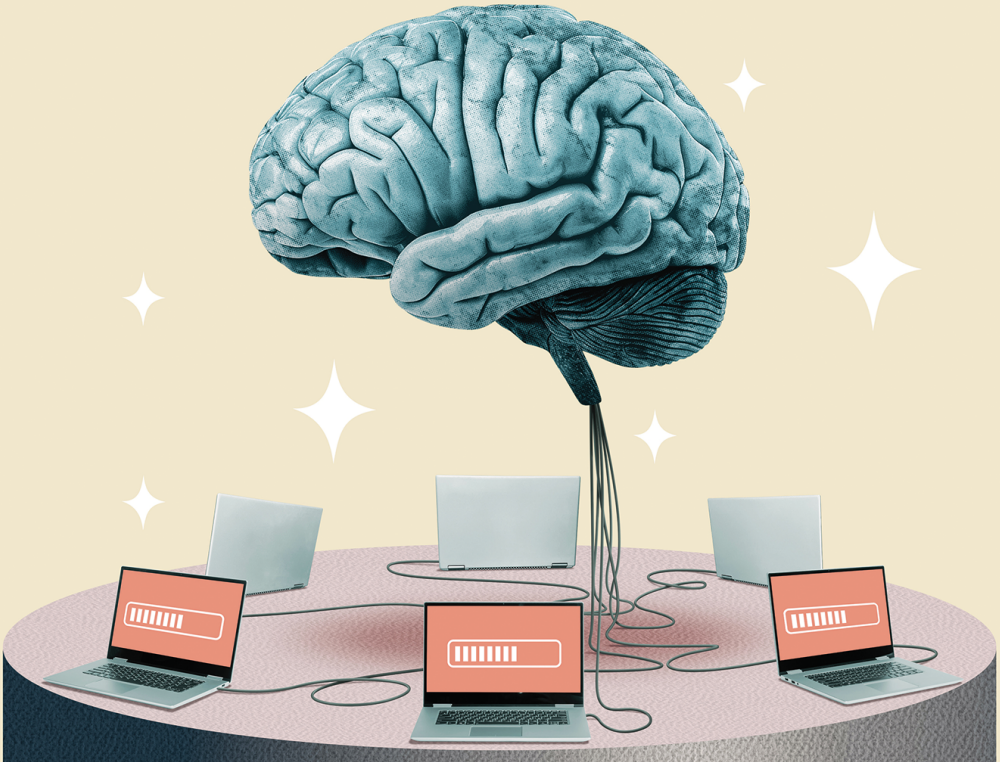
FABRÍCIO MORAES DE ALMEIDA
(ORGANIZADOR)

CIÊNCIA E TECNOLOGIA

CATALISADORES DA INOVAÇÃO 3

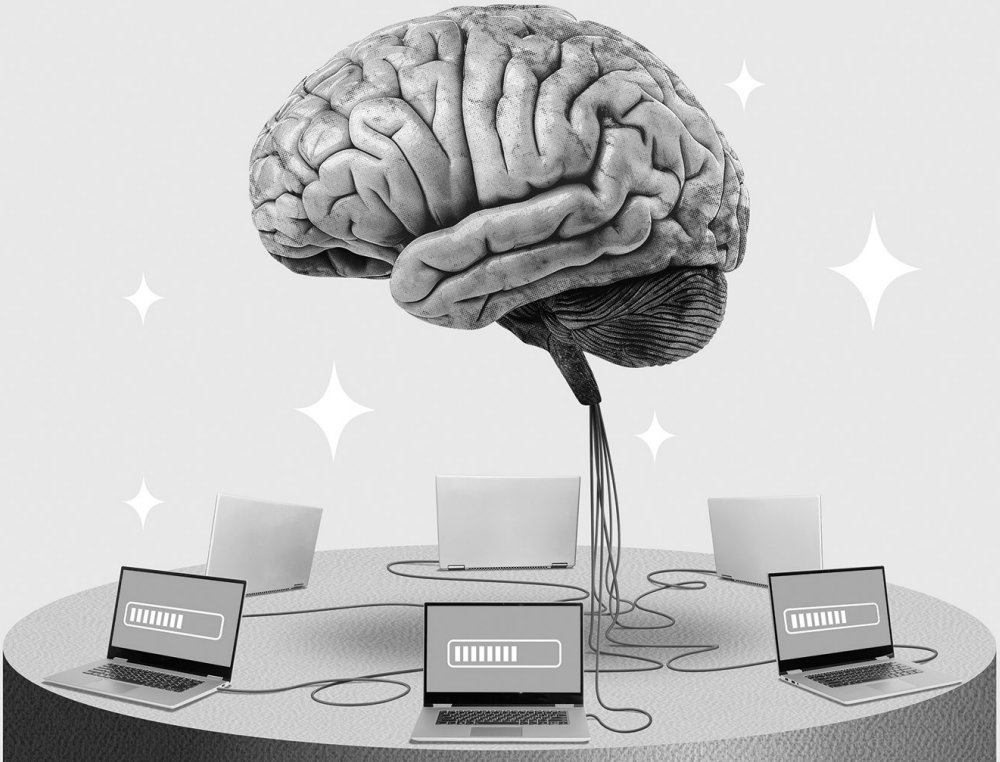


Atena Editora
Ano 2024

FABRÍCIO MORAES DE ALMEIDA
(ORGANIZADOR)

CIÊNCIA E TECNOLOGIA

CATALISADORES DA INOVAÇÃO 3



Atena Editora
Ano 2024

CIÊNCIAS EXATAS E DA TERRA E ENGENHARIAS

Editora chefe
Profª Drª Antonella Carvalho de Oliveira
Editora executiva
Natalia Oliveira
Assistente editorial
Flávia Barão
Bibliotecária
Janaina Ramos
Projeto gráfico
Ellen Andressa Kubisty
Luiza Alves Batista
Nataly Evilin Gayde
Thamires Camili Gayde
Imagens da capa
iStock
Edição de arte
Luiza Alves Batista

CIÊNCIAS EXATAS E DA TERRA E ENGENHARIAS

Ciência e tecnologia: catalisadores da inovação 3

Diagramação: Camila Alves de Cremo
Correção: Maiara Ferreira
Indexação: Amanda Kelly da Costa Veiga
Revisão: Os autores
Organizador: Fabrício Moraes de Almeida

Dados Internacionais de Catalogação na Publicação (CIP)

C569 Ciência e tecnologia: catalisadores da inovação 3 / Organizador Fabrício Moraes de Almeida. – Ponta Grossa - PR: Atena, 2024.

