UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS VII PATOS-PB
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS - CCEA
CURSO DE BACHARELADO EM CIÊNCIAS DA COMPUTAÇÃO

DANIEL DANTAS BARBOZA

INTERNET DAS COISAS APLICADA NA EDUCAÇÃO E OS PERIGOS NA FALTA DE SEGURANÇA DOS SEUS DISPOSITIVOS: uma Revisão Sistemática da Literatura

PATOS - PB
2022

DANIEL DANTAS BARBOZA

INTERNET DAS COISAS APLICADA NA EDUCAÇÃO E OS PERIGOS NA FALTA DE SEGURANÇA DOS SEUS DISPOSITIVOS: uma Revisão Sistemática da Literatura

Trabalho de Conclusão de Curso apresentado ao Departamento de Computação da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Graduação em Ciência da Computação.

Área de concentração: Internet das Coisas.

Orientador: Prof. Me. Francisco Anderson Mariano da Silva.

Co-orientador: Prof. Me. Geovane de Souza Ferreira Junior.

PATOS - PB
2022

É expressamente proibido a comercialização deste documento, tanto na forma impressa como eletrônica. Sua reprodução total ou parcial é permitida exclusivamente para fins acadêmicos e científicos, desde que na reprodução figure a identificação do autor, título, instituição e ano do trabalho.

B239i Barboza, Daniel Dantas.

Internet das coisas aplicada na educação e os perigos na falta de segurança dos seus dispositivos [manuscrito] : uma revisão sistemática da literatura / Daniel Dantas Barboza. - 2022.

47 p.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Computação) - Universidade Estadual da Paraíba, Centro de Ciências Exatas e Sociais Aplicadas , 2022.

"Orientação : Prof. Me. Francisco Anderson Mariano da Silva , Coordenação do Curso de Computação - CCEA."

"Coorientação: Prof. Me. Geovane de Souza Ferreira Júnior , Coordenação do Curso de Computação - CCEA."

1. Internet das coisas. 2. Segurança da informação. 3. Ferramentas tecnológicas. 4. Ambiente escolar. I. Título

21. ed. CDD 004.678

Elaborada por Edson M. A. Monteiro - CRB - CRB 15/743 BSC7/UEPB

DANIEL DANTAS BARBOZA

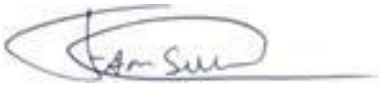
INTERNET DAS COISAS APLICADA NA EDUCAÇÃO E OS PERIGOS NA FALTA DE SEGURANÇA DOS SEUS DISPOSITIVOS: uma Revisão Sistemática da Literatura

Trabalho de Conclusão de Curso apresentado ao Curso de Bacharelado em Ciência da Computação da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção do grau de Bacharel em Ciência da Computação.

Área de concentração: Internet das Coisas.

Aprovado em 10/11/2022

BANCA EXAMINADORA



Prof. Me. Francisco Anderson Mariano da Silva
(Orientador)

Prof. Me. Geovane de Souza Ferreira Júnior
(Coorientador - CCEA)

Prof. Dr. Wellington Candeia de Araujo
(Examinador - CCT)

Prof. Vinicius Reuteman Feitoza Alves de Andrade
(Examinador - CCEA)

Dedico este trabalho em memória da minha querida avó (Maria de Fátima Dantas Martins) e a todos da minha família e amigos que me apoiaram nesta caminhada.

AGRADECIMENTOS

Primeiramente agradeço a Deus pela oportunidade de chegar até aqui com saúde, pela segurança em toda essa caminhada e pela força para enfrentar todas as dificuldades.

A minha avó Maria de Fátima Dantas Martins (*in memoria*), por todo carinho e torcida para que eu pudesse ser alguém melhor.

Ao meu pai Paulo Barbosa e minha mãe Milanne Kherlle, por todo incentivo e apoio para encarar todos os desafios e dificuldades, e por todo aprendizado que me fizeram ser quem sou hoje.

Ao meu irmão Paulo Júnior, por me ajudar a escolher esse curso em um momento de indecisão e por ser um exemplo na família de como ser uma pessoa melhor por meio do estudo no qual me espelho todos os dias.

Aos meus irmãos Aleff Dantas e Míryam Dantas por estarem presentes na minha vida e torná-la melhor.

Ao meu orientador e professor Francisco Anderson Mariano da Silva, por toda a assistência e profissionalismo, que por meio de suas correções, dicas e incentivos tornaram possível a realização deste trabalho.

A esta universidade por todo apoio e por proporcionar um ambiente para que eu pudesse me desenvolver.

A minha namorada Luana, por toda paciência, compreensão e assistência para que eu pudesse desenvolver este trabalho.

E por fim, a todos os meus amigos que estiveram me acompanhando durante essa trajetória.

RESUMO

Contexto: Com a evolução da tecnologia, o ambiente escolar vem sofrendo modificações para se adaptar ao mundo moderno, e após um período pandêmico, se fez necessário olhar ainda mais para ferramentas tecnológicas e novos conceitos da tecnologia, pois por meio delas podemos desenvolver novas formas de aprendizagem e melhorar a qualidade de ensino. A Internet das Coisas (do inglês *Internet of Things* - IoT) pode modificar a forma atual de ensino e tornar o processo mais eficiente, porém é necessário cuidados na aplicação dessa tecnologia uma vez que o ambiente pode sofrer ataques caso não seja aplicado de forma adequada, priorizando a segurança. **Objetivo**: Esta pesquisa tem como objetivo apresentar uma Revisão Sistemática da Literatura (RSL) da IoT quando aplicada na educação e apresentar os perigos na falta de segurança dos dispositivos conectados além de apresentar a importância de manter um ambiente seguro a fim de evitar ataques que podem expor informações importantes que deveriam estar protegidas. **Metodologia**: Foi utilizado a RSL, pois é uma metodologia que propõe a realização de buscas por estudos, visando a cobertura de estudos consistentes e publicações adequadas sobre um determinado tema, assim sendo um método justo e não tendencioso. Por meio desta RSL, foram utilizados o Google Acadêmico e Scielo como base de dados com estudos entre o período de 2007 até 2022, na qual foram analisadas 7 publicações relevantes. **Resultados:** Como resultado, foram investigadas as diferentes publicações buscando encontrar os perigos na falta de segurança dos dispositivos IoT para que possamos ter cuidado ao aplicá-la no contexto educacional e saber sobre sua importância, contribuindo para futuras pesquisas relacionadas ao tema.

Palavras-Chave: Internet das Coisas. Segurança da Informação. Revisão Sistemática da Literatura. Educação.

ABSTRACT

Context: With the evolution of technology, the school environment has been undergoing changes to adapt to the modern world, and after a pandemic period, it became necessary to look even more to technological tools and new concepts of technology, because through them we can develop new ways of learning and improve the quality of teaching. The Internet of Things (IoT) can change the current way of teaching and make the process more efficient, but care must be taken when applying this technology, since the environment can suffer attacks if it is not applied properly, prioritizing security. **Objective:** This research aims to present a systematic review of the literature of the IoT when applied to education and to present the dangers in the lack of security of connected devices, besides presenting the importance of maintaining a secure environment in order to avoid attacks that may expose important information that should be protected. **Methodology:** The Systematic Literature Review (RSL) was used, because it is a methodology that proposes the search for studies, aiming at the coverage of consistent studies and adequate publications about a certain theme, thus being a fair and unbiased method. Through this RSL, Google Academic and Scielo were used as a database with studies between the period from 2007 to 2022, in which 7 relevant publications were analyzed. **Results:** As a result, the different publications were investigated seeking to find the dangers in the lack of security of IoT devices so that we can be careful when applying it in the educational context and know about its importance, contributing to future research related to the topic.

Keywords: Internet of Things. Information Security. Systematic Literature Review. Education.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

DoS	Denial-of-Service
IOE	Internet of Everything
IOT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LGPD	Lei Geral de Proteção de Dados Pessoais
RFID	Radio-Frequency IDentification
RSL	Revisão Sistemática da Literatura
SSF	Smart Security Framework
TIC	Tecnologias da Informação e Comunicação

SUMÁRIO

1 INTRODUÇÃO

Com a evolução da tecnologia, o ambiente escolar vem sofrendo modificações para se adaptar ao mundo moderno, e após um período pandêmico, se fez necessário olhar ainda mais para ferramentas tecnológicas, pois por meio delas podemos desenvolver novas formas de aprendizagem e melhorar a qualidade de ensino.

A Internet das Coisas (do inglês *Internet of Things* - IoT) é integrante das chamadas Tecnologias da Informação e da Comunicação (TIC), que consistem no tratamento da informação combinados com processos de transmissão e de comunicação, o que torna o processo de ensino mais eficiente, e estão cada vez mais presentes na educação (SAIBA..., 2018). Porém, é necessário alguns cuidados na aplicação dessa tecnologia pois num ambiente conectado é preciso que toda a rede se mantenha segura e longe de ataques.

De acordo com Magrani (2018), a IoT pode ser entendido como um ambiente de objetos físicos interconectados com a *internet* por meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente (Ubíqua), voltado para a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia.

Magrani (2018) também diz que todas as definições de IoT têm algo em comum, que seria como elas se concentram em como computadores, sensores e objetos interagem uns com os outros e processam informações/dados em um contexto de hiperconectividade. O termo *Internet of Things* (IoT) foi definido originalmente em 1999 por Kevin Ashton, professor da *Massachusetts Institute of Technology*.

