RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

ESTUDO SOBRE SEGURANÇA E PRIVACIDADE NA INTERNET DAS COISAS (IoT)

STUDY ON SECURITY AND PRIVACY IN THE INTERNET OF THINGS (IOT)

ESTUDIO SOBRE SEGURIDAD Y PRIVACIDAD EN EL INTERNET DE LAS COSAS (IOT)

Lucas Della Rovere[1], Fabiana Florian[2]

e361601
https://doi.org/10.47820/recima21.v3i6.1601

PUBLICADO: 06/2022

RESUMO
O artigo tem por objetivo estudar sobre a segurança e a privacidade na Internet das Coisas (IoT). Foi realizada uma pesquisa bibliográfica sobre o tema e observou-se que a IoT evoluiu de forma rápida e suas aplicações são utilizadas em áreas variadas. O estudo revela que muitas vezes, por limitações de *hardware*, a segurança e privacidade se tornam um obstáculo a ser vencido em IoT, mas, com novos esforços, como a criação de documentos de padrões e regras por parte de organizações internacionais, estes problemas tendem a afetar cada vez menos suas aplicações.

PALAVRAS-CHAVE: Internet das Coisas. Segurança. Privacidade.

ABSTRACT
The article aims to conduct a study on security and privacy in the Internet of Things (IoT). A bibliographic research was carried out on the subject and it was observed that the IoT has evolved quickly and its applications are used in different areas. The study reveals that often, due to hardware limitations, security and privacy become an obstacle to be overcome in IoT, but with new efforts, such as the creation of standards and rules documents by international organizations, these problems tend to affect their applications less and less.

KEYWORDS: *Internet of Things. Security. Privacy.*

RESUMEN
El artículo tiene como objetivo estudiar la seguridad y la privacidad en el Internet de las Cosas (IoT). Se realizó una investigación bibliográfica sobre el tema y se observó que IoT evolucionó rápidamente y sus aplicaciones se utilizan en diversas áreas. El estudio revela que a menudo, debido a las limitaciones de hardware, la seguridad y la privacidad se convierten en un obstáculo a superar en IoT, pero con nuevos esfuerzos, como la creación de estándares y documentos de reglas por parte de organizaciones internacionales, estos problemas tienden a afectar cada vez menos a sus aplicaciones.

PALABRAS CLAVE: *Internet de las Cosas. Seguridad. Privacidad.*

INTRODUÇÃO

Em um mundo cada vez mais conectado, principalmente após um cenário pós pandêmico no qual diversas pessoas ficaram isoladas em suas casas, tendo como principal entretenimento a internet e apetrechos tecnológicos, é de extrema importância compreender a evolução relacionada a segurança na internet e nos equipamentos a ela conectados. Cada vez mais novos equipamentos se conectam a

[1] Universidade de Araraquara - UNIARA
[2] Universidade de Araraquara - UNIARA

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

internet e trazem facilidades e melhorias no dia a dia, como interruptores, relógios inteligentes, lâmpadas, fechaduras e tantos outros, equipamentos estes que compõem os objetos da Internet das Coisas (IoT). Mesmo com avanços, até que ponto estes equipamentos realmente são seguros e privados e quais os esforços realizados para que eles sejam cada vez mais impenetráveis, protegendo informações das ameaças da internet.

A IoT não é considerada exatamente como uma tecnologia, mas sim um conceito, abrangendo várias tecnologias, plataformas e modelos de negócio. Pode ser entendida como uma extensão da Internet atual, proporcionando que objetos do dia a dia que possuem capacidade computacional e de comunicação, se conectem à Internet e possam ser controladas remotamente e acessadas como provedores de serviços (SANTOS *et al*., 2016).

Apesar de parecer algo novo, o termo IoT foi mencionado pela primeira vez na *Procter & Gamble* (P&G) por Ashton, em 1999 e ganhou força após avanços obtidos nas áreas de sistemas embarcados, comunicação, microeletrônica e sensoriamento. Ashton propunha que todos os objetos do dia a dia fossem equipados com identificadores e conectividade sem fio, permitindo a comunicação entre eles e o gerenciamento por computadores. Um conceito simples e eficiente, mas que esbarrava nas limitações tecnológicas da época (LOPEZ RESEARCH, 2013).

