabalho. Com isso as empresas dão a seu funcionário a oportunidade de utilizar seus próprios aparelhos para acessar os dados e as informações da empresa.

Só que essa facilidade além de gerar uma maior produtividade, já que transforma qualquer ambiente em local de trabalho, ela traz também novas ameaças e vulnerabilidades para à segurança coorporativa.

Exemplo disso é o funcionário mal-intencionado, que tem acesso a todos os dados e informações da empresa, podendo copia-las através de seus dispositivos para clouds gratuidas, além disso, já que a informação está trafegando através de seus dispositivos pessoal ele pode se achar detentor da informação e copia-la para seu notebook, pendrive, smartphone, tablet, dentre outros. A questão maior é que todos esses dispositivos estão sujeitos a infecções de malwares e spywares, e até mesmo mais suscetíveis a roubo.

Os riscos e vulnerabilidades em dispositivos da Internet das Coisas, a cada dia que passa se torna mais comum, como pode ser visto em uma matéria da computerworld (2017), estudos mostram que dispositivos da Internet das Coisas devem ser pensados como parte da rede, e que esse estudo mostra um medo crescente de ameaças um tanto sem forma, principalmente porque erros cometidos por fabricantes de dispositivos que ainda não estão familiarizados com as práticas de segurança.

Segundo a visão de 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. (Zani, 2016).

Com o crescimento rápido da Internet das Coisas, muitas empresas estão adicionando as funcionalidades IP a seus dispositivos, afim de obter mais informações sobre como esse dispositivo é utilizado para poder melhorar a sua eficiência, todo problema é que a maioria dessas empresas têm pouca ou até nenhuma experiência com dispositivos conectados, com isso podendo vim cometer erros que possam comprometer a segurança do dispositivo e assim consequentemente a segurança dos usuários.

Alguns erros que podem vim a ser cometidos são: níveis de privilégios desnecessários, senhas padrões além de vulnerabilidades não corrigidas ou até mesmo desconhecidas no momento do lançamento do dispositivo.

Os dispositivos que compõem a Internet das Coisas, podem ser classificados em três grupos, de acordo com as funções que eles realizam, o primeiro grupo é o dos dispositivos que coletam informações através de sensores para transmitir essa informação de forma constante, o segundo grupo, é desenvolvido para receber essas informações que são coletadas pelo primeiro grupo via internet, e realizarem alguma atividade especifica, já o terceiro grupo realiza a função dos dois anteriores, ou seja coleta e recebe informações para ter um melhor funcionamento

Em qualquer um desses grupos, tem que ser observada com cuidado a questão da Segurança da Informação, já que temos que nos preocupar com quem pode ter acesso aos dados coletados e para que? E também, quem está comandando as ações desses dispositivos?

Um ponto que tem que ser observado é que praticamente todos os dispositivos da Internet das Coisas são potenciais alvos de ataques de negação e serviço (DDoS), esses são capazes de causar sérios problemas, como por exemplo parar o serviço prestado pelo dispositivo.

Segundo a visão de Pagliusi, é necessário se ter novas soluções de Segurança da Informação, especificas para a Internet das Coisa, porque só assim os sistemas serão capazes de se defender de ataques internos a rede.

**Conclusão**

O desenvolvimento desse trabalho, possibilitou analisar e entender um pouco mais sobre o surgimento e disseminação da internet das coisas, assim como também, um dos principais problemas que impedem que essa tecnologia possa ser utilizada de forma mais segura, seus impactos na Segurança da Informação, uma vez que, se existe a dificuldade de garantir a Confidencialidade, Integridade e Disponibilidade, que são os três principais pilares da Segurança da Informação.

De um modo geral, percebe-se que, para que a Internet das Coisas, possa trilhar um caminho de sucesso e com o mínimo de problemas possíveis, será necessário que ocorra uma conscientização principalmente por parte dos fabricantes de dispositivos, de que a Segurança da Informação é um dos principais aspectos a ser levado em conta.

Mesmo com a criação de órgãos regulatórios, como por exemplo a ABINC, ainda está longe de se ter um consenso com relação as especificações de segurança dos dispositivos da Internet das Coisas. Após a exposição de algumas preocupações dais como, a iniciativa lançada pelos EUA para proteger aviões de ataques Hackers e a nota de alerta do FBI e dois órgãos de transito norte-americanos, sobre ataque hacker a carros inteligentes, pode-se observar que a problemática tratada nesse trabalho realmente existe e é algo que realmente precisa ser estudada a fim de ser elucidada com a maior brevidade possível.

**REFERÊNCIAS**

OLIVEIRA, Silvio Luiz de. **Tratado de Metodologia Científica**: Projetos de Pesquisas, TGI, TCC, Monografias, Dissertações e Teses. São Paulo: Companhia Brasileira do Livro, 1999.