Podemos perceber que a IoT vem para simplificar, automatizando processos que facilitarão a vida das pessoas. Isso tem a ver com a evolução que a tecnologia vem trazendo ao longo dos anos e uma das mais importantes se chama *Internet*, que revolucionou a forma que nos comunicamos, além de fazer com que possamos enviar e receber dados seja esses com pessoas, aplicativos ou máquinas.

Ferrasi *et al*. (2016) dizem que são inúmeras as possibilidades que podemos aplicar na prática pedagógica onde os alunos em vez de abstrair o conhecimento passam a instanciá-lo por meio da interconexão desses sensores com dispositivos

móveis criando situações reais alinhadas a ambientes virtualizados com o uso de um simples *smartphone*.

Ferrasi *et al*. (2016) também afirmam que as práticas pedagógicas a IoT pode proporcionar recursos a gestão acadêmica, como o gerenciamento de livros em bibliotecas por etiquetas *Radio-Frequency IDentification* (RFID), interação direta com alunos e professores por meio de dispositivos móveis e sensores de proximidade, automatizando processos operacionais como frequência de alunos, informativos sobre atividades, eventos, notas e desempenho nas disciplinas, detecção de pessoas em ambientes controlados, solicitações diversas entre alunos, professores e direção acadêmica.

Além disso, Ferrasi *et al*. (2016) diz que, outra aplicação muito provável será a inclusão de pessoas com necessidades especiais com aplicações especializadas apoiadas ao uso das tecnologias assistivas.

Nota-se que podem ser muito os benefícios que a IoT pode trazer no ambiente educacional porém o uso de toda essa tecnologia pode atrair a atenção de cibercriminosos para invasões, ciberespionagem, roubo de dados. Para evitar isso é necessário investir em segurança no ambiente IoT pois quanto mais seguro for mais as pessoas poderão usufruir da tecnologia sem se preocupar.

A IoT tem o desafio de focar na segurança e se adaptar a leis como a Lei Geral de Proteção de Dados Pessoais (LGPD), que segundo Agostinelli (2018) visa fortalecer a proteção das informações pessoais e a transparência na forma de tratamento e armazenamento de dados.

O trabalho em questão, tem como objetivo gerar uma RSL unindo estudos sobre a IoT com aplicação na educação, assim como apresentar os perigos na falta dessa segurança. Pensando nisso, busca-se responder a seguinte pergunta: Quais são os perigos na falta de segurança dos dispositivos na IoT quando aplicada na Educação?

1.1 Problemática

A segurança é fundamental em qualquer área de nossas vidas, a falta dela pode nos trazer diversos prejuízos desde financeiros até emocionais. Na IoT não é diferente, trazendo para o contexto educacional, pode trazer diversos benefícios, mas assim como qualquer tecnologia/conceito que tem dispositivos conectados à *Internet*, traz consigo perigos que devemos nos atentar e prevenir para que seja evitado problemas de segurança, e ocorram como por exemplo, vazamento de dados dos alunos, que podem conter informações sensíveis.

Souza (2019) diz que no cenário iminente da IoT são inevitáveis os problemas de segurança de todas as ‘coisas’ conectadas e que é preciso que os dispositivos e sistemas para IoT sejam projetados e desenvolvidos seguindo técnicas de segurança e de privacidade e é preciso que os usuários sejam devidamente instruídos a utilizar equipamentos compatíveis com os princípios básicos de segurança.

Ribeiro (2020) destaca o desafio associado à segurança na IoT, pois a tecnologia usada concebe os sensores para recolher informações de forma discreta do ambiente. Porém, muitas dessas informações recolhidas são informações sensíveis tanto para pessoas como para organizações.

Diante dessa problemática, um dos pontos que podemos perceber é que para prevenirmos e até mesmo resolver problemas de segurança na IoT, precisamos conhecer quais os perigos que ela pode apresentar, sabendo como um atacante pode agir, assim melhorando a segurança. Por meio de pesquisas relacionadas a soluções para essa questão, este trabalho une informações que buscam responder ao problema de pesquisa.

1.2 Justificativa

Baseando-se nas informações descritas acima, será realizada uma análise de como a IoT está sendo aplicada no ambiente educacional, e como a segurança pode ser aplicada para evitar invasões, além de alertar sobre os perigos na falta dela. A segurança é um dos principais pontos de qualquer tecnologia, e é de suma importância haver um ambiente seguro em que os usuários possam estar transmitindo informações sem que sejam prejudicados por invasões.

A apresentação desse trabalho será no formato de RSL, sendo essa uma relevante ferramenta de pesquisa e de auxílio a comunidade científica e acadêmica pois por meio dela podemos obter importantes dados sobre a segurança na IoT no contexto educacional.

Foi optado pela RSL pois essa garante a confiabilidade e a qualidade técnica e científica do trabalho. Segundo Galvão e Ricarte (2019) revisar a literatura permite observar possíveis falhas nos estudos realizados, conhecer os recursos necessários para a construção de um estudo com características específicas, desenvolver estudos que cubram brechas na literatura trazendo real contribuição para um campo científico. Segundo Kitchenham e Charters (2007), uma RSL é uma forma de estudo que usa uma metodologia para identificar, avaliar e interpretar todas as evidências disponíveis que são relevantes para uma questão particular de maneira imparcial e repetível. Sendo assim, esta RSL foi desenvolvida para contribuir no estudo da segurança na área da IoT para o contexto educacional.

Por meio dos resultados desse trabalho, espera-se apresentar a IoT aplicada na Educação, e mostrar sobre os perigos existentes na falta de segurança dos dispositivos, para que possa ser dada mais importância ao assunto. Com isso, esse trabalho irá analisar os trabalhos de pesquisadores na área e trazer uma visão geral sobre o assunto.

1.3 Objetivos

1.3.1 *Objetivo geral*

O propósito deste trabalho é apresentar uma RSL sobre a aplicação da IoT na educação, com o objetivo de mostrar sobre os perigos na falta de segurança dos dispositivos IoT, apresentando a importância de ter dispositivos cada vez mais focados na segurança.

1.3.2 *Objetivos específicos*

- Apresentar os benefícios da IoT quando aplicada na educação;
- Identificar quais os desafios que a IoT vem enfrentando para melhorar a segurança;
- Identificar como ter uma aplicação da segurança de IoT eficiente;
- Expor os perigos que podem haver.

2 REFERENCIAL TEÓRICO

Neste capítulo, será tratado o referencial teórico deste trabalho. Onde estão estabelecidos os seguintes temas: Revisão Sistemática da Literatura, Internet das Coisas (IoT), IoT aplicada na educação, segurança e privacidade na IoT, e ameaças e vulnerabilidades na IoT.

2.1 Revisão Sistemática da Literatura

Segundo Kitchenham e Charters (2007), uma RSL é uma forma de estudo que usa uma metodologia para identificar, avaliar e interpretar todas as evidências disponíveis que são relevantes para uma questão particular de maneira imparcial e repetível. As RSL são úteis para integrar as informações de um conjunto de estudos realizados separadamente sobre determinada terapêutica/intervenção, que podem apresentar resultados conflitantes e/ou coincidentes, bem como identificar temas que necessitam de evidência, auxiliando na orientação para investigações futuras(SAMPAIO; MANCINI, 2007).

Donato e Donato (2019) afirmam que a RSL é reprodutível e tende a ser imparcial. Visa reduzir o viés por meio do uso de métodos explícitos para realizar uma pesquisa bibliográfica abrangente e avaliar de forma crítica os estudos individuais. Assim, em contraste com a revisão tradicional ou narrativa, a RSL responde a uma questão de investigação bem definida e é caracterizada por ser metodologicamente abrangente, transparente e replicável.

Para Schütz, Santana e Santos (2011), a RSL exige um esforço muito maior do que as opiniões tradicionais, que por muitas vezes observamos em revisões convencionais ou tradicionais. Sua grande vantagem é fornecer informações sobre os efeitos de alguns fenômenos por meio de uma ampla gama de configurações e métodos empíricos. Ou seja, os estudos dão resultados consistentes e as fontes de variações podem ser estudadas.

Como afirmam Galvão e Ricarte (2019), a RSL está focada no seu caráter de reprodutibilidade por outros pesquisadores, que irá apresentar de forma explícita, as bases de dados bibliográficos que foram consultadas, as estratégias de busca empregadas em cada base, o processo de seleção dos artigos científicos, os critérios de inclusão e exclusão dos artigos e o processo de análise de cada artigo.

Galvão e Ricarte (2019) completam que, de forma geral, a RSL possui um alto nível de evidência e se constitui em um importante documento para tomada de decisão nos contextos públicos e privados. Dito de um outro modo, a RSL é uma pesquisa científica composta por seus próprios objetivos, problemas de pesquisa, metodologia, resultados e conclusão, não se estabelecendo apenas como uma mera introdução de uma pesquisa maior.

De acordo com Dermeval, Coelho e Bittencourt (2020), as RSL devem ser executadas de acordo com uma estratégia de busca previamente definida e que permita que sua completude seja avaliada por outros pesquisadores, deve ser considerado um período específico para a busca, recuperar trabalhos que atendam palavras-chaves pré determinadas, além de definir de forma clara os critérios de inclusão e exclusão dos trabalhos buscados.

Sampaio e Mancini (2007), completam que é importante publicar nas RSL os aspectos positivos e negativos das intervenções/tratamentos, pois isso só aumentará o conhecimento a respeito da sua eficácia e da sua limitação.