Com os avanços cada vez mais velozes nessa área e o surgimento de novos dispositivos, torna-se importante a disseminação desse conhecimento, seja no meio acadêmico ou fora dele, para que se conheça mais sobre o universo das "coisas", e que as casas, carros e até cidades “inteligentes”, sejam compreendidos por todos.

Assim, este trabalho possui como principal objetivo estudar sobre a segurança e privacidade na internet das coisas (IoT), analisando os avanços atingidos na área, quais as possibilidades de evolução e como estes princípios são aplicados nos dispositivos de IoT.

1 PROCEDIMENTOS METODOLÓGICOS

Para que os objetivos propostos fossem alcançados, foi realizada a revisão bibliográfica como principal metodologia, fazendo uso de repositórios de universidades, sites de busca, livros e base de dados, como fontes de pesquisa para fomentar a fundamentação teórica aqui apresentada.

Como afirmam Marconi e Lakatos (2006), as pesquisas bibliográficas possuem como principal intuito o levantamento bibliográfico já produzido sobre um determinado tema, independente do formato utilizado, de modo que, a partir deste novo enfoque ou abordagem utilizada durante este levantamento, novas conclusões inovadoras e dados atualizados sejam produzidos.

Ao buscar pelo tema, diversos registros foram retornados, e com o intuito de filtrar o resultado obtido, alguns critérios foram estabelecidos, como estudos publicados em português ou inglês, que continham como palavra-chave os termos “internet das coisas" e “segurança na internet das coisas" e que tiveram sua data de publicação a partir de 2010. Aproximadamente 16.000 resultados foram obtidos, sendo os mais relevantes utilizados como fonte de informação, tendo seu conteúdo analisado

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

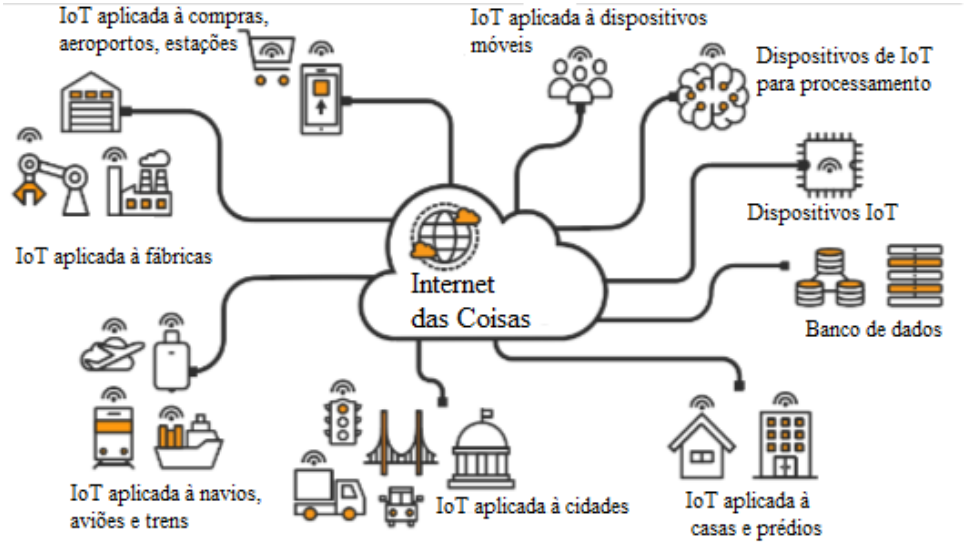
e apresentado aqui de forma compilada a fim de descrever as características de IoT e os princípios de segurança e privacidade a ela aplicada.

2 A IMPORTÂNCIA DA INTERNET DAS COISAS (IoT): LIMITES E OPORTUNIDADES

2.1 INTRODUÇÃO À INTERNET DAS COISAS

De modo geral, IoT pode ser entendida como uma extensão da Internet atual, proporcionando que objetos do dia a dia que possuem capacidade computacional e de comunicação, se conectem à Internet e possam ser controladas remotamente e acessadas como provedores de serviços (SANTOS *et al*., 2016). Estes objetos são conhecidos então como as “coisas” e podem estar disseminados nas indústrias, cidades, hospitais, entre outros lugares (Figura 1).

Figura 1 – Representação de um sistema formado por IoT.



Fonte: Tibco, 2022.

Um dos grandes objetivos pretendidos com IoT é formar uma rede ubíqua e global que integra o mundo físico, tornando os dispositivos inteligentes o suficiente para reduzir o trabalho humano, compartilhando as informações entre si e com diversas pessoas.