Formato: PDF
Requisitos de sistema: Adobe Acrobat Reader
Modo de acesso: World Wide Web
Inclui bibliografia
ISBN 978-65-258-3179-4
DOI: https://doi.org/10.22533/at.ed.794242712

1. Ciência. 2. Tecnologia. I. Almeida, Fabrício Moraes de (Organizador). II. Título.

CDD 601

Elaborado por Bibliotecária Janaina Ramos – CRB-8/9166

Atena Editora
Ponta Grossa – Paraná – Brasil
Telefone: +55 (42) 3323-5493
www.atenaeditora.com.br
contato@atenaeditora.com.br

DECLARAÇÃO DO AUTOR

Para fins desta declaração, o termo 'autor' será utilizado de forma neutra, sem distinção de gênero ou número, salvo indicação em contrário. Da mesma forma, o termo 'obra' refere-se a qualquer versão ou formato da criação literária, incluindo, mas não se limitando a artigos, e-books, conteúdos on-line, acesso aberto, impressos e/ou comercializados, independentemente do número de títulos ou volumes. O autor desta obra: 1. Atesta não possuir qualquer interesse comercial que constitua um conflito de interesses em relação à obra publicada; 2. Declara que participou ativamente da elaboração da obra, preferencialmente na: a) Concepção do estudo, e/ou aquisição de dados, e/ou análise e interpretação de dados; b) Elaboração do artigo ou revisão com vistas a tornar o material intelectualmente relevante; c) Aprovação final da obra para submissão; 3. Certifica que a obra publicada está completamente isenta de dados e/ou resultados fraudulentos; 4. Confirma a citação e a referência correta de todos os dados e de interpretações de dados de outras pesquisas; 5. Reconhece ter informado todas as fontes de financiamento recebidas para a consecução da pesquisa; 6. Autoriza a edição da obra, que incluem os registros de ficha catalográfica, ISBN, DOI e demais indexadores, projeto visual e criação de capa, diagramação de miolo, assim como lançamento e divulgação da mesma conforme critérios da Atena Editora.

DECLARAÇÃO DA EDITORA

A Atena Editora declara, para os devidos fins de direito, que: 1. A presente publicação constitui apenas transferência temporária dos direitos autorais, direito sobre a publicação, inclusive não constitui responsabilidade solidária na criação da obra publicada, nos termos previstos na Lei sobre direitos autorais (Lei 9610/98), no art. 184 do Código Penal e no art. 927 do Código Civil; 2. Autoriza e incentiva os autores a assinarem contratos com repositórios institucionais, com fins exclusivos de divulgação da obra, desde que com o devido reconhecimento de autoria e edição e sem qualquer finalidade comercial; 3. A editora pode disponibilizar a obra em seu site ou aplicativo, e o autor também pode fazê-lo por seus próprios meios. Este direito se aplica apenas nos casos em que a obra não estiver sendo comercializada por meio de livrarias, distribuidores ou plataformas parceiras. Quando a obra for comercializada, o repasse dos direitos autorais ao autor será de 30% do valor da capa de cada exemplar vendido; 4. Todos os membros do conselho editorial são doutores e vinculados a instituições de ensino superior públicas, conforme recomendação da CAPES para obtenção do Qualis livro; 5. Em conformidade com a Lei Geral de Proteção de Dados (LGPD), a editora não cede, comercializa ou autoriza a utilização dos nomes e e-mails dos autores, bem como quaisquer outros dados dos mesmos, para qualquer finalidade que não o escopo da divulgação desta obra.

Scientia é o cerne da palavra ciência, produto do conhecimento acumulado e a tecnologia é o resultado da evolução e do desenvolvimento científico.

Em linhas gerais, ciência e tecnologia estão implicitamente ligados, implicando uma relação simbiótica que impulsiona a inovação.

Usualmente, no livro, são demonstrados diversos tipos de abordagens teórico-práticos nos resultados obtidos pelos vários autores na construção de cada capítulo. Habitualmente, a Atena Editora propõe a divulgação técnico-científica com excelência, essencial para assegurar o destaque entre as melhores editoras.

Fabrício Moraes de Almeida

SUMÁRIO

SUMÁRIO

JOGOS NARRATIVOS E GAMIFICAÇÃO APLICADOS AO TREINAMENTO PARA O DIAGNÓSTICO PRECOCE DO CÂNCER INFANTOJUVENIL

Data de submissão: 29/10/2024 *Data de aceite: 02/12/2024*

Felipe de Assis Ribeiro
Programa de Pós-Graduação em Tecnologia da Informação e Gestão em Saúde, Universidade Federal de Ciências da Saúde de Porto Alegre, Porto Alegre, RS, Brasil

Isabel Cristina Siqueira da Silva
Programa de Pós-Graduação em Tecnologia da Informação e Gestão em Saúde, Universidade Federal de Ciências da Saúde de Porto Alegre, Porto Alegre, RS, Brasil

RESUMO: O câncer infantojuvenil, diferentemente do câncer nos adultos, não tem fatores de risco ligados ao estilo de vida ou condições ambientais e pode apresentar sintomas similares aos de doenças comuns entre as crianças, dificultando o diagnóstico da doença. Umas das principais formas de combate aos tumores infantis é o diagnóstico precoce, acompanhado de orientação terapêutica, a fim de proporcionar, ao indivíduo, maiores chances de cura e melhor qualidade de vida após o tratamento. Considerando tais questões, este trabalho teve por objetivo o desenvolvimento de uma plataforma informacional para apoio ao treinamento de profissionais da saúde e da educação sobre o diagnóstico precoce do câncer infantojuvenil. Este estudo iniciou com uma revisão da literatura e de trabalhos relacionados, buscando embasar cientificamente o presente estudo, além da realização de pesquisa exploratória junto aos profissionais do Instituto do Câncer Infantil (ICI) de Porto Alegre visando conhecer o seu dia a dia de trabalho e suas iniciativas voltadas à conscientização sobre a importância do diagnóstico precoce do câncer infantojuvenil. Estes profissionais auxiliaram no projeto e no desenvolvimento da plataforma proposta bem como na avaliação do conteúdo informacional a ser disponibilizado nesta. A plataforma desenvolvida apresenta o conteúdo informacional de duas formas principais: jogos sérios baseados em narrativa, os quais apresentam possíveis situações-problemas vivenciadas no dia a dia dos profissionais que constituem o público-alvo dos treinamentos; e um quiz interativo e gamificado, o qual visa auxiliar na avaliação formativa dos participantes dos treinamentos. A plataforma foi disponibilizada para os profissionais do ICI a fim de que estes possam a empregar nos próximos treinamentoss a serem realizados

e receber feedback sobre sua usabilidade e seu impacto junto aos usuários. Os profissionais do ICI, que colaboraram com esta pesquisa, atestaram que a plataforma atendeu suas expectativas, permitindo que estes a empreguem nas próximas capacitações a serem realizadas. Os profissionais destacaram, ainda, o caráter inovador e lúdico das soluções baseadas em jogos narrativos e no quiz gamificado, os quais representam novas formas de engajar os participantes dos treinamentos e colaboraram com a conscientização sobre a importância do diagnóstico precoce de sintomas relacionados ao câncer infantojuvenil.
PALAVRAS-CHAVE: Jogo Narrativo, Gamificação, Câncer Infantojuvenil, Diagnóstico Precoce