2.2 Internet das Coisas (IOT)

A tecnologia está mudando rapidamente a forma como interagimos com o mundo à nossa volta. Com o objetivo de atender às mais novas demandas dos consumidores, as empresas estão desenvolvendo hoje dispositivos com interfaces tecnológicas que seriam inimagináveis há uma década (MAGRANI, 2018).

Portanto, os dispositivos IoT, em sua essência, nada mais são do que pequenos computadores ou microcomputadores que se encontram conectados à internet e a nuvem, que vem com objetivo de buscar facilitar ou complicar ainda mais as nossas vidas (HAYASHI; MORAES, 2021).

Para Santos *et al*. (2016), a IoT é uma extensão da internet atual, que irá proporcionar aos objetos do dia a dia a capacidade computacional e de comunicação de se conectarem à Internet.

Carrion e Quaresma (2019) definem a IoT como um ecossistema que conecta objetos físicos por meio de um endereço de *Internet Protocol* (IP) ou outra rede, para trocar, armazenar e coletar dados para consumidores e empresas por meio de uma aplicação de *software*. Apontando a transformação dos dados de um objeto inteligente para os consumidores finais, o fluxo de dados da IoT pode ser

entendido como, primeiramente, sensores em máquinas, pois os sensores ‘sentem’ o entorno do ambiente e coletam os dados. Segundo, esses dados são transportados a partir das máquinas conectadas e armazenados e analisados por meio de computação em nuvem, um Centro de Dados (*Cloud*).

Carrion e Quaresma (2019) completam que, depois, as aplicações irão controlar os dados analisados e fornecer serviços ao usuário final. E por fim, o usuário final compartilha as informações úteis com serviços e outras pessoas.

Ashton (2009) destaca a importância da IoT dizendo que se tivéssemos computadores que soubessem tudo sobre as coisas, aprendendo apenas com os dados que são coletados sem ajuda do ser humano, poderíamos rastrear e contar tudo além de reduzir muito o desperdício, a perda e o custo. Além disso, poderíamos saber quando as coisas precisavam ser reparadas, substituídas, e se elas estavam boas o suficiente. Ele também destacou a necessidade de capacitar os computadores com seus próprios meios de coletar informações, para que assim eles possam ouvir, cheirar e ver o mundo sem precisar da ajuda de alguém.

Magrani (2018) afirma que os objetos inteligentes e interconectados podem nos ajudar na resolução de problemas reais. No que se refere aos consumidores, os produtos que estão integrados com a tecnologia da IoT possuem diversas funções nas mais variadas áreas como eletrodomésticos, meios de transporte e brinquedos além de peças de vestuário que integram uma categoria denominada *wearables*. Magrani (2018) diz que as tecnologias vestíveis fazem conexão uns aos outros e produzem informações sobre os usuários, sendo um dos principais produtos as pulseiras e tênis que monitoram a atividade física do usuário, assim como relógios e óculos inteligentes.

Segundo Zuin e Zuin (2016), a IoT representa um novo momento revolucionário da história da humanidade e que os efeitos dessa transformação já começam a ser visualizados nas mais variadas esferas, inclusive a educacional.

Zuin e Zuin (2016) também afirmam que os mundos material e informacional que estão se fundindo, por meio da interface comunicacional entre objetos e, objetos e pessoas, proporcionam o acesso aos dados de uma forma inédita na história da produção tecnológica. A tecnologia atual possibilita contactar não somente a origem da produção de objetos e relações humanas, como também respectivos históricos de transformações na medida que interagem com outros objetos e pessoas.

Lacerda (2015) diz que a IoT afeta a humanidade em diferentes escalas. Envolvendo desde nanochips implantados em seres vivos até objetos de uso comum que estão interconectados, equipados com RFID com a capacidade de trocar informações entre si, com as pessoas ou com o ambiente, até cidades inteiras que são projetadas para serem totalmente conectadas e automatizadas.

Lacerda (2015) também diz que as formas de manifestação da IoT são heterogêneas, isso inclui dispositivos de múltiplos propósitos (celulares, *tablets*, relógios e óculos inteligentes) e dispositivos especializados (sensores de temperatura, dispositivos ativos e passivos, etc.) que suportam uma variedade de plataformas de *software* e *hardware*.

Hayashi e Moraes (2021), dizem que a IoT tem subsistemas que envolvem basicamente três partes: a rede, que é uma camada de comunicação onde os dispositivos estarão conectados. Nesta camada, normalmente utilizamos tecnologias como Wi-Fi e *Bluetooth* ou mesmo alguns sistemas de comunicação de sensores que utilizam baixa potência, como o ZigBee. Em termos de arquitetura, essa camada digitaliza e transfere dados por meio de canais de comunicação seguros para sistemas que tratam esses dados. Outra parte é a plataforma que é responsável por transmitir os dados da camada de rede onde é possível encontrar os dispositivos. E por fim, a terceira parte é a aplicação, sendo essas relacionadas aos sensores da IoT, ela faz uso dos dados processados na camada anterior. Essa camada irá constituir toda a interface do usuário, normalmente as aplicações estão hospedadas na nuvem e são acessadas via aplicativos ou pela web.

Gubbi *et al*. (2013) afirma que para uma visão completa de IoT, é essencial uma computação eficiente, segura, escalável e recursos de armazenamento. Ele diz que a computação em nuvem é o paradigma mais recente que surgiu e promete serviços confiáveis por meio de *Data Centers* de última geração baseados em tecnologias de armazenamento virtualizado.

Hayashi e Moraes (2021) mostram que o ZigBee, um padrão aberto definido para comunicação entre dispositivos utilizando tecnologias de rede sem fio, é atualmente utilizado por milhares de dispositivos IoT e que o protocolo ZigBee é seguro e estável, o que garante a sua adoção. Os dispositivos ZigBee se conectam normalmente utilizando um roteador de um lado, que se comunica via rádio ZigBee e, do outro, conecta os dispositivos à *internet*.

Farahani (2011) diz que o ZigBee não é a melhor escolha para ser implementado à *internet* caso a taxa de transmissão seja de qualidade superior a 1Mbps, pois essa é a taxa de dados do ZigBee, que é muito baixa, mais baixa até mesmo que *Bluetooth* e Wi-fi. Porém, se o objetivo é enviar e receber dados simples, como temperatura, umidade, o ZigBee fornece a maior potência e a solução mais rentável, já que também apresenta um baixo consumo de energia.

Cisco Ibgs (2011) menciona que várias barreiras têm o potencial de retardar o desenvolvimento da IoT, sendo as três maiores a implantação de *Internet Protocol version 6 (*IPv6), a alimentação dos sensores e um acordo de padrões. Os bilhões de novos sensores exigirão endereços de *Internet Protocol* (IP), na implantação do IPv6 há uma facilidade no gerenciamento de redes devido a recursos de auto configuração e oferece recursos de seguranças aprimorados, já o *Internet Protocol version 4 (*IPv4) havia ficado sem endereços em fevereiro de 2010, e essa situação tende a diminuir o progresso da IoT.

Cisco Ibgs (2011) completa que, com relação a alimentação dos padrões, os sensores deverão ser autossustentáveis para que possam atingir seu potencial completo, pois seria como trocar as baterias de bilhões de dispositivos implantados no planeta inteiro. Por fim, o terceiro problema, que são os padrões, que ainda que haja muitos progressos na área de normas técnicas, ainda não é o suficiente.

2.3 IoT aplicada na Educação

Gasque e Casarin (2016), afirmam que a aprendizagem escolar está em transformação e que nunca se discutiu tanto sobre melhores práticas em salas de aula e os requisitos para potencializar a aprendizagem. Também afirmam que para essas mudanças há razões pedagógicas e tecnológicas.

Dentre essas tecnologias podemos citar a IoT, que está cada vez mais presente no ambiente educacional. A IoT pode ser usada para desenvolver laboratórios virtuais online para diversas áreas da educação, as instituições de ensino podem implementar esses laboratórios e possibilitar um fácil acesso de ensino a distância, até mesmo para especializações técnicas. Nesse contexto, entra o importante papel da IoT, que pode fornecer a estrutura adequada para o desenvolvimento de plataformas para um laboratório virtual (CORNEL, 2015).

Gul *et al*. (2017), dizem que a tecnologia está desempenhando um papel para a melhoria da educação em todos os níveis, incluindo o ensino escolar. Do aluno ao professor, da sala de aula ao campus, tudo pode receber o benefício dessa tecnologia. Outra forma de entender o impacto da IoT na educação é por meio do uso de sensores. Por exemplo, o produto da Twine da *Super Mechanical's*, permite que usuários veiculem quase qualquer objeto físico a uma rede local.

O Twine integra sensores com um serviço baseado em nuvem, que permite uma fácil configuração. Basta apontar o Twine para uma rede Wi-Fi e os sensores são imediatamente reconhecidos pelo aplicativo web, que mostra o que os sensores veem em tempo real (GUL, *et al*. 2017).

Para Claro (2016), o conceito por trás da IoT prevê a conexão de tudo o que nós usamos. Ele diz que se levarmos esse conceito para dentro dos portões da escola, podemos pegar alguns exemplos simples, como transformar um celular dos alunos em algo valioso de acompanhamento da vida escolar. Ele afirma que ao conectar diferentes espaços e objetos da escola, um aluno pode utilizar o celular para acessar laboratórios, verificar a disponibilidade de livros na biblioteca, marcar reuniões ou até comprar lanches. Isso tudo ficaria registrado, ao mesmo tempo em que haveria sensores no material escolar que poderiam contabilizar ou acompanhar o seu trajeto de volta para casa.