Um estudo conduzido pela Lopez Research (2013) evidencia que a IoT possui três pilares principais, os quais chamaram de "os três Cs da IoT", sendo eles, comunicação, controle e automação e custos reduzidos (LOPEZ RESEARCH, 2013). Como principal característica do pilar de comunicação, a IoT tem como objetivo divulgar informações as pessoas e aos sistemas, uma vez que podem ser coletadas com uma frequência muito maior utilizando objetos que contam com a tecnologia de IoT, como por exemplo, os *smartwatch*, relógios inteligentes que são capazes de monitorar diversos sinais vitais, como pressão, batimento cardíaco, entre outras informações; o pilar de controle e automação tem como objetivo permitir que as pessoas sejam capazes de controlar dispositivos remotamente, isto

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

é, a partir de um ambiente diferente daquele em que o dispositivo se encontra, como por exemplo, ligar ou desligar uma lâmpada em um determinado cômodo quando se está em um local totalmente diferente; e no que diz respeito aos custos reduzidos, a adoção da IoT permite a economia de capital tanto para empresas quanto para pessoas, dando origem ao pilar de custos reduzidos. Com seu uso empresas podem monitorar o desempenho e integridade de seus equipamentos, por exemplo, permitindo que um problema ou necessidade de troca de alguma peça seja previsto antecipadamente, minimizando a falha do equipamento e permitindo que a empresa execute a manutenção planejada.

Porém, além dos desafios técnicos e sociais para seu desenvolvimento, a IoT traz consigo problemas de segurança que diferem bastante das ameaças tradicionais encontradas nos ambientes das tecnologias de informação e comunicação, uma vez que estes dispositivos se tornam vulneráveis por muitas vezes possuírem portas de comunicação abertas, sistemas insuficientes de privacidade, proteção e encriptação, falta de atualizações, entre outros (RIBEIRO, 2020).

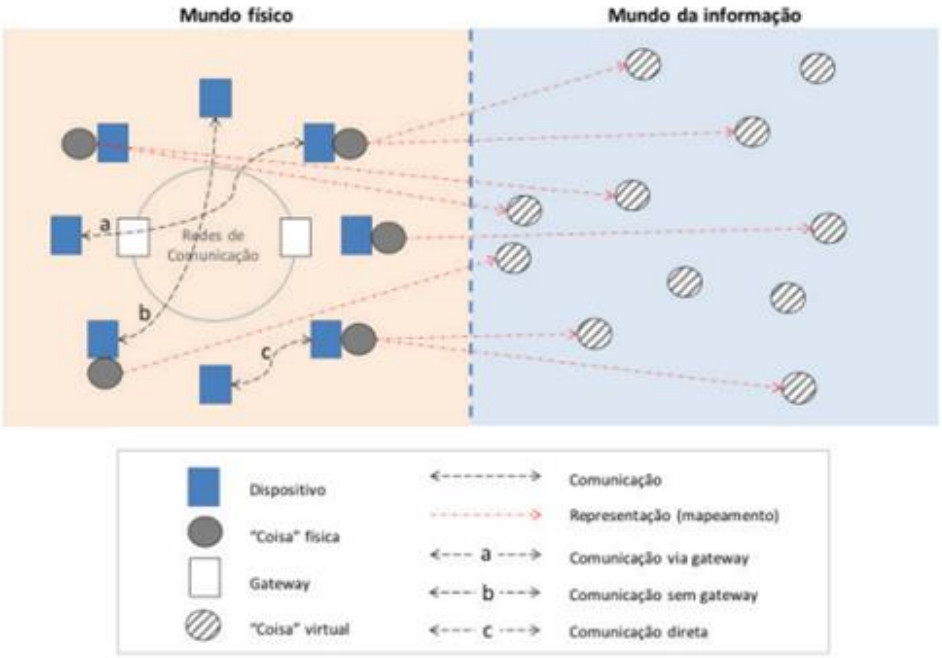
Ribeiro (2020) explica que muitas dessas vulnerabilidades se devem ao fato de os dispositivos de IoT possuírem limitações de *hardware*, como a capacidade de processamento, memória, taxas de transferência reduzidas, uso de protocolos inseguros, entre outros motivos.