ABSTRACT: Childhood cancer, unlike cancer in adults, has no risk factors linked to lifestyle or environmental conditions and can present symptoms like those of common diseases among children, making the disease difficult to diagnose. One of the main ways to combat childhood tumors is early diagnosis, accompanied by therapeutic guidance, to provide the individual with greater chances of cure and a better quality of life after treatment. Considering these issues, this work aimed to develop an informational platform to support the training of health and education professionals on the early diagnosis of childhood cancer. This study began with a review of the literature and related works, seeking to scientifically support the present study, in addition to carrying out exploratory research with professionals from the Children's Cancer Institute of Porto Alegre aiming to understand their day-to-day work and their initiatives aimed at raising awareness about the importance of early diagnosis of childhood cancer. These professionals assisted in the design and development of the proposed platform as well as in the evaluation of its informational content. The developed platform presents informational content in two main ways: narrative games, which present problem situations experienced in the daily lives of professionals who constitute the target audience for the training; and an interactive and gamified quiz, which aims to assist in the formative assessment of training participants. The platform is available to Children's Cancer Institute professionals so that they could use it in upcoming training sessions and receive feedback on its usability and impact on users. Children's Cancer Institute professionals, who collaborated with this research, attested that the platform met their expectations. The professionals also highlighted the innovative and playful nature of the solutions based on narrative games and gamified quizzes, which represent new ways of engaging participants in participating in training and helped raise awareness about the importance of early diagnosis of symptoms related to the childhood cancer.
KEYWORDS: Narrative game, Gamification, Childhood Cancer, Early Diagnosis

1 | INTRODUÇÃO

De acordo com o Instituto do Câncer Infantil (ICI) de Porto Alegre (ICI) [1] [2], o câncer infantojuvenil corresponde a um grupo de doenças que tem em comum o crescimento desordenado de células, as quais invadem os tecidos e os órgãos. O câncer representa a primeira causa de morte por doença entre crianças e adolescentes de 1 a 19 anos [3] [4].

Os tumores infantojuvenis são diferentes dos tumores adultos, visto que eles geralmente afetam as células do sistema sanguíneo e os tecidos de sustentação. Dentre

tais tumores, os mais frequentes na infância e adolescência são as leucemias (glóbulos brancos), os tumores do sistema nervoso central e os linfomas (sistema linfático), o neuroblastoma (tumor de células do sistema nervoso periférico, frequentemente de localização abdominal), o tumor de Wilms (tumor renal), o retinoblastoma (tumor da retina do olho), o tumor germinativo (tumor das células que vão dar origem às gônadas), o osteossarcoma (tumor ósseo) e os sarcomas (tumores de partes moles) [4]. Até o momento, diferente do câncer nos adultos, não existem evidências científicas que deixem clara a associação entre a doença e fatores de risco ligados ao estilo de vida ou às condições ambientais [5]. Além disso, tumores infantojuvenis podem apresentar sintomas parecidos com os de doenças comuns entre as crianças, razão pela qual a doença pode não ser identificada facilmente [5].

O atraso na identificação de um câncer infantojuvenil pode impactar na sobrevida e nas chances de cura do paciente. Segundo o Instituto Nacional de Câncer (INCA) [3] [4], em torno de 80% das crianças e adolescentes acometidos pela doença podem ser curados, caso sejam diagnosticados precocemente e tratados em centros especializados. O diagnóstico precoce e uma das ferramentas que pode ajudar a combater o câncer infantojuvenil, melhorar o tratamento e entender como a doença se manifesta, dando a crianças, de todas as idades, maiores chances de sobrevivência [6].

Observa-se a necessidade de os responsáveis serem persistentes com o profissional de saúde, que atende os seus filhos, a fim de proceder com maiores investigações para evitar um possível atraso nesse diagnostico [7]. Como destacado pela Organização Mundial de Saúde (OMS) [8], o papel do diagnóstico precoce é o de permitir que gestores de saúde selecionem e implementem programas que auxiliem a identificar, o mais cedo possível, tu mores malignos para se ter resultados mais eficientes no trata mento e na utilização de recursos. Fica evidente, assim, a importância do diagnóstico precoce para que o paciente tenha maiores chances de apresentar resultados positivos a partir da realização de um tratamento adequado já no início da doença. Segundo Santos e Soares [9], a detecção precoce e rápida depende das ações de todos os envolvidos em torno do paciente.

Nota-se a necessidade de promover, de forma constante, o treinamento de profissionais da saúde, principalmente aqueles não especializados em oncologia infantojuvenil, e da população em geral para que se possa detectar, de forma precoce, tumores malignos em crianças e adolescentes. Para tanto, ações relacionadas à atenção básica são de fundamental importância, uma vez que constituem o primeiro nível de atenção em saúde, no âmbito individual e coletivo. Os profissionais, que atuam nesse primeiro nível de atenção, devem estar aptos para reconhecer sinais e sintomas que podem indicar um câncer infantojuvenil. Soma-se a tal questão o fato de que, além de profissionais da saúde, profissionais da educação, que estão em contato com crianças diariamente, podem auxiliar na identificação de sintomas precoces do câncer infantojuvenil, alertando os responsáveis pela criança.

Sistemas computacionais e aplicativos móveis podem auxiliar no treinamento de profissionais de saúde e da educação visando à realização do diagnóstico precoce de câncer infantojuvenil, principalmente em relação ao entendimento da importância da identificação de sintomas de um tumor em estágio inicial [10] [11]. A tecnologia da informação é uma importante aliada para a disseminação de informações através de diferentes formas, sendo uma dessas o desenvolvimento de aplicativos voltados à área da saúde que possam ser acessados por aplicativos moveis e/ou web [12].

Dentre as diferentes tecnologias da informação, tem-se os jogos lúdicos baseados em narrativa e aplicativos interativos e gamificados, como, por exemplo, o quiz. Jogos lúdicos se referem a simulações (digitais ou não digitais) que combinam informações educacionais com conteúdo de entretenimento e tecnologias [13] [14]. Considerando as diferentes formas de desenvolver um jogo lúdico, tem-se os jogos baseados em narrativa. Segundo Zhu et al. [15], esses jogos permitem uma imersão significativa no enredo narrado aos usuários, pois proporciona o envolvimento destes com toda uma narrativa criada para proporcionar conhecimento. Chun et al. [13] complementam tal informação, afirmando que jogos baseados em narrativa, baseados em histórias reais, mostraram uma autoeficácia, mas reduziram o prazer em comparação com histórias de fantasia.

Na cidade de Porto Alegre, fica a sede do ICI, o qual atua há mais de trinta anos na prevenção e no tratamento do câncer infantojuvenil. A missão do ICI é aumentar os índices de cura e melhorar a qualidade de vida dos pacientes e seus familiares. Para tanto, dentre as diferentes ações realizadas, uma se concentra em treinamentos para profissionais da saúde e da educação sobre a importância do diagnóstico precoce bem como sobre os principais sintomas do câncer infantojuvenil.

A partir de reuniões com profissionais que atuam no núcleo de atenção ao paciente do ICI e de visitas às suas instalações, foi proposto o desenvolvimento de uma plataforma informacional, para computadores e dispositivos moveis, visando o auxílio a tais capacitações. Esta plataforma deveria permitir o controle da identificação de usuário, a fim de categorizá-lo como profissional da saúde ou da educação e a disponibilização de conteúdos de treinamento e avaliativo sobre o diagnóstico precoce.

Com base em tais questões, este capítulo teve, por objetivo, o desenvolvimento de tal plataforma informacional, para apoio ao treinamento sobre o diagnóstico precoce do câncer infantojuvenil, voltada a profissionais da saúde e da educação. A plataforma apresenta o conteúdo informacional de duas formas principais:

- Jogos lúdicos baseados em narrativa, os quais visam auxiliar a capacitação a partir da apresentação de possíveis situações-problema vivenciadas do dia a dia dos profissionais que constituem seu público-alvo;
- Um quiz interativo e gamificado, o qual visa auxiliar na avaliação formativa dos participantes da capacitação.

