Revista Científica UNAR (ISSN 1982-4920), Araras (SP), v.21, n.1, p.67-81, 2021.
D**OI: 10.18762/1982-4920.20210005**

A ASCENSÃO DA INTERNET DAS COISAS (IOT) E OS PROBLEMAS DE SEGURANÇA QUE A ACOMPANHAM

Kele Viviane de Oliveira **NASCIMENTO[1*]**

Wdson de **OLIVEIRA[2]**

RESUMO:

A ascensão da internet atrelada ao surgimento constante de novas tecnologias, tem viabilizado o desenvolvimento de dispositivos cada vez mais sofisticados e que nos permitem a otimização de nossas atividades rotineiras. A IoT – *Internet of Things* (Internet das Coisas), como ficou conhecida, está relacionada à capacidade que dispositivos presentes em nosso dia a dia têm de se interconectar por meio da rede. No entanto, à medida em que nos tornamos cada vez mais adeptos a ela, mais soluções demandamos do mercado, fazendo com que o desenvolvimento de novos dispositivos aumente de forma expressiva, o que reflete diretamente nos problemas de segurança que também são maximizados, uma vez que, conforme a IoT se torna mais popular, novas falhas e vulnerabilidades também vão sendo descobertas e exploradas. Além do mais, a isso se soma a falta de padrões e regulamentações voltadas ao tema. Portanto, o presente estudo procurou analisar tanto os porquês, quanto os atores envolvidos nesta problemática, bem como, o cenário atual, como este poderia piorar ao longo do tempo e qual seriam as possíveis soluções para assegurar que a questão recebesse a devida atenção, trazendo à tona uma reflexão sobre o quanto somos afetados por esse cenário e o que poderia ser feito para modificá-lo. Para tanto, a pesquisa realizada, que envolveu o levantamento e estudo de material relacionado, possibilitou toda a contextualização inicial, bem como, o alcance das conclusões do estudo.

PALAVRAS-CHAVE: IoT, Internet das Coisas, Segurança da Informação, Vulnerabilidades.

[1*] Graduanda em Segurança da Informação. Bacharel em Administração Pública.

E-mail do autor: kele_nascimento@yahoo.com.br;

[2] Mestre. Especialista. Graduado em Ciência da Computação.

E-mail do autor: wdson.oliveira01@fatec.sp.gov.br.

Recebido em: 07/09/2021 - Aceito para publicação em: 13/12/2021

ABSTRACT:

The rise of the internet coupled with the constant emergence of new technologies has enabled the development of increasingly sophisticated devices that allow us to optimize our routine activities. The IoT – Internet of Things, as it became known, is related to the ability of devices present in our daily lives to interconnect through the network. However, as we become more and more adept at it, we also demand more solutions from the market, causing the development of new devices to increase significantly, which directly reflects on the security problems that are maximized too, since that as the IoT becomes more popular, new flaws and vulnerabilities are also being discovered and exploited. Furthermore, to this is added the lack of standards and regulations focused on the subject. Therefore, this study sought to analyze the whys and the actors involved in this issue, as well as the current scenario, how it could get worse over time and what would be the possible solutions to ensure that the issue received due attention, bringing a reflection on how much we are affected by this scenario and what could be done to change it. So, the research, which involved the survey and study of related materials, enabled all the initial contextualization as well as the reach of the study's conclusions.

KEYWORDS: IoT, Internet of Things, Information Security, Vulnerabilities.

INTRODUÇÃO

Por volta dos anos de 1980, a Internet se difundiu no âmbito acadêmico de renomadas universidades norte-americanas, sobretudo, atrelada a pesquisas voltadas ao seu próprio desenvolvimento, passando somente na década seguinte a ser inserida na sociedade como um todo, até se tornar a grande potência como a conhecemos atualmente e que se faz presente de forma intrínseca em boa parte de nossas atividades diárias.