Claro (2016) ainda afirma que a integração desses objetos à *internet* permite registrar as preferências dos alunos e reunir um grande volume de dados, como a quantidade de vezes que ele comprou doces na cantina ou chegou atrasado na escola. Reunindo esses dados em uma plataforma adequada, seria possível levar informações qualificadas para gestores, professores ou pais tomarem decisões.

Para Galegale *et al*. (2016), um dos potenciais benefícios da IoT está na possibilidade de melhor adaptação diante das mudanças no ambiente, assim como mais embasamento no processo de tomada de decisão.

Com isso, Araujo, Galhardo e Santos (2019) acreditam que com a utilização dos conceitos de IoT na interface das plataformas de ensino e acervos bibliográficos digitais, podem ser gerados dados sobre os acessos, frequências e sobre as demandas dos estudantes sobre os conteúdos que foram explorados. Também afirmam que dessa forma, os dados que foram gerados servirão como base para os atores educacionais acompanharem melhor o desenvolvimento do processo no

ensino-aprendizado e complementarem o conjunto de conteúdo das instituições em que atuam.

Segundo Zuin e Zuin (2016), a comunicação onipresente entre os mundos físico e informacional proporcionada pela IoT, já ocasiona numa forma de repensar como professores elaboram estratégias didáticas em relação ao modo com as informações serão apreendidas e aprendidas pelos alunos no processo de ensino-aprendizagem.

Para Tarouco *et al*. (2017) aprimorar a educação é uma preocupação de todos pois isso resulta em melhores condições sociais e econômicas para as comunidades e para todo o país. Ainda afirmam que os métodos educacionais têm sido impactados pela disseminação da TIC e de ambientes virtuais que agora são comuns nas escolas e universidades, o que permite acesso à informações e serviços. Pruet *et al*. (2015) afirmam que graças às tecnologias IoT também é plausível possibilitar acesso e controle de processos ou eventos locais ou remotos, o que enriquece a experiência de aprendizagem.

Silva, Braga e Calado (2017) afirmam que, são possíveis inúmeras aplicações quando utilizamos a tecnologia IoT em cenários educacionais. Para eles, é possível que a frequência dos alunos seja realizada de forma automática e os objetos utilizados para algum tipo de prática do aprendizado sejam corretamente identificados e localizados, já com as tecnologias vestíveis como pulseiras, relógios e camisas seja obtido dados sobre as condições físicas, psicológicas e biológicas dos estudantes.

O gerenciamento adaptaria o aprendizado ao contexto do aluno, aumentando o engajamento e a colaboração entre professores e estudantes, além disso permite aos educadores ações mais dinâmicas na sala de aula e com isso, aprimorar o processo de ensino-aprendizagem (SILVA; BRAGA; CALADO, 2017).

Zuin e Zuin (2016) alegam que, a presença de câmeras nas salas de aula cumpre muito bem a função de disciplinar não só os alunos, como também os professores, sendo que ambos se transformam em caricaturas de si mesmos, pois, na condição de atores, representam seus papéis para a plateia que os assiste por meio de uma transmissão *on-line*. Com a justificativa dos diretores das instituições escolares de que, graças às câmeras, os pais podem acompanhar o aprendizado de seus filhos em quaisquer tempos e espaços, o autor chama de panóptico eletrônico

que permite fazer com que a própria autoridade do professor seja subsumida à da câmera.

Por fim, para o futuro da rede IoT, a tendência é de que as salas de aula se tornem globais, sendo acessadas e controladas por toda a Internet. Para isso, já existe uma nova versão da IoT, que está sendo chamada de IoE (Internet de Todas as Coisas ou *Internet of Everything*), que busca integrar, além dos objetos físicos, pessoas, processos e dados em uma rede pervasiva global. Essa integração deverá tornar-se conexões mais relevantes e essenciais para aplicações na área de educação, o que possibilita uma experiência mais rica e gera diversas oportunidades de negócios (SILVA; BRAGA; CALADO, 2017).

2.4 Segurança e privacidade na IoT

Segundo Hayashi e Moraes (2021), não devemos tratar a segurança em IoT diferentemente de como fazemos com outras tecnologias, devemos sempre abordar o aspecto tecnológico, o aspecto de processos e as pessoas. Isto é, os fundamentos de segurança e a forma como realizar um trabalho de maneira segura não irão mudar, mas precisam ser adaptados ao uso dessas tecnologias. Desde que obedeçam aos princípios fundamentais de segurança, definidos pela tríade CID (Confidencialidade, Integridade e Disponibilidade), em inglês *CIA Triad* (*Confidentiality, Integrity and Availability*) .

Chicarino *et al*. (2017), afirmam que a segurança e privacidade são princípios essenciais de qualquer sistema de informação. Nos referimos a segurança como a combinação de Integridade, Disponibilidade e Confidencialidade. Também afirmam que a privacidade pode ser definida como o direito que um indivíduo tem em compartilhar suas informações.

Como apontam Hayashi e Moraes (2021), a CIA Triad define esses três fundamentos básicos da segurança da informação como:

- **Confidencialidade:** é o modo de assegurar que as informações trocadas entre os dispositivos sejam trafegadas de um modo seguro, garantindo que apenas pessoas autorizadas tenham acesso a tal informação. Na IoT, a confidencialidade deve incorporar duas grandes áreas, sendo que a primeira é garantir que a informação trafegue de forma segura entre os distintos

sistemas de comunicação, conhecido por dados em movimento. A segunda é como garantir que os armazenados, ou em descanso, estejam protegidos.

- **Integridade:** consiste em garantir que uma determinada ação executada pelo sistema ocorra de forma íntegra, ou seja, durante o processamento, o fluxo e os dados da informação sejam coerentes, que não tenham sido alterados de forma proposital. Os controles de integridade garantem que uma operação ou o estado do dispositivo sejam mantidos íntegros durante toda a realização.
- **Autorização:** no conceito de autorização, em um plano mais amplo, também irá incorporar a autenticação, a maneira de garantir que o usuário ou o sistema do dispositivo seja autêntico, e autorizado a utilizar o sistema da maneira correta e íntegra.

Hayashi e Moraes (2021) afirmam que, além desses fundamentos básicos, precisamos acrescentar mais dois serviços de segurança, que são disponibilidade e não repúdio. A disponibilidade consiste em garantir que o sistema estará funcionando 24 horas por dia, 7 dias por semana, sendo possível por meio do uso de servidores *backup* em uma arquitetura *hot stand-by*, ou seja, irá existir uma mesma infraestrutura e aplicação pronta para entrar no ar caso ocorra alguma falha nos sistemas principais. O não repúdio permite ao sistema identificar, de forma efetiva, quem realizou determinada operação e que este não possa negar que a tenha realizado, pois haverá provas de que ele realizou determinada ação.

Ribeiro (2020) afirma que, as características dos dispositivos da IoT, tem na sua concessão, constrangimentos de *hardware*, como limitações de processamento, memória, capacidade de arquivo reduzida, alimentação (bateria), taxas de transferências reduzidas, tamanho, que associado a comunicações nem sempre tem uma elevada confiabilidade, com isso, um dos maiores problemas e desafios da IoT está relacionado a essas limitações dos dispositivos. Essas características mostram o motivo dos dispositivos serem vulneráveis em termos de segurança, tais como: portas de comunicação aberta, sistemas insuficientes de privacidade, proteção e encriptação, falta de atualizações, componentes inseguros, etc.

Ribeiro (2020) diz que um outro problema que irá dificultar o controle da segurança e privacidade nos dispositivos da IoT, está relacionado ao ambiente que muitos deles são utilizados, pois muitos dispositivos são utilizados em ambientes não controlados, o que aumenta o risco deles serem comprometidos. Florian e Rovere (2022), completam dizendo 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 em que eles estão presentes, já que há um risco de comprometimento.

Souza (2019) diz que, quando nos baseamos no problema da segurança da informação na internet, várias técnicas foram criadas ao longo dos últimos anos com o objetivo de melhorar a privacidade dos dados que foram gerados. Uma das técnicas mais conhecidas no estudo é a criptografia, que tem como objetivo distorcer o valor de uma informação para que ela não seja interpretada por pessoas e sistemas que não estão autorizados.

Segundo Hayashi e Moraes (2021), a criptografia é uma ferramenta fundamental para garantir a confidencialidade, pois uma vez que uma informação ou texto tenha passado pelo processo de criptografia (cifrado), ele está seguro e protegido, e que apenas os usuários autorizados, que irão possuir a chave criptográfica, irão conseguir acessar essas informações.

Souza (2019), afirma que com o aumento da diversidade de dispositivos que são capazes de gerar ou coletar dados, é necessário que os algoritmos de criptografia sejam implementados por todos os dispositivos com essas capacidades. Com isso, a privacidade dos dados é algo que precisa estar sempre evoluindo, para garantir que o desenvolvimento de novas tecnologias sejam acompanhadas de boas práticas e culminem em sistemas seguros e com dados privados.

Souza (2019), diz que a IoT é um conceito que se mantém praticamente idêntico desde sua concepção original na computação e que é preciso pensar em segurança da informação para que possamos oferecer segurança aos dispositivos e privacidade aos usuários. Ele ainda destaca que a IoT produz um ambiente com um número muito maior de dispositivos ativos e que eles podem ser afetados em caso de uma má gestão de segurança, sendo algo que deve ser priorizado pois isso pode gerar uma exposição de dados pessoais, o que afeta os direitos humanos.