A plataforma desenvolvida foi apresentada aos profissionais do ICI, que colaboraram com esta pesquisa, os quais ates taram que a plataforma atendeu suas expectativas, permitindo que estes a empreguem nos próximos treinamentos a serem realizados. Os profissionais destacaram, ainda, o caráter inovador e lúdico das soluções baseadas em jogos narrativos e no quiz gamificado, os quais representam novas formas de engajar os participantes na participação dos treinamentos e colaboraram com a conscientização sobre a importância do diagnóstico precoce de sintomas relacionados ao câncer infantojuvenil.

Além desta seção introdutória, o artigo está organizado como segue. A seção 2 apresenta os materiais e métodos empregados neste estudo. A seção 3, por sua vez, apresenta os resultados atingidos. Já a seção 4 discute tais resultados e, por fim, a seção 5 traz as conclusões obtidas até o momento.

2 | MATERIAIS E MÉTODOS

A presente seção traz a descrição dos materiais e métodos empregados no projeto e desenvolvimento deste estudo.

2.1 Estratégia de busca e critérios de inclusão

Esta pesquisa iniciou com buscas por artigos científicos em bases de conhecimento como Google Acadêmico, Scopus, Pubmed, Web of Science, IEEE e Arxiv. Foram, então, selecionadas publicações, a partir de 2018, cujos objetivos estivessem relacionados ao câncer infantojuvenil aliado a uma ou mais palavras-chave: diagnóstico precoce, jogo sério baseado em narrativa, plataforma informacional, gamificação. Observou-se que a divulgação da importância do diagnóstico precoce do câncer infantojuvenil vem despertando o interesse da comunidade científica, principalmente em relação à proposição de soluções digitais.

Silva [16] apresenta um estudo que objetivou avaliar a eficácia de um programa de capacitação sobre o diagnóstico precoce do câncer infantojuvenil entre profissionais da atenção básica. A amostra do estudo foi composta por profissionais que atuam na área da estratégia de saúde da família e nos núcleos de apoio à saúde da família. Os profissionais foram divididos em equipes de, no máximo, quarenta pessoas e passaram por três etapas: (1) aplicação de um questionário pré-teste, com questões que abordavam sinais e sintomas frequentes na oncologia pediátrica e situações assistência multidisciplinar desses pacientes, e um questionário socioeconômico; (2) treinamento dos profissionais sobre como reconhecer os sinais e sintomas da doença da criança e do adolescente com câncer infantojuvenil; (3) aplicação de um questionário pós-teste para avaliar o impacto do treinamento na obtenção de conhecimento sobre crianças e adolescentes com câncer. Como resultado, o estudo revelou que os profissionais da atenção básica melhoraram a

sua performance.

Vasquez et al. [17], por sua vez, realizaram um estudo piloto prospectivo nas cidades de Callao e Lima no Peru que teve, por objetivo, testar a viabilidade de implementação de um aplicativo, chamado ONCOped, e explorar sua utilidade potencial na redução da latência do diagnóstico e tempo de referência em crianças e adolescentes com câncer. O aplicativo funciona como um sistema integrado de consulta e tomada de decisão, onde o profissional responsável insere informações sociodemográficas, sintomas clínicos e outras informações. Tais dados são, então, enviados a um especialista de plantão que faz recomendações para avaliações adicionais ou encaminhamentos oportunos. O resultado deste estudo foi a redução do tempo para o diagnostico, que passou de vinte e dois dias da forma convencional para sete dias utilizando, além da redução do tempo entre a data de referência e a data da primeira consulta, o qual passou de sete dias para dois dias.

Destaca-se, ainda, o estudo de Da Silva et al. [10] que descreve o desenvolvimento de um aplicativo, voltado ao treinamento e à atualização de profissionais de saúde e do público em geral, através da parceria entre o Instituto Federal do Ceará e a Associação Peter Pan. Tal aplicativo aborda a detecção de sintomas do câncer infantojuvenil, através de conteúdos digitais espera disponibiliza um chat que permite que o profissional da saúde converse diretamente com um médico plantonista da Associação Peter Pan. Já para o público geral, o aplicativo não exige um cadastro e disponibiliza conteúdo sobre os tumores malignos, sobre tratamentos e cuidados que se deve ter com os pacientes.

Por fim, o estudo de Doulavince, e Mandetta [18] teve por objetivo elaborar e validar o jogo de tabuleiro, chamado “Skuba! An adventure under the sea”, voltado a comunicação efetiva entre profissionais da saúde e crianças com câncer. Para tanto, as autoras seguiram as cinco fases descritas a seguir. Na primeira, foi realizada uma análise onde se utilizaram os resultados de um estudo descritivo de abordagem qualitativa para identificar as necessidades de informação de crianças diagnosticadas com câncer e que estavam em tratamento quimioterápico. A segunda fase, denominada de conceito, se deu por reuniões que visaram definir o objetivo do jogo e os elementos para a composição deste. Já a terceira fase, chamada de projeto, focou na criação de um protótipo de jogo enquanto a quarta fase, chamada de implementação, abordou a projeção do protótipo na plataforma escolhida. A quinta fase foi responsável pela avaliação do jogo ˜ em termos de jogabilidade, validação do conteúdo e usabilidade. Como resultado, as autoras sugerem o desenvolvimento de jogos que contemplem a participação de crianças no processo, bem como na avaliação, de modo a adequar estes a sua compreensão e as suas necessidades.

Nota-se que o tema do desenvolvimento de jogos e aplicativos interativos e gamificados, digitais ou não, relacionados ao câncer infantojuvenil, vem sendo discutido e abordado em trabalhos científicos.

2.2 Coleta de Requisitos

Com o objetivo de levantar requisitos para a plataforma informacional, esta etapa consistiu em visitas as instalações do ICI e em realizar uma pesquisa exploratória, junto ao dia a dia dos profissionais da instituição, a fim de conhecer suas atividades. Pôde-se, assim, conhecer as suas principais iniciativas realizadas para a capacitação de profissionais de saúde e educação em relação ao diagnóstico precoce. Assim, após reuniões com estes profissionais, foram identificados os seguintes requisitos para o desenvolvimento da plataforma informacional proposta:

- Os usuários seriam profissionais da saúde e da educação que tenham contato com crianças e adolescentes;
- A plataforma deveria auxiliar na apresentação informações sobre o câncer infantojuvenil;
- A plataforma deveria auxiliar na avaliação formativa dos ˜ participantes da capacitação;
- A plataforma deveria empregar um ou mais recursos que auxiliassem a engajar e a incentivar a participação de profissionais da saúde e da educação na realização das capacitações ofertadas pelo ICI.

A partir de tais requisitos, foi realizado o projeto e o desenvolvimento da plataforma informacional proposta.

2.3 Projeto e desenvolvimento da plataforma informacional

Para o desenvolvimento da plataforma informacional proposta, foi adotada a metodologia de desenvolvimento centrada no usuário, onde este participa ativamente das etapas de ideação, desenvolvimento e testes de validação. Para tanto, contou-se com a participação de cinco profissionais do ICI:

- Uma doutora em genética e biologia molecular, líder de projetos do ICI;
- Um doutor em ciências médicas, médico oncologista pediátrico do ICI;
- Um bacharel em pedagogia, coordenadora do núcleo de apoio ao paciente, e responsável pela área de recreação e apoio pedagógico do ICI;
- Dois responsáveis técnicos pelo setor de tecnologia da informação e desenvolvimento institucional do ICI.