2.2 A ARQUITETURA DE IoT

A IoT não é considerada exatamente como uma tecnologia, mas sim um conceito, abrangendo várias tecnologias, plataformas e modelos de negócio e, por esse motivo, é preciso que existam regras básicas que estabeleçam as bases técnicas de IoT, sendo a *International Telecommunication Union* (ITU), o principal órgão a estabelecer essas regras em 2012 (FACCIONI FILHO, 2016). A Figura 2 ilustra uma visão técnica geral da IoT segundo a ITU, apresentando os diversos dispositivos e tecnologias que a compreendem e estão presentes em praticamente todas as definições de organismos e fabricantes.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Figura 2 – Visão técnica geral de IoT segundo a organização ITU.



Fonte: Adaptação de Recommendation ITU-T Y.2060, 2012**.**

A arquitetura de IoT é formada pelos elementos do mundo físico e da informação, de modo que um objeto ou “coisa” do mundo físico pode ter a sua representação no mundo da informação como um objeto ou “coisa” virtual, porém, no mundo da informação existem elementos virtuais que não possuem correspondência ao mundo físico.

Estes objetos são considerados então os dispositivos de IoT que possuem a capacidade mandatória de comunicação e capacidades opcionais, como sensoriamento, atuação, captura de dados, memória e processamento. O objetivo principal desses dispositivos é coletar vários tipos de informações e as encaminharem para as redes de comunicação e informação para que possam ser processados, executando ou não alguma operação (FACCIONI FILHO, 2016).

A comunicação desses dispositivos pode ocorrer de três formas diferentes: i) pela rede de comunicação por meio de um *gateway*; ii) pela rede de comunicação sem o uso de um *gateway* e iii) diretamente, sem passar pela rede de comunicação. Estes tipos de comunicação são presentados na imagem acimas pelos casos “a”, “b” e “c”, respectivamente (FACCIONI FILHO, 2016).

De acordo com as capacidades opcionais dos dispositivos é possível categorizá-los em i) dispositivos de transporte de dados, que estão conectados a um objeto do mundo físico e possibilitam a comunicação indireta entre esse objeto e as redes de comunicação, ii) dispositivos de captura de dados, o qual estão conectados ao objeto e são capazes de ler seus dados e escrever informações, iii) dispositivo sensor/atuador, capaz de detectar e medir informações do ambiente e transformá-las em sinais digitais, ou então transformar sinais digitais oriundos das redes de comunicação em operações

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

nesse objeto e, por fim, iv) dispositivo geral que possui capacidade própria de processamento e comunicação com as redes de comunicação via cabos ou sem fio (FACCIONI FILHO, 2016).

Segundo a ITU, é de responsabilidade das redes de comunicação a transferência de dados dos dispositivos para as aplicações e para outros dispositivos, bem como a transferência de instruções das aplicações para os dispositivos, de maneira eficiente e confiável, fazendo uso das redes existentes, como, por exemplo, a TCP/IP (RECOMMENDATION ITU, 2012).

Com isso, é possível definir a arquitetura da IoT em quatro camadas, sendo elas compreendidas em capacidades de gestão e segurança que garantem a estrutura do todo, como demonstra a Figura 3. Esta arquitetura parte dos elementos básicos da IoT que são a forma como as "coisas" interagem por meio de uma rede de comunicações; nas aplicações que usam as "coisas", recebendo dados e enviando ordens; e no suporte necessário para a interação entre as "coisas" e as aplicações.

Figura 3 – As quatro camadas da arquitetura da IoT propostas pela ITU.

Fonte: Recommendation ITU-T Y.2060, 2012

2.3 CAPACIDADES DE SEGURANÇA DA IoT

Uma vez que o objetivo principal do trabalho é estudar sobre os princípios de segurança e privacidade aplicados em IoT, um foco nas capacidades de segurança será dado em relação a imagem apresentada anteriormente.

Como afirma Ribeiro (2020), a segurança é algo primordial em IoT, uma vez que a tecnologia usada nestes dispositivos tem como principal objetivo recolher informações de forma discreta, porém, em diversos casos são recolhidas informações sensíveis, tanto para as pessoas, como para as organizações, o que implica em uma preocupação ainda maior com segurança e privacidade.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Segundo a ITU (2012), existem capacidades de segurança genéricas e específicas para as aplicações de IoT. As capacidades genéricas são independentes de aplicações e são subdivididas em três camadas:

- Camada de aplicação: responsável pela autorização, autenticação, confidencialidade de dados e proteção da integridade, proteção da privacidade, auditoria da segurança e antivírus;
- Camada de rede: responsável pela autorização, autenticação, confidencialidade dos dados de uso e de sinalização e proteção à integridade de sinalização;
- Camada de dispositivo: responsável pela autorização, autenticação, validade da integridade do dispositivo, controle de acesso, confidencialidade de dados e proteção à integridade.