Com a ascensão da internet ao longo dos anos, bem como, com o surgimento de novas tecnologias constantemente, nossas atividades rotineiras estão sendo executadas de forma cada vez mais simples devido às facilidades que novos dispositivos nos proporcionam. A *Internet of Things* (Internet das Coisas) - IoT, como ficou conhecida, está relacionada à capacidade que dispositivos presentes em nosso dia a dia, como refrigeradores, aparelhos de ar-condicionado, *smartwatches*, dentre outros – têm de se interconectar, trocando dados por meio da rede.

Atualmente, já existem até mesmo automóveis que possuem conexão direta com a internet, e o que se espera, é que estes se tornem cada vez mais inteligentes e ganhem ainda mais autonomia, deixando, inclusive, de necessitar de seres humanos para conduzi-los (cabe mencionar que o Google já possui, em fase de testes desde 2015, um protótipo desse tipo de veículo). Além disso, nossas casas também estão evoluindo e se tornando *"smart homes"* (casas inteligentes) com um número cada vez maior de soluções integradas a dispositivos de assistência pessoal.

A internet que outrora se restringia a um conjunto limitado de atividades, hoje está presente em praticamente todas as áreas e lugares que permeiam nossas vidas, tornando-se cada vez mais essencial conforme nossas exigências e necessidades vão aumentando. Em contrapartida, a fim de atender a essa crescente demanda, o desenvolvimento de novos dispositivos com capacidade de conexão à rede tem se maximizado de forma expressiva, e consequentemente, os problemas atrelados à segurança da informação também.

Levando-se em conta o fato de que atualmente os dados são considerados o ativo mais valioso dos últimos anos e que com mais dispositivos conectados à rede,

maior têm sido a produção e tráfego de informações, alavancando ainda mais este valor, chegamos ao tema central deste estudo: Como a ascensão da Internet das Coisas tem se tornado um grande problema para a área de Segurança da Informação.

PROBLEMÁTICA

Conforme a Internet das Coisas tem evoluído e mais dispositivos estão sendo abarcados por essa tecnologia nos mais diversos segmentos, novas falhas e vulnerabilidades também estão sendo descobertas e exploradas. Embora se espere que com a evolução tecnológica, os dispositivos também evoluam, tornando-se cada vez mais sofisticados e seguros, na prática, não é exatamente isso o que vem ocorrendo.

Estamos cada vez mais conectados virtualmente e, consequentemente, mais suscetíveis a determinados tipos de ataques, que podem nos atingir de forma direta ou indireta, causando inúmeros transtornos devido a interconexão cada vez maior entre dados, informações e dispositivos – algo que tem se intensificado com a ascensão da IoT.

Costumávamos estar expostos a riscos cibernéticos geralmente ao utilizarmos nossos computadores pessoais, navegando em sites de procedência duvidosa, por exemplo. Hoje, estamos vulneráveis a cada toque na tela de nossos *smartphones,* no uso de *tablets* para simples leituras, na instalação de câmeras de segurança para vigilância de nossas residências, na aquisição de veículos com sistemas embarcados, na utilização de aparelhos de ar-condicionado com termostatos inteligentes ou mesmo de refrigeradores de última geração com seus sistemas interativos, todos com capacidade de conexão à Internet.

Em um cenário ideal, os problemas relacionados à segurança da informação, sobretudo, aqueles que se referem à privacidade e proteção de dados, poderiam estar sendo tratados e solucionados pela indústria de desenvolvimento, através de uma abordagem conhecida como *“Privacy by Design”*, ou seja, os fabricantes de softwares e *firmwares* (classe específica de softwares de computador que fornecem controle de baixo nível para hardwares específicos de determinados dispositivos) deveriam estar

considerando ao menos a questão da privacidade das informações desde o início da concepção de cada solução a ser desenvolvida.