Tais profissionais atuaram como *stakeholders* neste projeto.

A primeira fase desta etapa foi a de ideação sobre o projeto, considerando as etapas 2.1 e 2.2. A partir de então, decidiu-se que o conteúdo informacional da plataforma seria apresentado através de dois recursos principais:

- Jogos sérios baseados em narrativa, cada um tratando de um tipo de câncer infantojuvenil e seus sintomas. Estes jogos visam auxiliar nos treinamentos de profissionais da saúde e da educação através da apresentação de possíveis situações-problemas vivenciadas do dia a dia destes;
- Um quiz interativo e gamificado, o qual visa auxiliar na avaliação formativa dos participantes dos treinamentos.

As próximas seções apresentam os resultados obtidos a partir do desenvolvimento da ferramenta e uma discussão sobre estes e testes realizados pelos profissionais do ICI.

3 | RESULTADOS

A partir das etapas da seção 2, foi possível identificar os principais tipos de câncer infantojuvenil e suas características:

- Leucemia;
- Linfoma;
- Neuroblastoma;
- Tumor de Wilms;
- Rabdomiossarcoma;
- Retinoblastoma;
- Osteossarcoma;
- Tumores do sistema nervoso central.

A seguir, passou-se para o desenvolvimento da plataforma no formato *web app* a fim de que fosse possível utilizá-la em diferentes dispositivos. A primeira funcionalidade implementada foi o cadastramento e a autenticação dos usuários. Para tanto, três tipos de perfis de acesso foram definidos:

- Administrador, o qual pode configurá-la, inserindo, alterando e/ou excluindo informações desta;
- Profissional da saúde, voltado ao participante do treinamento com tal perfil e sem permissões de administrador;
- Profissional da educação, voltado ao participante da capacitação com tal perfil e sem permissões de administrador.

Ao acessar a plataforma, o usuário deve efetuar *login* a fim de validar seu perfil e suas informações de acesso. Uma vez validado o acesso, a tela inicial e exibida para o usuário (Figura 1). Esta tela apresenta os *cards* de informações sobre os tipos de câncer infantojuvenil e o menu com as demais opções (na versão *mobile*, as opções são exibidas no rodapé, e, na versão *desktop*, as opções são exibidas em um menu lateral esquerdo).

As informações sobre os tumores variam conforme o tipo de usuário logado na

plataforma, sendo que, para o profissional da saúde, são disponibilizadas informações sobre a doença, sintomas, alertas e um fluxograma, enquanto, para os profissionais da educação, são disponibilizadas informações sobre o câncer e os sintomas do tumor. A Figura 2 apresenta as informações acessadas sobre a leucemia por um profissional da educação e por um profissional da educação onde, além das informações em forma de texto, permite o acesso a um fluxograma sobre sinais de alerta para as leucemias (Figura 3).

Além dessa tela inicial, tem-se a seção do quiz e a dos jogos narrativos.

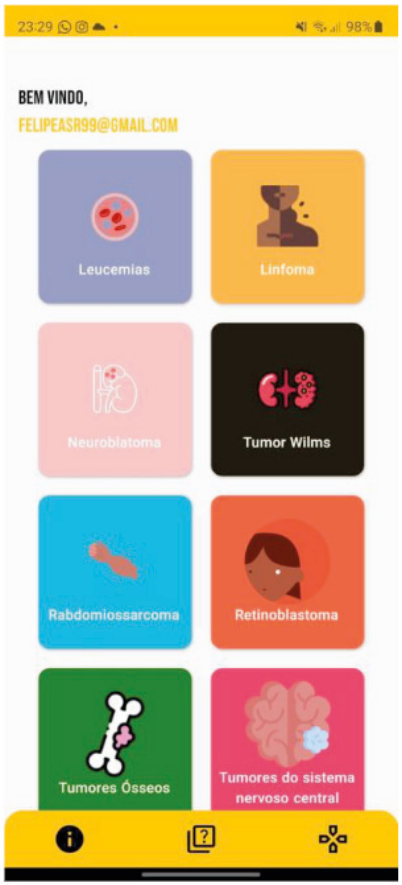


Figura 1: Tela inicial da plataforma, apresentando os cards que permitem acessar as principais informações sobre os tipos de câncer infantojuvenil para ambos os profissionais da saúde e da educação.

Figura 2: Tela de informação sobre leucemia para profissionais da saúde.

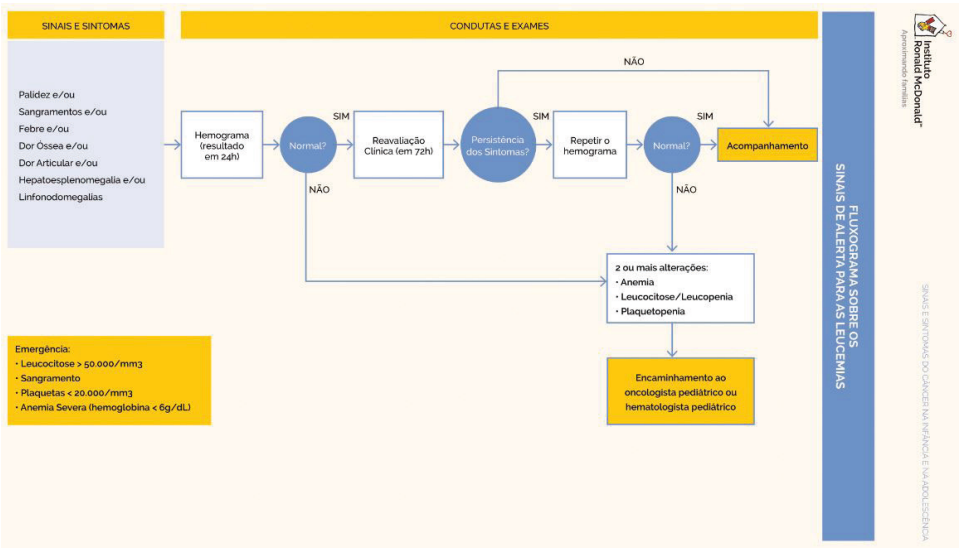


Figura 3: Fluxograma exibido na tela de informação sobre leucemia para profissionais da saúde (Fonte: Instituto Ronald McDonald).

3.1 Quiz

Ao conversar com os profissionais do ICI a fim de levantar os requisitos necessários para a plataforma, estes nos informaram que seria interessante o desenvolvimento de uma solução digital voltada à avaliação formativa dos participantes dos treinamentos. Foi proposto, então, o desenvolvimento de um quiz, interativo e gamificado, o qual apresenta dezenove afirmações sobre o conteúdo do treinamento com duas opções de respostas: verdadeiro e falso.