Já as capacidades específicas de segurança devem ser adotadas por aplicações que possuem requisições especiais, como pagamento móvel, aplicações de segurança patrimonial e física, entre outros (ITU, 2012).

De acordo com Shelby e Bormann (2011), existem pelo menos três grupos de objetivos desejáveis para segurança, sendo eles, confidencialidade, integridade e disponibilidade. A confidencialidade é o requisito que determina que os dados transmitidos possam ser “escutados” e entendidos por elementos participantes da comunicação, de modo que elementos sem autorização saibam da comunicação, mas não tenham acesso ao conteúdo da comunicação. O requisito da integridade determina que os dados não possam ser alterados por elementos da rede sem devida autorização, sendo necessário a implementação de criptografia nas mensagens com posterior verificação no lado do receptor. Esta criptografia é muito importante, pois, um dos ataques comuns de *hackers* é a adulteração de mensagens sem deixar vestígios, o que pode levar a quebra da integridade caso ela não seja aplicada. Por fim, o requisito da disponibilidade determina que os sistemas estejam sempre disponíveis e seguros contra-ataques maliciosos, sendo primordial que as aplicações de IoT identifiquem e tratem problemas de interferências de comunicação em redes sem fio, evitando assim ataques de *Denial of Service* (DoS), muito comum entre *hackers* que atuam nessas vulnerabilidades.

Um dos grandes empecilhos ligados a segurança em IoT está associado aos próprios dispositivos, isso porque grande parte deles possuem limitações de memória, largura de banda, energia e capacidade de processamento, impossibilitando que os mecanismos de segurança utilizados em outros sistemas e equipamentos sejam aplicados a eles (RIBEIRO, 2020). Outro problema que dificulta o controle de privacidade e segurança nos dispositivos de IoT está associado ao ambiente em que muitos deles são utilizados, isso porque muitos são utilizados em ambientes não controlados, o que aumenta o risco de eles serem comprometidos, como, por exemplo, a partir de algum tipo de sabotagem física ou manipulação indevida (RIBEIRO, 2020).

Além do ITU, diversas outras organizações buscam desenvolver regras e princípios básicos a serem seguidos para um desenvolvimento mais seguro de dispositivos de IoT, como o *National Institute of Standards and Technology* (NIST), *European Telecommunications Standards Institute* (ETSI), *European Union Agency for Cibersecurity* (ENISA), entre outros. Como afirma Ribeiro (2020), uma das

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

organizações que merece destaque por suas colaborações é a ENISA, pois ela provê seis documentos diferentes que direcionam o desenvolvimento de IoT em diferentes setores, que são:

- Segurança e Resiliência em Casas Inteligentes: tem o intuito de guiar o desenvolvimento de dispositivos de IoT para ambientes residenciais, de modo que estes sejam protegidos de ameaças cibernéticas em todas as etapas do ciclo de vida do produto (ENISA, 2015).
- Recomendações base para IoT: apresenta as recomendações básicas de cibersegurança para IoT, dando foco às questões de infraestrutura crítica de informação, abrangendo instalações, redes, serviços e equipamentos físicos de tecnologia da informação (ENISA, 2017).
- Boas Práticas de Segurança para IoT: Produção Inteligente, aborda os principais desafios de segurança e privacidade relacionados à evolução dos sistemas e serviços da indústria, que foram acelerados pela introdução de inovações de IoT (ENISA, 2018).
- Convergência Segura de Cloud e Iot: Desafios de Segurança: Combinação de conhecimentos da ENISA em IoT e em segurança em *cloud*, apresentando uma análise dos desafios de segurança e possíveis sugestões de segurança, que fornecedores de dispositivos e provedores de serviços em *cloud* podem considerar (ENISA, 2018).
- Análise de falhas: Requisitos de Grupos: Fornece informações sobre os requisitos de segurança de IoT, mapeando ativos críticos e ameaças relevantes, avaliando possíveis ataques e identificando potenciais boas práticas, além de medidas de segurança a serem aplicadas para proteger os sistemas de IoT (ENISA, 2019).
- Cibersegurança na Indústria 4.0: Documento que tem como objetivo reunir boas práticas para garantir a segurança de IoT no contexto da indústria 4.0, mapeando os desafios relevantes de segurança, privacidade, ameaças, riscos e cenários de ataque. Este documento fornece ainda os principais desafios à adoção das medidas de segurança, segurança na indústria 4.0 e em IoT industrial (ENISA, 2019).