AGRAVANTES

A corrida desenfreada pela conquista deste novo e tão promissor nicho de mercado somada à falta de padronizações e legislações pertinentes que regulamentem as atividades de desenvolvimento, tem sido um dos principais agravantes dos problemas relacionados à segurança da informação no que diz respeito aos dispositivos de IoT, já que esta acaba sendo deixada de lado em detrimento da urgência que a indústria emprega em desenvolver e lançar soluções cada vez mais inovadoras e que atendam prontamente às crescentes demandas dos consumidores.

Enquanto a indústria continua priorizando a velha premissa de que *"tempo é dinheiro"* e os consumidores não enxergam a questão da privacidade e proteção de dados como um grande problema, tendo vista que já nos acostumamos a expor muito de nossa vida privada em redes sociais, por exemplo, também não são identificados grandes esforços por parte do governo voltados a definição de regulamentações, nem por parte do próprio setor de tecnologia, que costuma se posicionar e estabelecer critérios que posteriormente acabam sendo naturalmente aceitos como padrões.

Além disso, também devemos considerar que o tema é relativamente novo, já que a Internet das Coisas só começou a ganhar forças por volta de 2015 e que ainda há muito o que se considerar em relação à questão, tendo em vista que os problemas que a IoT pode desencadear, não estão vinculados apenas à privacidade e proteção de dados, mas também à infraestrutura da rede como um todo, levando-se em conta a sobrecarga pelo elevado e crescente tráfego de informações, que pode afetar outros requisitos fundamentais de segurança da informação, como a disponibilidade.

SEGURANÇA DA INFORMAÇÃO E IOT

Conforme a produção e tráfego de dados vai se maximizando exponencialmente devido à conectividade que a Internet das Coisas proporciona, o gerenciamento dessas informações tem se tornado um problema cada vez maior para a área de segurança. Quanto mais dispositivos são conectados à rede, maior se torna nosso nível de exposição e, consequentemente, maior é o número de vulnerabilidades que podem ser exploradas.

A maioria das ameaças à segurança da informação são aquelas que podem afetar os princípios fundamentais evidenciados pela tríade CIA (*Confidentiality, Integrity and Availability*) – Confidencialidade, Integridade e Disponibilidade – comprometendo as informações.

No que concerne à disponibilidade, a questão está atrelada principalmente aos aspectos de capacidade da infraestrutura de rede em suportar a crescente demanda, que é refletida diretamente no aumento do tráfego de dados. Além disso, a estrutura de endereçamentos IPv4 (*Internet Protocol version 4* – Protocolo de Internet versão 4), protocolo que opera na camada de rede e que já estava à beira do esgotamento, também já não daria conta de suprir as necessidades da IoT.

O princípio da integridade seria provavelmente o menos afetado (diretamente) pela ascensão da IoT, embora, se vinculado ao princípio da confidencialidade, também poderia ser prejudicado de forma considerável.

Já em relação ao princípio da confidencialidade, notadamente o mais frágil no que diz respeito à segurança da informação em IoT, os problemas estariam voltados à questão da privacidade e proteção de dados, matéria ainda não devidamente regulamentada e, portanto, aberta às implementações definidas pelo próprio mercado, que nem sempre tem se preocupado em adotar padrões que poderiam tornar os dispositivos mais seguros, de modo que, a privacidade e proteção dos dados poderia ser facilmente comprometida por meio de acessos indevidos aos dispositivos, o que possibilitaria o uso, roubo ou até mesmo modificação das informações, afetando, inclusive, o princípio da integridade neste último caso. Além disso, também podemos considerar a possibilidade de invasão de privacidade propriamente dita, através do acesso a dispositivos de captação de áudio e imagem. Portanto, conclui-se que, em

muitos casos, os dispositivos IoT podem ser excelentes vias de acesso, facilitando a execução de ataques à segurança da informação.