2.5 Ameaças e Vulnerabilidades na IoT

Os sistemas e dispositivos baseado em IoT, assim como qualquer serviço ou dispositivo que esteja conectado à *Internet*, não são isentos de ameaças e vulnerabilidades. Neste tópico serão apresentadas algumas delas.

Segundo Hayashi e Moraes (2021), a vulnerabilidade é uma fraqueza que um produto ou solução pode ter e que afeta a sua integridade, disponibilidade e confidencialidade. Essa fraqueza pode ser explorada por um *hacker*, com isso podemos considerá-lo como um *software* inseguro e também como *bugs*, quando ele é vulnerável. A ameaça é uma violação da segurança que pode impactar uma organização e seu patrimônio. Essas ameaças podem estar relacionadas a acessos não autorizados, alteração e destruição, ou até mesmo exploração de uma vulnerabilidade.

De acordo com Ribeiro (2020), muitas são as ameaças e vulnerabilidades, algumas delas estão expostas no Quadro 1:

Quadro 1 - Ameaças e Vulnerabilidades

NOME	DESCRIÇÃO
Dispositivo vulnerável ao software	Dispositivos de IoT que no seu software podem ter más opções de design e/ou erros de segurança, um exemplo seria o buffer overflow e tratamentos inadequados de exceções. Isso torna os dispositivos vulneráveis a diversos ataques que podem comprometer a confidencialidade e/ou integridade dos dados.
Ameaça de privacidade	Dispositivos que têm a possibilidade de rastreamento da localização podem representar um alto risco na privacidade pois um atacante pode obter dados confidenciais desses dispositivos e utilizá-los para fins ilícitos, como por exemplo vender a informação obtida na dark web.
	A comunicação da rede IoT pode ser

Eavesdropping	interceptada e decifrada caso o canal em que está havendo a comunicação não esteja protegido suficientemente, como por exemplo, se a chave de cifragem, parâmetros de segurança ou definições de configuração, forem trocados de forma clara ou se forem utilizados algoritmos de criptografia fraca ou inadequada.
Negação de Serviço (*Denial-of-Service*, DoS)	Por haver limitação nos dispositivos, eles ficam vulneráveis a ataques de negação de serviço, que nada mais é que um atacante enviar solicitações de forma contínua, o que causa um esgotamento dos recursos do dispositivo, e eles ainda podem ser utilizados para interromper operações de outras redes ou sistemas por meio desse tipo de ataque.
Ataque ao nível do *Firmware*	Um atacante pode substituir um firmware do dispositivo com o pretexto de que seria uma atualização de rotina, ou uma instalação base do dispositivo.
Cópia ou substituição do dispositivo	Uma fábrica não-confiável pode copiar as características físicas, software e configuração de segurança dos dispositivos.
Data-Leakage	Divulgação de dados confidenciais, de forma intencional ou não, para organizações não autorizadas. Esses dados podem ser capturados a partir de dispositivos individuais durante o trânsito desses dados ou no back-end.
Malware	Os dispositivos podem ser infectados com programas criados para executar ações não autorizadas no sistema, e que irão utilizar vulnerabilidades existentes nos softwares ou nos firmwares.
	gestão deficiente de credenciais,

Credenciais fracas de autenticação dos utilizadores/administradores	como senhas fracas e falta de autenticação multifator para interfaces de utilizadores e administrativas de dispositivos, gateways ou back-ends, sendo essa uma vulnerabilidade muito comum em sistemas de informação, incluindo a IoT.

Fonte: Ribeiro (2020)

3 METODOLOGIA

A característica metodológica deste trabalho é influenciada pela necessidade de adquirir conhecimento para apresentação de seus resultados. Levando em conta que para a realização deste, foram feitas revisões bibliográficas para obter o fundamento necessário para a compreensão da pesquisa, sendo fundamentado em teorias existentes, em estudos presentes na literatura e trabalhos que têm relação com o assunto.

O método escolhido para a produção deste trabalho foi a Revisão Sistemática da Literatura (RSL), sendo essa uma modalidade de pesquisa, que segue protocolos específicos, e que irá buscar entender e dar alguma sensatez a um grande corpus documental, sendo verificado o que funciona e o que não funciona em determinado contexto.

Com isso, a RSL está focada no seu caráter de reprodutibilidade por outros pesquisadores, apresentando bases de dados bibliográficos que foram consultadas, sendo essa de forma explícita. A RSL é uma pesquisa científica que será composta por seus próprios objetivos, problemas de pesquisa, metodologia, resultados e conclusão, não se formando apenas como uma introdução de uma pesquisa mais ampla (GALVÃO; RICARTE, 2019).

A pesquisa será realizada com análise de estudos sobre a IoT, no contexto educacional, segurança e suas vulnerabilidades no contexto da IoT, essa investigação foi realizada por meio de estudos publicados entre março de 2007 até junho de 2022.

Após ter sido identificado a importância do tema da IoT no contexto educacional, o problema de pesquisa foi criado e desenvolvido por meio de questões de pesquisa. O protocolo foi utilizado como guia ao decorrer da RSL para obter evidências que foram elaboradas por meio da questão do trabalho: Quais são os perigos na falta de segurança dos dispositivos na IoT quando aplicada na educação?

A RSL foi realizada utilizando o protocolo proposto por Kitchenham e Charters (2007), sendo composta por três fases que são: planejamento, condução/execução e apresentação de resultados adquiridos.

Na fase do planejamento foi identificado a necessidade da revisão sobre o tema, e definido o protocolo onde é relatado por completo o processo e os métodos

que serão aplicados durante a execução. Nessa fase são definidos os objetivos, termos de busca, bases consultadas e foram definidos de forma explícita, os critérios de inclusão e exclusão.

Na fase de condução/execução foram realizadas pesquisas com o objetivo de obter um grupo inicial de estudos primários, essas pesquisas foram realizadas por meio de *strings* de busca. Por meio dessas pesquisas foram extraídos os dados necessários.

A fase da apresentação de resultados, irá mostrar sobre o resumo dos resultados que foram obtidos por meio dos estudos realizados e que tem como objetivo responder a questão deste trabalho. É possível notar que uma RSL para IoT no contexto educacional é muito importante, visto que há grandes vantagens para isso além de diversos perigos e saber sobre os riscos dessa aplicação pode ajudar universidades e escolas a se protegerem dos perigos que existem ou podem surgir.

3.1 Critérios de inclusão e exclusão

Segundo Kitchenham e Charters (2007) os critérios de inclusão e exclusão devem ser baseados na questão de pesquisa e devem ser testados para garantir que possam ser interpretados de forma confiável e que classifiquem os estudos corretamente. Abaixo estão os critérios de inclusão que guiaram a pesquisa na seleção dos estudos:

- Foram escolhidas publicações que contém os termos Internet das Coisas, Internet das Coisas aplicada na Educação e/ou Segurança da Informação;
- Artigos/materiais que estejam entre 1 de março de 2007 até 30 de junho de 2022;
- Foram escolhidas publicações que contribuem no que tange a segurança na IoT e/ou a IoT na educação;
- Artigos/materiais em português e inglês;

Os critérios de exclusão escolhidos para limitar os resultados de acordo com o objetivo de investigação foram:

- Artigos/materiais que fujam do foco da pesquisa;

- Artigos/materiais que não foram publicados no tempo determinado;
- Artigos/materiais que não contemplam os idiomas inglês ou português;

3.2 Base de dados utilizadas

Como base de dados foram utilizados o Google Acadêmico e o Scielo para uma melhor investigação. Visto que essas bases dispõe de diversos artigos para que possamos chegar a uma resposta para a questão desta pesquisa.

3.3 *String* de busca

Para buscas por produções em português foram utilizadas as seguintes expressões:

- "Internet das Coisas" AND Educação AND Segurança.

Para buscas por produções em inglês foram utilizadas as seguintes expressões:

- “Internet of Things” AND Education AND Security.

3.4 Restrições

Serão considerados apenas resultados publicados no período de 2007 a 2022, com idioma em inglês ou português. Seguindo os critérios de inclusão e exclusão para a busca de estudos.

3.5 Período de busca

O período de busca foi delimitado de 1 de março de 2007 até 30 de junho de 2022.

4 RESULTADOS E DISCUSSÕES

Este capítulo apresenta a principal contribuição deste estudo, que é a apresentação de resultados conforme definido no protocolo da RSL discutido na metodologia.

Para a execução desta RSL foram determinadas as palavras-chave: Internet das Coisas; Segurança da informação; Revisão Sistemática da Literatura; Educação. Posteriormente foram aplicados os critérios de inclusão e exclusão. O próximo passo foi a seleção da base de dados para a pesquisa, onde foram selecionadas as bases Google Acadêmico e Scielo, elas contam com números relevantes sobre diversos estudos e com opções para filtrar pesquisas. Consultando a base do Google Acadêmico, aplicando as expressões Internet das Coisas e Educação foram identificados um total de 106.000 resultados. Após aplicar o filtro utilizando as *strings* de busca: Internet das Coisas, Educação e Segurança a resposta é de 77.600 resultados. Já com a utilização das *strings* para buscas em inglês, que são: *Internet of Things*, *Education* e *Security*, a resposta foi de 251.000 resultados.

No Quadro 2, estão expostos os 7 artigos que foram identificados e selecionados por meio das *strings* de busca, publicados no período de 2007 até 2022, organizados em uma sequência numérica, por títulos dos seus respectivos artigos, endereços de onde foram encontrados, seus devidos autores, e suas palavras-chave.