2.4 AMEAÇAS E VULNERABILIDADES EM IoT

Assim como todos os serviços de tecnologia da informação, os dispositivos e sistemas de IoT enfrentam diversas ameaças e vulnerabilidades no dia a dia, sendo os principais e mais críticos apresentados nesta seção.

Como já mencionado anteriormente, a privacidade é um ponto que deve se ter muita atenção, uma vez que as ameaças relacionadas a elas são muitas, como por exemplo a possibilidade de rastreamento da localização do dispositivo, podendo um *hacker* conseguir informações confidenciais desses dispositivos, podendo usá-las para fins ilícitos, como a venda destes dados para monitoria não autorizada.

Outra ameaça frequente é a interceptação e descriptografia das informações trafegadas por uma rede IoT, ataque conhecido como *eavesdropping*. Como forma de lidar com estas ameaças é

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

preciso utilizar algoritmos criptográficos fortes e adequados para cada tipo de dispositivo (RIBEIRO, 2020).

O principal pilar do IoT é a coleta de informação dos sistemas e pessoas que fazem uso dele e, em um mundo em que o conhecimento das preferências de uma pessoa valem cada vez mais, ataques para obtenção destas informações são cada vez mais comuns, sendo estes ataques conhecidos como *data-leakage.* O intuito deste ataque é obter dados confidenciais a partir de dispositivos individuais e pessoais durante o tráfego dessas informações para que posteriormente sejam divulgados para organizações não autorizadas (RIBEIRO, 2020).

Por fim, outra ameaça muito comum e que não se restringe aos dispositivos e sistemas de IoT é a cópia ou substituição do dispositivo, afirma Ribeiro (2020). Neste tipo de ataque, fábricas não confiáveis copiam características físicas, software e configurações de segurança dos dispositivos originais, de modo que os dispositivos copiados sejam vendidos mais baratos no mercado, podendo conter modificações funcionais, incluindo *backdoors*, que são formas de obter acesso ao sistema do dispositivo sem conhecimento do proprietário.

3 CONSIDERAÇÕES FINAIS

De acordo com o objetivo proposto, foi possível observar que os conceitos de IoT ganharam força a partir do final da década de 90, impulsionados principalmente pelos avanços tecnológicos nessa época e hoje fazem parte do nosso dia a dia, em residências, ambientes corporativos e até mesmo vestuário. Há muitos estudos envolvendo a segurança e privacidade, o que pode ser explicado pelo crescente número de dispositivos de IoT no mercado e a preocupação cada vez maior com a segurança da informação devido as novas regulamentações da LGPD, no Brasil. A preocupação com a segurança e privacidade de dispositivos e sistemas de IoT é grande, uma vez que o tráfego de informações por eles é constante e conta muitas vezes com dados sensíveis, sendo esses sistemas alvos de diversas ameaças, como ataques DoS, *eavesdropping*, entre outros. Como forma de prevenir essas ameaças e garantir a segurança e privacidade dos usuários, diversas organizações internacionais, tais como ENISA, NIST e ETSI, regulamentaram regras a serem seguidas durante todo o ciclo de desenvolvimento do produto e de acordo com o ambiente que estes dispositivos serão utilizados, merecendo destaque os documentos criados pela *European Union Agency for Cybersecurity* (ENISA).

Foi possível ainda evidenciar que um dos grandes empecilhos ligados a segurança em IoT está associado aos próprios dispositivos, isso porque grande parte deles possuem limitações de *hardware*, como memória, largura de banda, energia e capacidade de processamento, impossibilitando que os mecanismos de segurança utilizados em outros sistemas e equipamentos sejam aplicados a eles, tornando assim estes dispositivos ainda mais seguros.

É importante ressaltar que não é impossível aplicar bons princípios de segurança e privacidade em IoT, mas é preciso mais cuidado e atenção devido às limitações que esses dispositivos apresentam e o ambiente que estão presentes, já que o risco de comprometimento, como, por exemplo, a partir de algum tipo de sabotagem física ou manipulação indevida é possível.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

4 REFERÊNCIAS

ASHTON, K. That “Internet of Things” Thing - In the real world, things matter more than ideas. **RFID journal**, 2009. Disponível em: http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf. Acesso em: 2 abr. 2022.