Cabe mencionar que o intuito deste trabalho não é o de condenar ou desestimular o uso da IoT, mas sim o de demonstrar que por conta do seu alto potencial expansionista e facilitador, a mesma precisa ser observada atentamente, para que além de excelentes funcionalidades, o mercado também ofereça segurança em níveis no mínimo razoáveis aos seus consumidores.

VISÃO ACADÊMICA

Os autores Júnior e Moreno (2016) ressaltam em seus estudos que além do desenvolvimento, também há de se despender tempo com a pesquisa e o tratamento dos aspectos de segurança aplicáveis em infraestrutura para Internet das Coisas, discutindo ainda os desafios e as soluções adequadas para tal, sobretudo, quanto à necessidade de manutenção da privacidade dos usuários e as questões de interoperabilidade entre os dispositivos de IoT. Os autores também fazem menção à necessidade de atendimento dos princípios básicos de segurança da informação, composto pela tríade CIA e chamam a atenção quanto aos desafios e trabalhos futuros na área em questão.

Segundo Khan et al. (2012), a Internet das Coisas promoverá a conectividade de tudo e de todos. E, como podemos notar quase que diariamente frente às novidades lançadas pela indústria tecnológica, esta premissa se torna cada vez mais concreta. Assim sendo, Kumari et al. (2010) evidencia que antes da implementação de redes de sensores sem fio, algo que se aplica à IoT, também há de se pensar na adoção de níveis de proteção para tais.

Autores como Tan e Wang (2010), por sua vez, apresentam estudos acerca da infraestrutura voltada à IoT e a subdivide basicamente em cinco camadas. No entanto, para o objetivo deste trabalho, as camadas que mais nos interessam é a responsável pelos aspectos físicos da tecnologia e interação com o meio (objetos/ sensores) e a camada de rede, responsável pelo transporte da informação percebida e coletada na camada anterior, direcionando-a para o processamento supostamente adequado.

Dwivedi e Yvas (2010), também se concentram na parte física da Internet das Coisas e apresentam certas especificações técnicas quanto aos hardwares, demonstrando a limitada capacidade de processamento dos dispositivos.

Já os estudos de Fukuda (2019), demonstram preocupação com a necessidade de se entender como a Internet das Coisas é vista pelos usuários e pela indústria. O autor ainda reforça a questão de que é preciso uma espécie de conscientização coletiva, por parte dos fabricantes e dos usuários finais, de modo a propagar a segurança da informação como um critério relevante para a IoT.

> [...] 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.

Conforme pressuposição de Balaguer (2015), frente à crescente utilização da IoT mundialmente, bem como, com a alta disseminação de *malwares* (softwares maliciosos), a segurança da informação deveria seguir como uma das principais prioridades da indústria. Porém, isso ainda não é uma realidade.

De acordo com Zani (2016), muitos dos dispositivos de IoT não são projetados levando-se em conta quesitos de segurança – não há restrições de acesso, como a necessidade de uso de senhas ou a devida preocupação com o armazenamento das informações trafegadas, dentre tantas outras vulnerabilidades passíveis de exploração por agentes de ameaça. Gomes (2016) enfatiza que grande parte dos fabricantes concentra suas preocupações unicamente nos requisitos de funcionalidade dos dispositivos, deixando às margens os requisitos de segurança.

Diversos autores analisam ainda as principais vulnerabilidades atreladas à Internet das Coisas, destacando questões como a da privacidade, do processamento e do gerenciamento dos dados, tendo em vista a sobrecarga gerada devido ao alto volume do tráfego de informações produzidas por dispositivos IoT.

INDÚSTRIA

A indústria, atenta às necessidades de seus consumidores e às oportunidades de mercado, procura sempre de forma rápida e objetiva atender a essas demandas apresentando soluções pontuais e inovadoras. Tal dinâmica, é impulsionada ainda mais pelo fator concorrência intrínseco ao setor, de modo que, em muitos casos, as soluções apresentadas, nem sempre são as mais efetivas, apenas as mais atrativas ou simplesmente lançadas de antemão. Embora normalmente eficazes, muitas vezes carecem de aprimoramentos e, não raro, esses estão centralizados justamente na parte referente à segurança.