A Figura 4 (a) apresenta o exemplo de uma questão apresentada no quiz. O quiz foi desenvolvido com o conteúdo disponibilizado pelos profissionais do ICI, que tem como público-alvo tanto os profissionais da saúde quanto os da educação. A fim se inserir elementos de desafios e recompensas, próprios do conceito de gamificação, a ideia e incentivar os participantes a interagirem com o quiz a fim de reforçar os conceitos trabalhados no treinamento ao mesmo tempo em que os profissionais do ICI conseguem avaliar o processo de ensino-aprendizagem. Para cada participante da capacitação, ou a cada rodada que um mesmo participante responde ao quiz, as questões são embaralhadas. Cada acerto ou erro é computado e, ao final, a plataforma apresenta um *ranking* com a pontuação de todos os participantes (Figura 4 (b)).

(a) (b)

Figura 4: Quiz. (a) Exemplo de uma questão apresentada no quiz; (b) Exemplo de ranking ao final do quiz.

Considerando que a avaliação formativa não caráter tem classificatório, embora se tenha o *ranking* com a pontuação dos participantes ao final do quiz, cada um destes tem acesso a seus acertos e erros de forma individual, podendo rever os conceitos que precisam ser mais trabalhados junto aos profissionais do ICI que ministram as capacitações e, então, refazer o quiz.

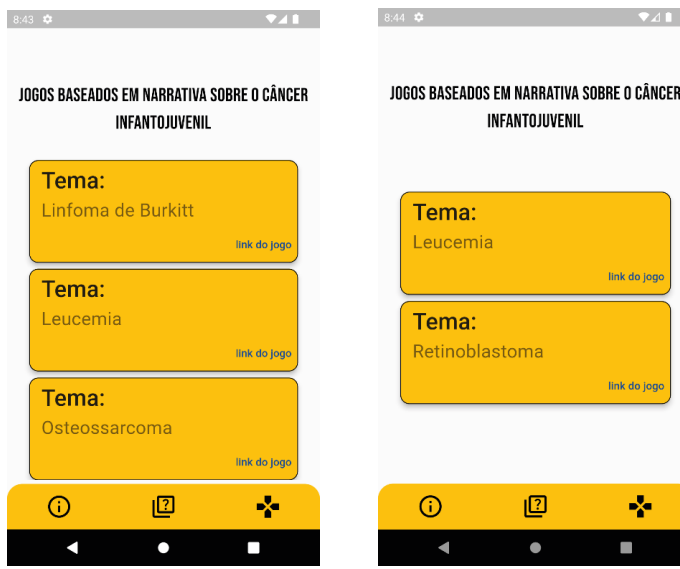
O *ranking* e ordenado pela maior pontuação, ou seja, e pelas quantidades de acertos nas perguntas respondidas no quiz.

3.2 Jogos Sérios Baseados em Narrativas

Completando a proposta deste estudo, esta subseção apresenta os jogos sérios baseados em narrativa desenvolvidos. Inicialmente, foram desenvolvidos quatro jogos, sendo dois jogos específicos para o treinamento dos profissionais da saúde, um jogo específico para o treinamento dos profissionais da educação e um jogo que considera ambos os usuários. Foram trabalhadas as seguintes temáticas para os jogos:

- Linfoma de Burkitt (profissional da saúde);
- Osteossarcoma (profissional da saúde);
- Neuroblastoma (profissionais da educação);
- Leucemia (profissionais da saúde e da educação).

As Figura 5 apresenta as telas com as opções de jogos para os profissionais da saúde e da educação.



(a) (b)

Figura 5: Opções de jogos narrativos. (a) Jogos para profissionais da saúde; (b) Jogos para profissionais da educação.

Os jogos possuem a proposta de serem sérios, apresentando conceitos sobre tumores específicos, e de serem baseados em narrativa. As narrativas foram desenvolvidas para apresentar situações-problemas que podem ocorrer no dia a dia dos profissionais da saúde e da educação que lindam com crianças e adolescentes. A ideia principal e auxiliá-los a reforçar os conceitos sobre sintomas do câncer infantojuvenil visando o diagnostico precoce da doença.

Para tanto, à medida que o enredo vai sendo apresentado ao usuário, este deve tomar decisões que influenciam na continuidade e no desfecho das situações. As narrativas, por esse motivo, se diferenciam na linguagem e cenários para cada profissional:

- Para os profissionais da saúde, as situações se passam em unidades básicas de saúde (UBS) e apresentam informações técnicas sobre os sintomas do câncer infantojuvenil;
- Para os profissionais da educação, as situações ocorrem em escolas e e empregada uma linguagem não técnica para abordar os sintomas do câncer infantojuvenil.

No jogo relacionado ao de linfoma de Burkitt, põe exemplo, o jogador e um médico da UBS que se encontra quase no final do seu horário de atendimento ao público. Este atende uma mãe e seu filho, o qual está sentindo dores na região da barriga. Conforme os sintomas da criança são relatados pela sua mãe, decisões possíveis vão sendo apresentadas ao jogador. Cada decisão leva a um cenário diferente, nos quais o jogador pode, como desfecho, descobrir um diagnóstico precoce de Linfoma de Burkitt ou diagnosticar a criança, erroneamente, com uma infecção gastrointestinal. As Figuras 6 e 7 apresentam algumas telas desse jogo.

Figura 6. Tela inicial da narrativa sobre linfoma de Burkitt (profissionais da saúde).

Figura 7. Tela da narrativa sobre linfoma de Burkitt apresentada logo após o usuário escolher a opção "Pergunta para o Jairo sobre o local da dor" na tela da Figura 6.

Embora o cenário da narrativa seja estático, as telas apresentam dois ou mais botões de escolha para que o usuário selecione uma opção referente à decisão tomada após analisar a situação-problema apresentada. Tem-se a possibilidade de dois finais, os quais são definidos a partir das escolhas do usuário. Por exemplo, a narrativa sobre o linfoma de Burkitt possui os finais apresentados nas Figuras 8 e 9.

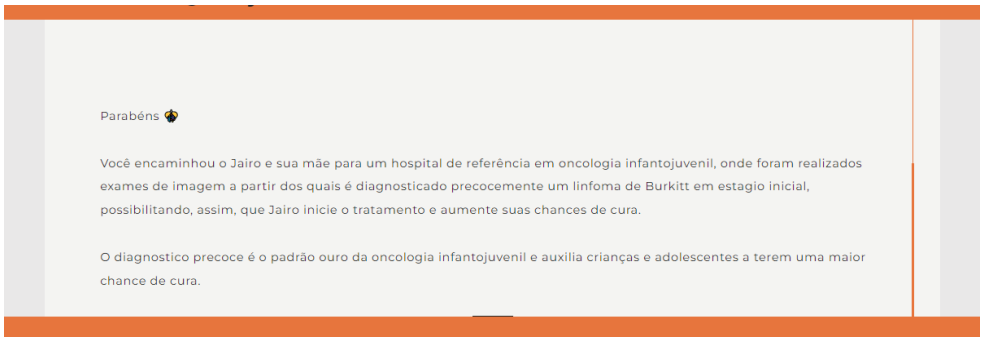


Figura 8. Tela final da narrativa sobre linfoma de Burkitt após o jogador realizar as análises corretas que permitiram a realização do diagnóstico precoce.