Quadro 2 - Artigos selecionados para a RSL

ID	Título	Endereço	Autor	Palavras-chave
1	**Internet das Coisas: Uma Possibilidade de Aplicação das Tecnologias Móveis na Educação**	**https://seer.faccat.br/index.php/redin/article/view/433**	**Ferrasi *et al*. (2016)**	**Tecnologias Móveis; Internet das Coisas(IoT); Educação; Tecnologias da Informação e Comunicação(TIC).**
2	**Internet das Coisas e Seus Impactos Positivos no Ambiente Educacional**	**https://www.al-enterprise.com/-/media/assets/internet/documents/iot-for-education-solutionbrief-ptbr.pdf**	**Sousa, Lacerda e Faria (2019)**	**Tecnologia; Política de Segurança da Informação; Proteção.**

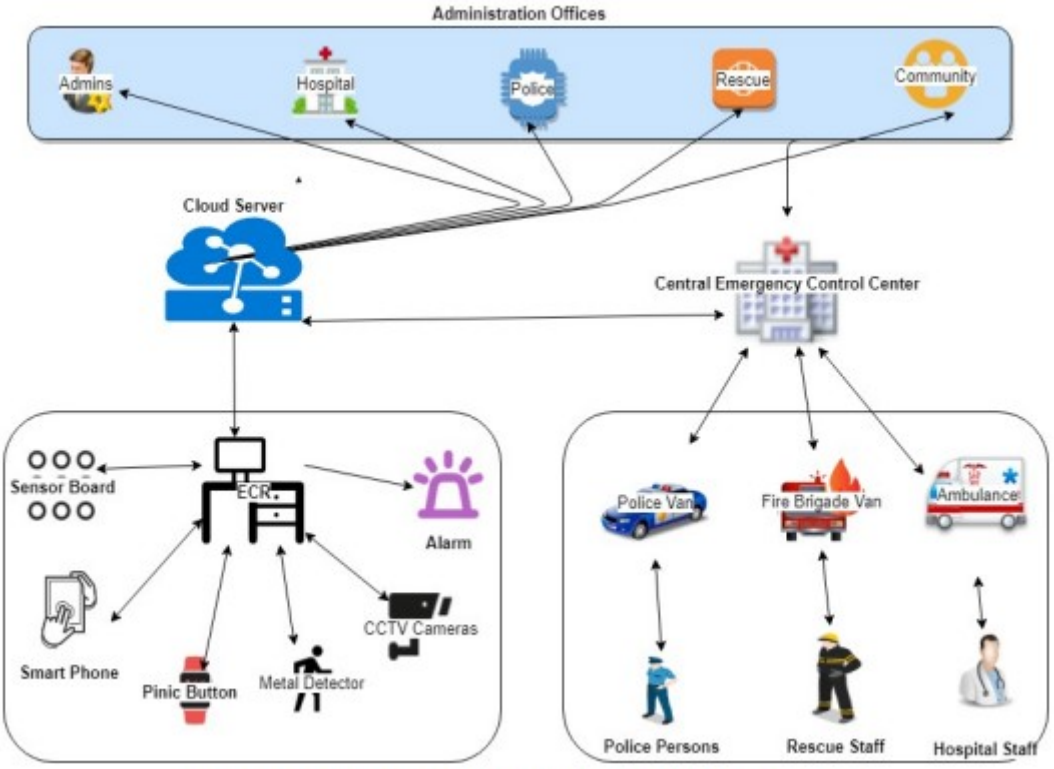
3	**Smart Security Framework for Educational Institutions Using Internet of Things (IoT)**	**https://www.researchgate.net/publication/336069739_Smart_Security_Framework_for_Educational_Institutions_Using_Internet_of_Things_IoT**	**Badshah *et al*. (2019)**	**Internet of things, smart security framework, massacres, terrorism, smart emergency alert.**
4	**Aplicando Internet das Coisas na Educação: Tecnologia, Cenários e Projeções**	**http://ojs.sector3.com.br/index.php/wcbie/article/view/7514**	**Silva *et al*. (2017)**	
5	**“Internet das Coisas” – Um Estudo sobre Questões de Segurança, Privacidade e Infraestrutura**	**https://app.uff.br/riuff/handle/1/5150**	**Figueira (2016)**	**Internet das Coisas, Criptografia e Privacidade.**
6	**Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks**	**https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4**	**Abomhara e Koien (2015)**	**Internet of Things, Cyber-attack, Security threats.**
7	**General Survey on Security Issues on Internet of Things. International Journal of Computer Applications**	**https://www.ijcaonline.org/research/volume139/number2/das-2016-ijca-909113.pdf**	**Das e Sharma (2016)**	**Internet of Things, Machine-to-machine Communication, Vehicle-to-vehicle Communication, Security Issues, Secure Reprogrammable Networks.**

Fonte: Autoria própria (2022)

Ferrasi *et al*. (2016) diz que, a fase atual de evolução da Internet tem um grande potencial e pode promover uma nova revolução na educação, principalmente nas práticas pedagógicas no ensino em todos os seus níveis. Sousa, Lacerda e Faria (2019) sugerem que a tecnologia faça parte do ambiente educacional em uma escala maior, para auxílio de trabalhos dos professores e gestores, assim como para estudos, pesquisas e inclusão de novas formas de aprendizado dos alunos.

Observando bem esses pontos foi possível encontrar um exemplo onde é possível ver o grande potencial que a fase atual de evolução da internet tem, assim como a tecnologia fazendo parte do ambiente educacional em uma escala maior. Esse exemplo é uma proposta feita por Badshah *et al*. (2019) para melhorar a segurança das escolas e universidades, como por exemplo, evitando ou minimizando massacres, como ilustra a Figura 1.

Figura 1 - Estrutura de Segurança Inteligente



Fonte: Badshah *et al*. (2019)

Essa proposta é uma Estrutura de Segurança Inteligente (do inglês *Smart Security Framework* - SSF) para instituições educacionais que notificam instantaneamente os departamentos responsáveis por meio da coleta e análise de dados de todos os sensores e dispositivos de segurança para tomar decisões inteligentes durante uma emergência ou em situações anormais. Isso faria com que o ambiente educacional se tornasse mais seguro.

Além disso, a IoT quando aplicada na educação pode apresentar outros diversos benefícios entre eles estão: a inclusão de pessoas que não teriam fácil acesso à educação, uma personalização do método de ensino tornando-o mais

atrativo e facilitando a aprendizagem. Também automatização de atividades do dia a dia facilitando processos como a frequência dos alunos; informativos sobre atividades, eventos, notas e desempenho nas disciplinas; solicitações diversas entre alunos, professores e direção acadêmica (FERRASI, *et al*. 2016).

Silva *et al*. (2017) dizem que para que a IoT seja considerada uma rede essencial para o ensino é necessário que três pontos estejam bem definidos, são eles: Segurança, que é um ponto fundamental para o sucesso de uma rede IoT já que quanto mais objetos estiverem conectados à uma rede pervasiva de ampla abrangência geográfica, maior deverá ser o esquema de segurança implementado. Dispositivos Embarcados, realizando a comunicação e captura de dados do ambiente, criando novas interações entre usuários e máquinas. E por fim, Políticas, que devem ser instaladas para estimular o uso da tecnologia em sala de aula e sua integração ao currículo acadêmico de uma instituição.

Porém, na IoT existem problemas de segurança que precisam de bastante atenção, principalmente quando pensamos em aplicar ela em lugares que envolvem muitas pessoas como escolas e universidades.

Figueira (2016) diz que a IoT está longe de ser segura o suficiente contra problemas de segurança e ataques da internet atual, isso se deve a particularidades desta tecnologia, tais como:

- **Comunicações em IoT podem ser realizadas por meio de redes sem fio:** qualquer indivíduo com más intenções podem ouvir essas transmissões e se comunicar utilizando esse mesmo meio;
- **É possível acessar os dispositivos fisicamente:** os dispositivos IoT podem ser colocados em locais públicos onde estão ao alcance de qualquer indivíduo;
- **Muitos dispositivos contam com recursos limitados:** a limitação de recursos insere medidas de segurança bem restritas nesses dispositivos.

Diversos são os perigos que podemos encontrar na IoT sendo eles ameaças, vulnerabilidades e ataques. Abomhara e Koien (2015), mostram os tipos mais comuns de ataque cibernético, estando eles expostos no Quadro 3.

Quadro 3 - Tipos mais comuns de ataque cibernético

NOME	DESCRIÇÃO
Ataques físicos	Este tipo de ataque altera componentes de hardware. Devido à natureza autônoma da IoT, a maioria dos dispositivos normalmente opera em ambientes externos, que são altamente suscetíveis a ataques físicos.
Ataques de reconhecimento	Descoberta e mapeamento não autorizado de sistemas, serviços ou vulnerabilidades.
Ataques de acesso	Pessoas não autorizadas obtêm acesso a redes ou dispositivos aos quais não têm direito de acesso. Existem dois tipos diferentes de ataques de acesso: o primeiro é o acesso físico e o segundo é o remoto, que é feito para dispositivos conectados por IP.
Ataques à privacidade	A proteção da privacidade em IoT tornou-se cada vez mais desafiadora devido aos grandes volumes de informação facilmente disponíveis por meio de mecanismos de acesso remoto.
Crimes cibernéticos	A internet e os objetos inteligentes são usados para explorar usuários e dados para ganho material, como roubo de propriedade intelectual, roubo de identidade, roubo de marca e fraude.
Ataques Destrutivos	O espaço é usado para criar perturbações em larga escala e destruição de vidas e propriedades. Exemplos de ataques destrutivos são o terrorismo e ataques de vingança.
Negação de Serviço (DoS)	Este tipo de ataque é uma tentativa de tornar uma máquina ou recurso de rede indisponível para seus usuários pretendidos. Devido aos recursos de pouca memória e recursos computacionais limitados, a maioria dos dispositivos em IoT é vulnerável a ataques de enervação de recursos.