A falta de regulamentação específica (dispositivos legais), não é necessariamente um problema para o setor, no entanto, a falta de padronizações sim o é, uma vez que, a interoperabilidade entre os dispositivos pode se tornar um fator importante quando da oferta ao mercado, já que para os consumidores, pode ser de extrema relevância que seus equipamentos, independentemente de marca, modelo ou fabricante, sejam compatíveis uns com os outros, portanto, esta é uma questão que aos poucos tem despertado o interesse do setor e que poderá direcioná-lo à definição de padrões a serem adotados por todos da área.

A indústria também está começando a ser impulsionada por incentivos financeiros empregados pelos governos e estímulos acadêmicos ligados à pesquisa e desenvolvimento (P&D). Logo, percebe-se que esses três atores (indústria, governo e academia) estão caminhando rumo ao estabelecimento de um ecossistema de inovação voltado exclusivamente à Internet das Coisas. Observa-se, portanto, que a ação do Estado sobre as atividades da indústria de IoT é mais de cunho investidor do que regulador, isto é, a maioria dos governos têm se preocupado em impulsionar as atividades da área, deixando que o próprio setor, de certo modo, se autorregule. No entanto, um dos principais problemas dessa abordagem é o risco de que uma empresa que já exerça forte influência no ramo de tecnologia, monopolize o mercado e, consequentemente, reverta a estratégia do Estado, desestimulando as ações de concorrentes e desaquecendo o mercado.

ESFORÇOS GOVERNAMENTAIS

Alguns governos acreditam que o excesso de regulamentação tende a reprimir o avanço tecnológico inibindo a inovação. Portanto, ainda não há um consenso quanto ao envolvimento do Estado, bem como, à delimitação de ações específicas voltadas ao desenvolvimento da IoT no cenário mundial. No entanto, tendo em vista o potencial de transformação que a IoT representa em nosso cotidiano, influenciando de forma direta em nossas interações com os mais diversificados ambientes, o papel do Estado se faz fundamental, independentemente da estratégia adotada.

Levando-se em conta as particularidades de cada país, estudos realizados pelo Banco Nacional de Desenvolvimento Econômico e Social – BNDES (2017) a fim de viabilizar e incentivar a adoção da IoT no país, identificaram que os governos tendem a adotar três tipos de posicionamentos distintos:

- (i) podendo exercer presença ativa em IoT, por meio da participação no desenvolvimento do setor através da concessão de investimentos, definição de áreas prioritárias e do caminho a percorrer, estabelecimento de associações/parcerias, exercício de liderança em temas de interesse global, como padronização e segurança, bem como, influência à demanda e capacitação de pessoal;
- (ii) propiciando a formação do ecossistema, por meio de ações que aproximem empresas, startups e universidades através de programas e investimentos, por exemplo; ou ainda
- (iii) elaborando diretrizes e empregando investimentos em áreas focais, como padronização, pesquisa e desenvolvimento, difusão de melhores práticas, bem como, viabilizando a competitividade e abertura do mercado.

Não é possível eleger uma dessas abordagens como sendo a melhor, já que isso depende muito do contexto interno, no entanto, observou-se que nos países onde o papel do governo é mais ativo, o ecossistema de Internet das Coisas já está melhor consolidado, embora também seja possível identificar exceções. Países que apresentam menor envolvimento do governo têm revisado suas estratégias. Além

disso, cabe ressaltar que esse é um tema ainda muito novo, de modo que, boa parte dos países focou inicialmente em estabelecer diretrizes gerais, comumente definidas em um plano nacional, como é o caso do próprio Brasil, que em 2019, criou o seu Plano Nacional de Internet das Coisas.