BALAGUER, Adriano. **Segurança da Informação no mundo da Internet das Coisas**, Disponível em: <http://computerworld.com.br/tecnologia/2015/02/25/seguranca-da-informacao-no-mundo-da-internet-das-coisas> Acesso em 15 jan. 2017

**http://computerworld.com.br/tecnologia/2015/02/25/seguranca-da-informacao-no-mundo-da-internet-das-coisas**

EVANS, Dave. **Internet das Coisas**: Como a próxima evolução da Internet está mudando tudo. Disponível em: <http://www.cisco.com/c/dam/global/pt\_br/assets/executives/pdf/internet\_of\_things\_iot\_ibsg\_0411final.pdf>. Acesso em 11 jan. 2017

TONDIN, Raphael Kieling. **Internet das Coisas**, Disponível em: <https://prezi.com/ggqt7rkqzlbt/internet-das-coisas/> Acesso em 23 jan. 2017

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

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

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

SÊMOLA, Marcos. **Gestão de Segurança da Informação**: uma visão Executiva. Rio de Janeiro, Elsevier, 2003.

AVOYAN, Hovhannes. **Por que a Internet das Coisas vai transformar a gestão de dispositivos móveis**. Disponível em: <http://imasters.com.br/gerencia-de-ti/por-que-a-internet-das-coisas-vai-transformar-a-gestao-de-dispositivos-moveis/?trace=1519021197>. Acesso em 30 jan. 2017

MOGNON, Mateus. **FBI alerta sobre aumento de ataques de hackers contra carros conectados.** Disponível em: <http://adrenaline.uol.com.br/2016/03/18/41027/fbi-alerta-sobre-aumento-de-ataques-de-hackers-contra-carros-conectados/>. Acesso em 08 fev.2017

PASZTOR, Andy. **EUA lançam iniciativa para proteger aviões de ataques de hackers.** Disponível em: <http://br.wsj.com/articles/SB11301772451238044816904581082141455324676> Acesso em 07 fev. 2017

RODRIGUES, Marcelo. **Malware para Android usa celular para infectar roteadores e redes sem fio**. Disponível em: <https://www.tecmundo.com.br/malware/113013-malware-android-usa-celular-para-infectar-roteadores-redes-fio.htm>. Acesso 23 jan. 2017

JUNIOR, Izo. **Como fica a segurança da informação na era da internet das coisas?** Disponível em: <http://blog.bluepex.com/como-fica-a-seguranca-da-informacao-na-era-da-internet-das-coisas/> Acesso em 11 nov. 2016

PAYÃO, Felipe. **Hackers realizam o maior ataque DDoS da história**. Disponível em: <https://www.tecmundo.com.br/internet/110078-hackers-realizam-maior-ataque-ddos-historia.htm>. Acesso 20 jan. 2017

GOMES, Diogo. **Internet das Coisas:** mais desafios para a segurança da informação. Disponível em: <http://www.tieducacional.com.br/internet-das-coisas-mais-desafios-para-seguranca-da-informacao>. Acesso em 11 nov. 2016

COMPUTERWORLD, Redação. **Internet das Coisas vai atrair cada vez mais cibercriminosos.** Disponível em: <http://computerworld.com.br/internet-das-coisas-vai-atrair-cada-vez-mais-cibercriminosos>. Acesso em 08 fev. 17

CRUZ, Edgar Vásquez. **A vulnerabilidade da Internet das Coisas:** Entenda os riscos para as empresas. Disponível em: <http://www.administradores.com.br/noticias/tecnologia/a-vulnerabilidade-da-internet-das-coisas/110912/>. Acesso em 08 fev. 2017

ZANI, Bruno. **As vulnerabilidades e necessidades de segurança da Internet das Coisas.** Disponível em: <https://corporate.canaltech.com.br/noticia/seguranca/as-vulnerabilidades-e-necessidades-de-seguranca-da-internet-das-coisas-80975/>. Acesso em 08 fev. 17

D’AVILA, Raphael. **Os desafios em segurança digital com a ‘Internet das Coisas’**. Disponível em: <http://www.techmag.com.br/novidades/os-desafios-em-seguranca-digital-com-a-internet-das-coisas/>. Acesso em 12 dez. 2016

VERT. **Por que a segurança é um empecilho para a internet das coisas?.** Disponível em: <http://www.vert.com.br/blog-vert/por-que-a-seguranca-e-um-empecilho-para-a-internet-das-coisas/> Acesso em 12 dez. 2016

PAGLIUSI, Paulo**. Internet das Coisas e segurança de informação:** Impacto da tecnologia sobre a privacidade. Disponível em: <https://www2.deloitte.com/br/pt/pages/risk/articles/impacto-da-iot.html>. Acesso em 09 fev. 2017

SILVEIRA, Guilherme**, A Internet das Coisas.** Disponível em: <http://www.bluelux.com.br/internet-das-coisas-iot/>. Acesso em 09 fev. 2017

SILVEIRA, Denise Tolfo; CÓRDOVA, Fernanda Peixoto. **A Pesquisa ciêntifica**. In. GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. (Org.) *Métodos de pesquisa*. Porto Alegre: Editora da UFRGS, 2009. 31 – 42. Disponível em: <http://www.ufrgs.br/cursopgdr/downloadsSerie/derad005.pdf>. Acesso em 13 fev. 2017.

1. Aluno do Curso de Especiação em Segurança da Informação da Universidade Estácio de Sá. E-mail: lenivaldodias@hotmail.com. Artigo realizado sob orientação da Professora Erika Conceição Gelenske Cunha, apresentado como requisito para obtenção do título de Especialista em Segurança da Informação. [↑](#footnote-ref-1)