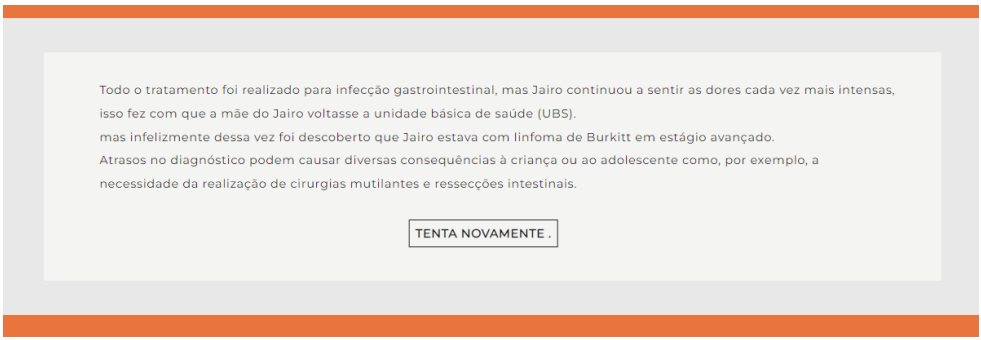


Figura 9. Tela final da narrativa sobre Linfoma de Burkitt após o jogador não realizar as análises corretas, não realizando o diagnóstico precoce.

Ao todo, cada jogo tem em torno de doze telas apresentando as diferentes possibilidades de desenvolvimento de narrativas além de dois finais diferentes. O jogo foi desenvolvido com foco em plataforma *online* e em páginas responsivas. Desta forma, pode rodar em diferentes dispositivos, como móveis e estações de trabalho. Para tanto, utilizou-se, na implementação, as ferramentas Flutter[1] e o Twine[2], além de imagens geradas de forma gratuita por ferramentas de inteligência artificial.

Os profissionais do ICI avaliaram a plataforma como um todo, o quiz e os jogos. Estes se mostraram satisfeitos com os resultados, indicando que a plataforma os auxiliará a tornar os treinamentos sobre sintomas do diagnóstico precoce do câncer infantil mais dinâmicas, desafiadoras e interessantes para os participantes. A próxima seção discute estes resultados.

4 | DISCUSSÃO

Os profissionais do ICI, responsáveis pelos treinamentos sobre o diagnóstico precoce, indicaram que a plataforma desenvolvida é uma ferramenta que, além de auxiliar em tais treinamentos, permite inovar junto aos recursos já usados pela instituição. Os treinamentos que, até então, eram realizados, unicamente, através do uso de apresentação de slides e avaliações em folhas de papel, passaram a contar com recursos digitais e tecnológicos que trazem vantagens de metodologias ativas: colocam o aluno como protagonista de sua própria aprendizagem. Assim, tanto os participantes dos treinamentos como os ministrantes passaram a contar com novos recursos, os quais podem ser acessados de forma remota sem exigir configurações específicas de *hardware* e *software*.

Os profissionais do ICI destacaram, ainda, que a plataforma informacional proporciona um acesso rápido as informações básicas sobre os tumores infantojuvenis, além de apresentar um quiz interativo e gamificado e jogos narrativos, os quais se propõem

1 https://flutter.dev/games
2 https://twinery.org/

a engajar os participantes nos treinamentos a partir da combinação de desafios e ludicidade.

No âmbito do desenvolvimento, foi destacado que, por ser um aplicativo do tipo *web app*, foi possível ter um produto que atinge uma ampla gama de dispositivos, tanto moveis como *desktop*. Foram destacadas como positivas as características relacionadas à funcionalidade, como o acesso a banco de dados, a portabilidade, a integração a outras ferramentas, a usabilidade (interface gráfica intuitiva, tanto para os administradores do sistema quanto para os usuários) e a comunicabilidade.

No entanto, indicaram que a ampliação da realização de testes com a plataforma, incluindo os participantes dos treinamentos, é importante a fim de que se possa identificar possíveis melhorias de usabilidade e comunicabilidade.

5 | CONCLUSÃO

Este artigo apresentou uma plataforma informacional voltada ao treinamento de profissionais da saúde e da educação sobre a importância do diagnóstico precoce do câncer infantojuvenil. Para tanto, esta aborda informações sobre os tumores como leucemias, linfoma, neuroblastoma, Tumor de Wilms, radomiossarcoma, retinoblastoma, tumores ósseos e os tumores do sistema nervoso central através de recursos digitais como quiz e jogos lúdicos baseados em narrativa.

Os jogos lúdicos narrativos e o quiz gamificado permitiram à combinação da apresentação de desafios, recompensas e ludicidade, abordando, para tanto, conceitos específicos através de ambientes gráficos e interativos. Estes têm a intenção de auxiliar na representação de situações reais voltadas, principalmente, ao ensino de determinados conceitos e treinamento de habilidades. Embora tais sistemas computacionais constituam uma área que tem crescido de forma acelerada nos últimos anos, nota-se, ainda, uma carência de propostas voltadas à área da oncologia, principalmente aquelas focadas no câncer infantojuvenil. Assim, pretende-se colaborar com os estudos e as propostas de soluções nesta área.

Por fim, como melhorias futuras na plataforma, planeja-se atualizar as imagens utilizadas nos jogos a partir da identidade visual do ICI, a qual traz personagens que representam a coragem das crianças e adolescentes a enfrentar o câncer infantojuvenil. Outra proposta futura trata da exibição dos acertos e erros para o usuário, ao final do quiz, de forma gráfica através de técnicas de visualização para apoio à decisão de gestores que atuam na área de oncologia pediátrica.

AGRADECIMENTOS

Agradecemos aos profissionais do Instituto do Câncer Infantil pela colaboração neste estudo.

REFERÊNCIAS

[1] ICI (2020). [link]. URL https://ici.ong/

[2] ICI, Entendendo o câncer infantojuvenil: Cartilha de orientação à escola, professores, estudantes e suas famílias. URL http://static.ici.ong/docs/Cartilha_Entendendo_o_ Cancer_Infantojuvenil.pdf

[3] INCA, Estimativa 2020: incidência de câncer no Brasi, Rio de Janeiro: INCA, Rio de Janeiro, 2020. URL https://www.inca.gov.br/sites/ufu. sti.inca.local/files//media/document//estimativa-2020-incidencia-de-cancer-no-brasil.pdf

[4] INCA, Incidência, mortalidade e morbidade hospitalar por câncer em crianças, adolescentes e adultos jovens no Brasil, Rio de Janeiro : INCA, Rio de Janeiro, 2016. URL https://www.inca.gov.br/publicacoes/livros/

[5] INCA, Cancer infantojuvenil, 2022. URL https://www.inca.gov.br/tipos-de-cancer/ cancer-infantojuvenil

[6] C. J. R. Mullen, R. D. Barr, E. L. Franco, Timeliness of diagnosis and treatment: the challenge of childhood cancers, Br J Cancer 125 (2021) 1612–1620. doi:10.1038/s41416-021-01533-4.

[7] R. K.E.s, C. B., Early diagnosis of childhood cancer: a team responsibility, Rev Assoc Med Bras 49 (2003) 29–34. doi:10.1590/ s0104-42302003000100030.

[8] WHO, Guide To Cancer Early Diagnosis, Gineva: WHO, Gineva, 2017. URL https://apps.who.int/iris/handle/10665/254500 [9] R. e ampliada (Ed.), Atenção Básica na detecção precoce e no acompanhamento das crianças e dia adolescentes com câncer. in: O diagnóstico precoce do câncer infantojuvenil e a atenção básica: estratégias e desafios para aumentar as chances de cura, Rio de Janeiro : Instituto Ronald McDonald, Rio de Janeiro.