PLANO NACIONAL DE INTERNET DAS COISAS

No caso do Brasil, o Plano Nacional de Internet das Coisas foi instituído pelo decreto nº 9.854 de 25 de junho de 2019, que também dispõe acerca da Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas. De acordo com o decreto em questão, por Internet das Coisas entende-se o seguinte:

> I - Internet das Coisas - IoT - a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade.

Segundo texto do próprio decreto, a finalidade do plano é a de implementar e desenvolver a IoT no Brasil, pautando-se na livre concorrência e na livre circulação de dados, com observância das diretrizes de segurança da informação e de proteção de dados pessoais. Seus objetivos estão relacionados a melhorar a qualidade de vida das pessoas e aumentar a eficiência na oferta de serviços; promover a capacitação profissional e gerar empregos na economia digital; incrementar a produtividade e fomentar a competitividade das empresas nacionais dentro de um ecossistema de inovação; firmar parcerias entre setor público e privado; bem como viabilizar a integração do Brasil no cenário internacional relacionado à pesquisas, desenvolvimento, inovação e internacionalização de soluções desenvolvidas internamente.

O decreto estabelece que o Ministro de Estado da Ciência, Tecnologia, Inovações e Comunicações será o responsável por indicar os ambientes que deverão

ser priorizados quando da aplicação de soluções de IoT, devendo, no mínimo, incluir os de saúde, cidades, indústrias e rural, observando critérios de oferta, demanda e capacidade de desenvolvimento local. Para os fins a que se destina este estudo, nos caberia focar na parte voltada à indústria, no entanto, como a referida premissa está vinculada a ato ministerial independente, não há muito o que se explorar diretamente no texto do decreto em questão, de modo que a parte que nos é mais relevante neste momento é a disposta no artigo 5º, que estabelece os temas que serão contemplados no plano de ação que visa identificar as soluções que possibilitem a viabilização do Plano Nacional de Internet das Coisas, definindo “regulamentação, segurança e privacidade” como um deles.

Assim, podemos notar que o governo federal começou a empregar esforços relacionados à questão recentemente, de modo que, mesmo com a criação de um decreto dispondo acerca da instituição de um Plano Nacional de Internet das Coisas, do ponto de vista prático, ainda não se pôde identificar avanços significativos. E, ainda que o Ministério supracitado tenha assinado um acordo com o BNDES para a condução de uma série de estudos relevantes a fim de se entender todo o contexto relacionado à IoT e viabilizar a definição do plano de ação, ainda há muito o que se fazer.

CONCLUSÕES

Diante do exposto, podemos concluir que os problemas relacionados à Internet das Coisas no que diz respeito à segurança da informação são em sua maioria de ordem técnica. Por se tratar de um tema ainda muito recente, existem uma série de requisitos a serem definidos e implementados, dos quais podemos destacar a necessidade de legislação regulamentar, bem como, definição de normas e padrões, a fim de garantir a justa concorrência no mercado e a entrega de soluções seguras aos consumidores. Além disso, a questão da própria infraestrutura necessária ao ecossistema de IoT, também é reconhecida como um potencial desafio à frente.

Cabe ressaltar que embora as questões de regulamentação e padronização sejam extremamente relevantes para assegurar aos dispositivos ao menos um nível

mínimo de segurança, boa parte dos governos tem concentrado seus esforços em estratégias voltadas ao estímulo das atividades do mercado, de modo a incentivar o desenvolvimento da IoT e fomentar a indústria nacional. Além disso, muitos ainda acreditam que o excesso de regulamentação pode inibir a inovação, de modo que também é possível notar certo empenho dos governos na aproximação do mercado às universidades, que por sua natureza, já supririam o requisito de Pesquisa e Desenvolvimento (P&D), base para qualquer avanço tecnológico.