Fonte: Abomhara e Koien (2015)

Além disso, Abomhara e Koien (2015), mostram que os ataques mais comuns à privacidade do usuário são: mineração de dados, espionagem, rastreamento e ataques baseados em senha.

Com isso, podemos perceber que são muitos os desafios de segurança que existem na IoT. Das e Sharma (2016) afirmam que dispositivos mal projetados podem expor os dados do usuário ao roubo, deixando o fluxo de dados e objetos sem vigilância. O custo competitivo e restrições técnicas em dispositivos IoT desafiam os fabricantes a projetar de forma razoável as características de segurança nesses dispositivos, criando potencialmente medidas de segurança e mantendo vulnerabilidades de manutenção maiores do que os computadores tradicionais.

Das e Sharma (2016) listam alguns desafios de segurança para IoT, dentre eles estão: as ferramentas, métodos e estratégias existentes associados à segurança da IoT que precisam de uma nova consideração com o sistema e as estratégias convencionais; a implantação da IoT homogênea que pode comprometer a sua simplicidade, assim esperando uma estratégia de implementação heterogênea que possa funcionar corretamente; podem surgir problemas em *backgrounds* como reconfiguração e evolução dos dispositivos; e um outro desafio é o suporte e gerenciamento à longo prazo desses dispositivos.

Além desses desafios, precisa-se obedecer aos princípios fundamentais de segurança da informação para um ambiente mais seguro. Abomhara e Koien (2015) dizem que, para ter sucesso com a implementação da segurança de IoT eficiente, devemos estar cientes dos principais objetivos de Segurança da Informação, esses objetivos estão expostos no Quadro 4:

Quadro 4 - Principais objetivos de Segurança da Informação

NOME	DESCRIÇÃO
Confidencialidade	Um importante recurso de segurança em IoT, mas pode não ser obrigatório em alguns cenários em que os dados são apresentados publicamente. No entanto, na maioria das situações e cenários, os dados confidenciais não devem ser divulgados ou lidos por entidades não autorizadas.

Integridade	uma propriedade de segurança obrigatória na maioria dos casos. Diferentes sistemas em IoT têm vários requisitos de integridade.
Autenticação e Autorização	A conectividade ubíqua da IoT agrava o problema de autenticação devido à natureza dos ambientes de IoT, onde a comunicação possível ocorreria entre dispositivo para dispositivo, humano para dispositivo e/ou humano para humano. Diferentes requisitos de autenticação exigem soluções diferentes em sistemas diferentes.
Disponibilidade	Um usuário de um dispositivo (ou o próprio dispositivo) deve ser capaz de acessar os serviços a qualquer momento, sempre que necessário.
Não repúdio	Produz certas evidências nos casos em que o usuário ou dispositivo não pode negar uma ação. O não repúdio não é considerado uma propriedade de segurança importante para a maior parte da IoT. Pode ser aplicável em determinados contextos, por exemplo, sistemas de pagamento em que usuários ou provedores não podem negar uma ação de pagamento.
Responsabilidade	Ao desenvolver técnicas de segurança para serem usadas em uma rede segura, a responsabilidade adiciona redundância e responsabilidade de certas ações, deveres e planejamento da implementação de políticas de segurança de rede.
Auditoria	É uma avaliação sistemática da segurança de um dispositivo ou serviço, medindo o quão bem ele está em conformidade com um conjunto de critérios estabelecidos. Devido a muitos bugs e vulnerabilidades na maioria dos sistemas, a auditoria de segurança desempenha um papel importante na determinação de quaisquer pontos fracos exploráveis que colocam os dados em risco. Na IoT, a necessidade

	de auditoria dos sistemas depende da aplicação e de seu valor.

Fonte: Abomhara e Koien (2015)

Com base nos conteúdos estudados por meio de publicações selecionadas, podemos concluir que a IoT ainda precisa de muitos ajustes, principalmente de segurança para que possa ser aplicada em diversas áreas sem muita preocupação, ficando longe dos mais diversos tipos de ataques cibernéticos que são bastante perigosos. Há muitos perigos na IoT justamente porque os seus dispositivos não apresentam uma excelente aplicação da segurança, e isso se deve ao fato de que desde a produção, os dispositivos são projetados de forma razoável em questões de segurança para que possam ter um custo competitivo.

Com isso, os perigos em aplicar a IoT na educação se assemelham bastante com os perigos da aplicação dela em qualquer área já que, um dos maiores desafios é deixar os dispositivos seguros, sendo eles muitas vezes a porta de entrada para invasões. Porém, podemos alertar que dependendo da intenção do invasor pode haver consequências gravíssimas, como por exemplo, um *hacker* obter informações do trajeto de um aluno, como horário, rota, se está sozinho ou não, para realizar um sequestro com o objetivo de conseguir dinheiro. Assim como, invasões de privacidade que roubam dados sensíveis de muitas pessoas, que estão na instituição/escola com o intuito apenas de ensinar ou aprender.

É importante destacar que, quanto mais um dispositivo estiver seguro, menos ele estará sujeito a ataques e ao atingir os objetivos básicos da segurança da informação, os dispositivos IoT estarão mais próximos deste tipo de segurança, mais distantes de ataques. Além disso, se faz necessário desenvolver novas formas de segurança, pois sempre há uma nova forma de ataque de cibercriminosos e é muito importante estar atento a isso para que seja mantido um ambiente seguro.

5 CONSIDERAÇÕES FINAIS

Esse estudo buscou produzir uma RSL para alertar sobre os perigos na falta de segurança dos dispositivos IoT quando aplicada na educação e destacar a importância de desenvolver dispositivos IoT cada vez mais seguros para que as instituições e usuários possam usufruir de tal tecnologia sem tanta preocupação. Foram utilizadas o Google Acadêmico e o Scielo como fontes de material, onde os estudos pesquisados foram publicados no período de 2007 até 2022 com o objetivo de buscar uma melhor compreensão sobre o tema.

A partir da análise dos artigos recuperados, observou-se que a falta de segurança nos dispositivos da IoT, gerada pela vulnerabilidade que por vezes se dá pela má projeção dos dispositivos, podem tornar o ambiente perigoso, suscetível a ataques. Também foi possível observar que existem diversos desafios para que a IoT se torne, de fato, segura.

Esta pesquisa também mostrou que a IoT aplicada no contexto educacional pode trazer benefícios e malefícios, mas que trabalhando da melhor forma possível, pode apresentar mais benefícios, principalmente se focar na segurança, pois a segurança é um dos pontos fundamentais em qualquer área e na IoT não é diferente.

Diante da metodologia proposta, percebe-se que o trabalho poderia ter sido realizado com uma pesquisa mais ampla na bibliografia para analisar de uma forma aprofundada, que contribuísse com o desenvolvimento de novos métodos de segurança no contexto educacional, ajudando a se prevenir desses perigos existentes e de possíveis novos perigos, porém, não foi possível devido a limitação de tempo.

O estudo realizado e apresentado, tem como finalidade contribuir para a literatura e poderá servir como base para futuras pesquisas que busquem conhecer mais sobre a IoT no contexto educacional, e saber como a falta de segurança dos dispositivos IoT afeta, caso não seja feito de forma adequada aos padrões de segurança da informação.

Além disso, como parte complementar deste trabalho, recomenda-se a continuidade dele por meio do reaproveitamento deste estudo, buscando maneiras de desenvolver novas formas para deixar a IoT no contexto educacional mais seguro

e/ou investigar mais formas de como invasores podem agir, para assim desenvolver novos modos de proteção e prevenção.

REFERÊNCIAS

ABOMHARA, M.; KOIEN, G. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security, Vol. 4, p. 65-88, jan. 2015. Disponível em: https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4 . Acesso em: 01 out. 2022.

AGOSTINELLI, J. **A importância da lei geral de proteção de dados pessoais no ambiente online, 2018.** ETIC-ENCONTRO DE INICIAÇÃO CIENTÍFICA-ISSN 21-76-8498,14(14). Disponível em: http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7025. Acesso em: 29 jun. 2022.

ARAÚJO, M.; GALHARDO, C.; SANTOS, V. A Internet das Coisas e suas implicações na Educação. Id on Line Rev.Mult. Psic., 2019, vol.13, n.46, p. 231-242. ISSN: 1981-1179. Disponível em: https://idonline.emnuvens.com.br/id/article/view/1865 Acesso em: 04 jul. 2022.

ASHTON, K. That “Internet of Things” Thing. **RFID Journal**, 22 jun. 2009. Disponível em: http://www.rfidjournal.com/articles/view?4986. Acesso em: 29 jun. 2022.

BADSHAH, A. *et al*. Smart Security Framework for Educational Institutions Using Internet of Things (IoT), 2019. Disponível em: https://www.researchgate.net/publication/336069739_Smart_Security_Framework_for_Educational_Institutions_Using_Internet_of_Things_IoT Acesso em: 03 out. 2022.