ENISA - EUROPEAN UNION AGENCY FOR CYBERSECURITY. **Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures**. Grécia: ENISA, 2017. Disponível em: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot. Acesso em: 3 abr. 2022.

ENISA - EUROPEAN UNION AGENCY FOR CYBERSECURITY. **Good Practices for Security of Internet of Things in the context of Smart Manufacturing**. Grécia: ENISA, 2018. Disponível em: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot. Acesso em: 3 abr. 2022.

ENISA - EUROPEAN UNION AGENCY FOR CYBERSECURITY. **Industry 4.0 Cybersecurity:** Challenges e Recommendations. Grécia: ENISA, 2019. Disponível em: https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations. Acesso em: 3 abr. 2022

ENISA - EUROPEAN UNION AGENCY FOR CYBERSECURITY. **IoT Security Standards Gap Analysis Mapping of existing standards against requirements on security and privacy in the area of IoT**. Grécia: ENISA, 2019. Disponível em: https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis. Acesso em: 3 abr. 2022.

ENISA - EUROPEAN UNION AGENCY FOR CYBERSECURITY. **Security and Resilience of Smart Home Environments:** Good practices and recommendations. Grécia: ENISA, 2015. Disponível em: https://www.enisa.europa.eu/publications/security-resilience-good-practices. Acesso em: 3 abr. 2022.

ENISA - EUROPEAN UNION AGENCY FOR CYBERSECURITY. **Towards secure convergence of Cloud and IoT**. Grécia, 2018. Disponível em: https://www.enisa.europa.eu/news/enisa-news/towards-secure-convergence-of-cloud-and-iot. Acesso em: 3 abr. 2022

FACCIONI FILHO, M. **Internet das Coisas.** Santa Catarina: UnisulVirtual, 2016. Disponível em: https://www.researchgate.net/profile/Mauro-Fazion-Filho/publication/319881659_Internet_das_Coisas_Internet_of_Things/links/59c038d5458515e9cfd54ff9/Internet-das-Coisas-Internet-of-Things.pdf. Acesso em: 3 abr. 2022.

LOPEZ RESEARCH, L. L. C**. Uma introdução à Internet das Coisas (IoT)**. São Francisco: [s. n.], 2013. Disponível em: https://www.cisco.com/c/dam/global/pt_br/assets/brand/iot/iot/pdfs/lopez_research_an_introduction_to_iot_102413_final_portuguese.pdf. Acesso em: 2 abr. 2022.

MAGRANI, E. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018.

MARCONI, M. A.; LAKATOS, E. M. **Metodologia do trabalho científico:** procedimentos básicos, pesquisa bibliografia, projeto e relatório, publicações e trabalhos científicos. 6. ed. São Paulo: Atlas, 2006.

RECOMMENDATION ITU-T Y.2060. **Overview of the Internet of things**. ITU-T – International Telecommunication Union, 2012. Disponível em: https://www.itu.int/rec/T-REC-Y.2060-201206-I. Acesso em: 3 abr. 2022.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

RIBEIRO, A. J. J. **Problemas de Segurança na Internet das Coisas**. 2020. 132 f. Dissertação (Mestrado em Cibersegurança e Informática Forense) – Escola Superior de Tecnologia e Gestão, Leiria, 2020.

SANTOS, B. P.; SILVA, L. A. M.; CELES, C. S. F. S.; BORGES, J. B; PERES. B. S.; VIEIRA, M. A. M.; VIEIRA, L. F. M.; GOUSSEVSKAIA, O. N.; LOUREIRO, A. A. F. **Internet das Coisas:** da Teoria à Prática, Belo Horizonte: UFMG, 2016. Disponível em: https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/internet-das-coisas.pdf. Acesso em: 4 abr. 2022.

SHELBY, Z.; BORMANN, C. **6LoWPAN:** The wireless embedded Internet. London: John Wiley & Sons, 2011. Vol. 43. Disponível em: https://www.chercheinfo.com/uploads/-bf6badef8f.pdf. Acesso em: 6 abr. 2022.

TIBCO Software Inc. **O que é a Internet das Coisas (IoT).** USA: Tibco, 2022. Disponível em: https://www.tibco.com/pt-br/reference-center/what-is-the-internet-of-things-iot. Acesso em: 2 maio 2022.