Por ora, fica evidente que a relação entre o setor público e o privado, no que diz respeito à questão, ainda não voltou o olhar para quem mais tem o potencial de influenciar na definição das diretrizes a serem adotadas pelo mercado: o consumidor, sendo este, o mais prejudicado nessa relação. Além disso, é possível concluir que a segurança da informação somente será efetivamente concebida com a adoção de um conjunto de controles, que não se restringem apenas às regulamentações, de modo que a padronização seria ainda mais relevante nesse primeiro momento, desde que atendesse às boas práticas de desenvolvimento seguro.

REFERÊNCIAS

BALAGUER, A. **Segurança da Informação no mundo da Internet das Coisas**. Disponível em: <https://computerworld.com.br/plataformas/seguranca-da-informacao-no-mundo-da-internet-das-coisas/>. Acesso em 22 de maio de 2021.

BNDES. **Produto 1 - Benchmark de iniciativas e políticas públicas - Relatório Final**. Abril de 2017. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/48fff464-7a3c-442b-98c3-aa4634ad08d8/Relatorio-de-benchmark-fase-1-20170516_Produto_Frente_1_Benchmark_ENTREGA_FORMAL_FinalRevisado.pdf?MOD=AJPERES&CVID=lNGCXmw>. Acesso em 22 de outubro de 2021.

BRASIL. **Decreto nº 9.854, de 25 de junho de 2019**. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das

Coisas. Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9854.htm>. Acesso em: 20 de outubro de 2021.

DE JESUS JUNIOR, A. A.; MORENO, E. D. **Segurança em Infraestrutura para Internet das Coisas**. Revista Gestão.Org, v. 13, Edição Especial, 2015. p. 370-380, ISSN 1679-1827. Disponível em: <https://periodicos.ufpe.br/revistas/gestaoorg/article/view/22122>. Acesso em 22 de maio de 2021.

DWIVEDI, A. K.; YVAS, O. P. **Network Layer Protocols for Wireless Sensor Networks: Existing Classifications and Design Challenges**. International Journal of Computer Applications (0975 8887), v. 8, n. 12, 2010. Disponível em: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.206.3522&rep=rep1&type=pdf>. Acesso em 22 de maio de 2021.

FUKUDA, L. M. **Segurança da informação em IOT**. 2019. Trabalho de Conclusão de Curso (Especialização em Gestão da Tecnologia da Informação e Comunicação) - Universidade Tecnológica Federal do Paraná, Curitiba, 2019. Disponível em: <http://repositorio.utfpr.edu.br/jspui/handle/1/19442>. Acesso em 22 de maio de 2021.

GOMES, P.C. **Exemplos e Aplicações de Internet das Coisas (IOT)**. OP Services, 02 de fevereiro de 2016. Disponível em: <https://www.opservices.com.br/exemplos-de-internet-das-coisas>. Acesso em 22 de maio de 2021.

KHAN, R., KHAN, S. U., ZAHEER, R.; KHAN, S. **Future Internet: the Internet of Things architecture, possible applications and key challenges**. In: Frontiers of Information Technology (FIT), 10th International Conference, 2012. Disponível em: <https://www.academia.edu/35984783/Future_Internet_The_Internet_of_Things_Architecture_Possible_Applications_and_Key_Challenges>. Acesso em 22 de maio de 2021.

KUMARI, P., KUMAR, M., RISHI, R. **Study of Security in Wireless Sensor Networks**. Internationa Journal of Computer Science and Technology, v. 1, n. 5, p. 347-354, 2010.

TAN, L. WANG, N. **Future internet: The internet of things.** In: Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference, IEEE, 2010. p. V5-376-V5-380. Disponível em: <https://ieeexplore.ieee.org/document/5579543?arnumber=5579543>. Acesso em 22 de maio de 2021.

ZANI, B. **As vulnerabilidades e necessidades de segurança em IoT**. Security Report, 29 de setembro de 2016. Disponível em: <https://www.securityreport.com.br/overview/mercado/vulnerabilidades-necessidades-seguranca-iot/#.YMv2nfKSmiMz>. Acesso em 22 de maio de 2021.