CARRION, P.; QUARESMA, M. Internet das Coisas (IoT): Definições e aplicabilidade aos usuários finais. Human Factors in Design, Florianópolis, v. 8, n. 15, p. 049-066, 2019. DOI: 10.5965/2316796308152019049. Disponível em: https://www.revistas.udesc.br/index.php/hfd/article/view/2316796308152019049. Acesso em: 29 jun. 2022.

CHICARINO, V. *et al*. Uso de Blockchain para Privacidade e Segurança em Internet das Coisas. Minicursos do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSeg2017, Capítulo: 4 p. 149-199. Editora: Sociedade Brasileira de Computação - SBC, 2017. Disponível em: https://www.researchgate.net/publication/321966650_Uso_de_Blockchain_para_Privacidade_e_Seguranca_em_Internet_das_Coisas. Acesso em: 6 jul. 2022.

CISCO IBGS. A Internet das Coisas como a próxima evolução da Internet está mudando tudo, 2011. Disponível em: https://www.cisco.com/c/dam/global/pt_br/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf Acesso em: 30 jun. 2022.

CLARO, M. Como a Internet das Coisas pode entrar na escola, 2016. Disponível em: https://www.moodlelivre.com.br/noticias/1481-como-a-internet-das-coisas-pode-entrar-na-escola. Acesso em: 01 jul 2022.

CORNEL, C. The Role of Internet of Things for a Continuous Improvement in Education Hyperion Economic Journal, Faculty of Economic Sciences, Hyperion University of Bucharest, Romania, vol. 3(2), pages 24-31, 2015. Acesso em: 16 jul. 2022.

DAS, D.; SHARMA, B. General Survey on Security Issues on Internet of Things. International Journal of Computer Applications, v. 139, n. 2, 2016. Disponível em: https://www.ijcaonline.org/research/volume139/number2/das-2016-ijca-909113.pdf . Acesso em: 01 out. 2022.

DERMEVAL, D; COELHO, Jorge AP de M.; BITTENCOURT, Ig Ibert. Mapeamento sistemático e revisão sistemática da literatura em informática na educação. Disponível em: https://metodologia.ceie-br.org/wp-content/uploads/2019/11/livro2_cap3.pdf. Acesso em: 16 set. 2022.

DONATO, H; DONATO, M. Etapas na Condução de uma Revisão Sistemática. Acta Médica Portuguesa, v. 32, n. 3, 2019. Disponível em: https://core.ac.uk/download/pdf/195808557.pdf . Acesso em: 09 jul 2022.

FARAHANI, S. ZigBee wireless networks and transceivers. San Diego: Elsevier, 2011. Disponível em: https://www.waveshare.com/w/upload/9/91/ZigBee-Wireless-Networks-and-Transceivers.pdf . Acesso em: 05 out. 2022.

FERRASI, F. A. *et al*. **INTERNET DAS COISAS: UMA POSSIBILIDADE DE APLICAÇÃO DAS TECNOLOGIAS MÓVEIS NA EDUCAÇÃO.** Redin-Revista Educacional Interdisciplinar, v. 5, n. 1, 2016. Disponível em: https://seer.faccat.br/index.php/redin/article/view/433 Acesso em: 4 jul. 2022.

FIGUEIRA, V. "Internet das Coisas" – Um Estudo sobre Questões de Segurança, Privacidade e Infraestrutura. Trabalho de conclusão de curso (Curso de Tecnologia em Sistemas de Computação) - Universidade Federal Fluminense, Niterói, 2016. Disponível em: https://app.uff.br/riuff/handle/1/5150 . Acesso em: 01 out. 2022.

FLORIAN, F.; ROVERE, L. ESTUDO SOBRE SEGURANÇA E PRIVACIDADE NA INTERNET DAS COISAS (IOT). RECIMA21 - Revista Científica Multidisciplinar - ISSN 2675-6218, [S. l.], v. 3, n. 6, p. e361601, 2022. DOI: 10.47820/recima21.v3i6.1601. Disponível em: https://recima21.com.br/index.php/recima21/article/view/1601. Acesso em: 6 jul. 2022.

GALEGALE, G. P., *et al*. Internet das Coisas aplicada a negócios – Um estudo bibliométrico. Journal of Information Systems and Technology Management, 2016.

GALVÃO, M. C. B.; RICARTE, I. L. M. **REVISÃO SISTEMÁTICA DA LITERATURA: CONCEITUAÇÃO, PRODUÇÃO E PUBLICAÇÃO**. Logeion: Filosofia da Informação, [S. l.], v. 6, n. 1, p. 57–73, 2019. Disponível em: https://revista.ibict.br/fiinf/article/view/4835. Acesso em: 09 jun 2022.

GASQUE, K; CASARIN, H. Bibliotecas Escolares: tendências globais. Em Questão. Porto Alegre, v. 22, n.3, 2016. Acesso em: 29 jun. 2022.

GUBBI, J. *et al*. Internet of Things (IoT): a vision, architectural elements, and future directions. Future Generation Computer Systems, v. 29, n. 7, p. 1645–1660, set. 2013. Disponível em: http://www.sciencedirect.com/science/article/pii/S0167739X13000241. Acesso em: 30 jun. 2022.

GUL, S. *et al*. A Survey on Role of Internet of Things in Education. JCSNS International Journal of Computer Science and Network Security, VOL.17 No.5, mai 2017. Acesso em: 29 jun. 2022.

HAYASHI, V; MORAES, A. **Segurança em IoT: Entendendo os riscos e ameaças em IoT.** 1°. ed. [S. l.]: ALTA BOOKS, 2021. 194 p.

KITCHENHAM, B.; CHARTERS, S.: Guidelines for performing systematic literature reviews in software engineering. Technical Report EBSE 2007-001, Keele University and Durham University Joint Report, 2007. Acesso em: 11 jul. 2022.

LACERDA, F. **Arquitetura da Informação Pervasiva: projetos de ecossistemas de informação na Internet das Coisas.** Brasília: Universidade de Brasília, 2015. 226 fls. Tese de Doutorado. Disponível em: http://repositorio.unb.br/bitstream/10482/19646/1/2015_FlaviaLacerda.pdf. Acesso em: 30 jun. 2022.

MAGRANI, E. **A internet das coisas.** 1°. ed. Rio de Janeiro, Rio de Janeiro.: FGV EDITORA, 2018. E-book. Acesso em: 30 jun. 2022.

PRUET, P. *et al* (2015). Exploring the Internet of “Educational Things”(IoET) in rural underprivileged areas. In Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2015 12th International Conference on (pp. 1-5). IEEE. Acesso em: 05 jul. 2022.

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. Disponível em: http://hdl.handle.net/10400.8/5568 . Acesso em: 07 jul. 2022.

SAIBA como a internet das coisas pode ser aplicada na educação. Redação Lyceum, 7 nov. 2018. Disponível em: https://blog.lyceum.com.br/internet-das-coisas-na-educacao/#O_que_e_a_Internet_das_Coisas . Acesso em: 30 jun. 2022.

SAMPAIO, F.; MANCINI M. C. Estudos de revisão sistemática: um guia para síntese criteriosa da evidência científica. Revista Brasileira de fisioterapia. São Carlos, v. 11, n. 1, p. 83-89, jan./fev. 2007. Disponível em: http://www.scielo.br/pdf/rbfis/v11n1/12.pdf Acesso em: 09 jul. 2022.

SANTOS, B. *et al*. 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: 07 jul. 2022.

SCHÜTZ, R.; SANTANA, S.; SANTOS, G. Política de periódicos nacionais em Educação Física para estudos de revisão sistemática. Revista Brasileira de Cineantropometria do Desempenho Humano, Santa Catarina, v. 13, n. 4, p. 313-319, 2011. Disponível em: http://www.scielo.br/pdf/rbcdh/v13n4/11.pdf . Acesso em: 09 jul. 2022.

SILVA, A.; BRAGA, R.; CALADO, I. Conectando as "coisas" na Educação. Computação Brasil. 2017. Acesso em: 05 jul. 2022.

SILVA, R. *et al*. Aplicando Internet das Coisas na Educação: Tecnologia, Cenários e Projeções, 2017. Disponível em: http://ojs.sector3.com.br/index.php/wcbie/article/view/7514. Acesso em: 03 out. 2022.

SOUSA, M; LACERDA, M; FARIA, A. INTERNET DAS COISAS E SEUS IMPACTOS POSITIVOS NO AMBIENTE EDUCACIONAL. v. 6, ed. 1, p. 31-39, 2019. Disponível em: https://www.al-enterprise.com/-/media/assets/internet/documents/iot-for-education-solutionbrief-ptbr.pdf . Acesso em: 30 set. 2022.

SOUZA, J. SEGURANÇA E PRIVACIDADE NA INTERNET DAS COISAS: ESTUDO DE CASOS COM A KAA IOT PLATFORM. Orientador: Prof. Dr. Marco Aurélio Spohn. 2019. 52 p. Trabalho de conclusão de curso (Bacharel em Ciência da Computação) - Universidade Federal da Fronteira Sul, Chapecó, 2019. Disponível em: https://rd.uffs.edu.br/handle/prefix/3369. Acesso em: 07 jul. 2022.

TAROUCO, L. *et al*. Internet das Coisas na Educação: trajetória para um campus inteligente. In VI Congresso Brasileiro de Informática na Educação, 2017. Disponível em: http://ojs.sector3.com.br/index.php/wcbie/article/view/7511. Acesso em: 05 jul. 2022.

ZUIN, A.; ZUIN, V. A formação no tempo e no espaço da Internet das Coisas. Revista Educação & Sociedade. Campinas, V. 37, N. 136, 2016. Acesso em: 04 jul. 2022.