[10] J. B. Da Silva, J. G. De Freitas, J. E. S. Moraes, J. D. F. Viana, T. F. L. Bandeira, R. B. Braga, S. E. A. Prazeres, C. T. De Oliveira, APPonco - Um aplicativo móvel para acesso rápido e seguro à informação sobre o câncer infantojuvenil, Porto Alegre: Sociedade Brasileira de Computação, Minas Gerais. Anais, 2021. URL https://doi.org/10.5753/webmedia_estendido.2021. 17613

[11] Instituto Beaba, Alphabet Cancer. URL https://www.mktvirtual.com.br/cases/appalphabeatcancer/

[12] West, Mark, Vosloo, Steven, Diretrizes de políticas da UNESCO para a aprendizagem móvel, Unesco: Brasília.

[13] C. Zhou, A. Occa, S. Kim, S. Morgan, A meta-analysis of narrative game-based interventions for promoting healthy behaviors, Journal of Health Communication 25 (2020). doi:10.1080/10810730.2019.1701586.

[14] D. L. Farias, E. F. Damasceno, um jogo serio para análise de dados psicossociais no enfrentamento do câncer infantil, Journal of Health Informatics 12 (2020). doi: https://docs.bvsalud.org/biblioref/2022/06/1371081/art_5_760.pdf.

[15] A. Zhu, M. Amith, L. Tang, R. Cunningham, A. Xu, J. A. Boom, C. Tao, experimenting with a prototype interactive narrative game to improve knowledge and beliefs for the hpv vaccine, Springer International Publishing 13097 (2021). doi:10.1007/978-3-030-90966-6_14.

[16] L. C. SILVA JUNIOR, Impacto da capacitação dos profissionais da atenção básica de saúde quanto ao diagnóstico precoce do câncer infantojuvenil. (2019).

[17] L. Vasquez, J. Montoya, C. Ugaz, L. R ´ ´ıos, E. Leon, I. Maza, E. Maradiegue, S. Chavez, F. Tarrillo, R. Diaz, C. Pascual, N. Rojas, ´ M. Tello, C. Moore, D. Shah, B. Cotrina, J. Bartolo, J. Perez, V. Palacios, Oncopeds: A mobile application to improve early diagnosis and timely referral in childhood cancer in a low- and middle-income country a pilot study, Pediatric Blood & Cancer 68 (4) (2021). doi:https: //doi.org/10.1002/pbc.28908.

[18] D. A. Doulavince, M. A. Mandetta, Desenvolvimento e validação de um jogo de tabuleiro para crianças com câncer, Paulista Enfermagem 35 ˆ (2022). doi:10.37689/acta-ape/2022AO00121.

[19] Flutter, Flutter, Disponível em: https://www.flutter.dev (2022). [20] Firebase, Cloud storage, Disponível em: https://cloud.google.com (2022). [21] miro, Miro, Disponível em: https://miro.com (2022).

[22] Twine, Disponível em: https://twinery.org (2022).

SEGURANÇA EM REDES WI-FI COM VPN

Data de submissão: 01/12/2024 *Data de aceite: 02/12/2024*

Fábio Hugo Souza Matos
Engenheiro Eletricista (UFRO).

Geraldo de Magela Carvalho de Oliveira
Professor at the Federal Institute of Education, Science and Technology of Rondônia – IFRO.
Porto Velho – RO, Brazil.

Marcelo José Peres Gomes da Silva
Esp. em Redes de Computadores e Comunicação de Dados (UEL).

Aírton Ribeiro dos Santos
Pós-graduação em docência do ensino superior. Mestrando PGDRA/UFRO.

Fabrício Moraes de Almeida
Doutor em Física (UFC) e pós-doutor. Esp. Análise e Desenvolvimento de Sistemas/ Eng. de Software (FUNIP). Professor do departamento de Engenharia Elétrica/ UFRO, Brasil.

RESUMO: O capítulo do livro tem como objetivo demonstrar alguns métodos de criptografia existentes para redes Wi-Fi e suas vulnerabilidades, dessa forma, realizou-se um estudo de caso apresentando alguns métodos de quebra das chaves de segurança dessas redes e uma opção de otimização na segurança do usuário, prevenindo possíveis riscos e ameaças à sua privacidade. As ferramentas que foram utilizadas para a realização do estudo de caso são conhecidas como *aircrack-ng*, *tcpdump, inSSIDer e OpenVPN*, onde todas elas são ferramentas livres, de fácil obtenção e de fácil utilização, sem que haja a necessidade de conhecimentos avançados. Em vista do grande crescimento das redes Wi-Fi e do grande aumento de sua utilização, tanto em ambientes residenciais quanto em grandes empresas, a segurança dessas redes chamou muita atenção e se tornou foco de muita preocupação e de muitos estudos. Em uma era em que a informação tem grande valor, é necessário que haja a garantia de que as informações que estão na rede estejam seguras, sem que haja a possibilidade de serem roubadas, alteradas, ou qualquer outra ameaça a sua segurança que possa resultar em algum dano a algo ou alguém. Existem muitas vulnerabilidades nos protocolos de segurança das redes Wi-Fi, já que, por ser uma rede sem fio que tem como meio de transmissão o ar, fica exposto e possui limitações quanto aos métodos de segurança aplicados, por isso a necessidade de implementação de um novo método de segurança. O estudo de

caso foi realizado na cidade de Porto Velho/RO(Brasil), onde inicialmente, foram analisadas diversas redes Wi-Fi espalhadas pela cidade para verificação das seguranças utilizadas e para a exploração das vulnerabilidades. Portanto, constatou-se que a segurança das redes analisadas apresentou fragilidades e falhas, deste modo, a proposta de testes de implementação é demonstrar otimização da segurança das informações que trafegam na rede, garantindo ao usuário a privacidade e proteção de dados.
PALAVRAS-CHAVE: VPN, Redes de computadores, redes sem fio, Wi-Fi, segurança de rede, vulnerabilidade.

SECURITY IN WI-FI NETWORKS WITH THE USE VPN

ABSTRACT: In this work are mentioned the many existent methods of encryption to Wi-Fi networks and their vulnerabilities, from where a case study were developed presenting some methods of breaking the security keys of these networks and an option for improving the user safety, preventing possible risks and threats to his privacy. The tools that were used for the case study are known as aircrack-ng, tcpdump, inSSIDer and OpenVPN, where all of them are free, easy to obtain and easy to use, without needing any advanced knowledge. Considering the large growth of Wi-Fi networks and the large increase in its use, both in residences and in large enterprises environments, the security of these networks drew much attention and became the focus of much concern and many studies. In an era where information is valuable, there must be a guarantee that the information that are on the network are secured, without the possibility of being stolen, modified, or any other threat to its safety that may result in something or someone damaged. There are many vulnerabilities in the Wi-Fi security protocols, since, being a wireless network that has the air as its transmission medium, it is exposed and has limitations for the matter of the security methods applied, that's why it needs to be implemented with a new security method. The case study was conducted in the city of Porto Velho/RO (Brazil), where many Wi-Fi networks around the city were analyzed to verify which securities were being used and to explore their vulnerabilities. It was possible to see that the security of the analyzed networks were weak, then, the proposed implementation of this work is a way of improving the information security that transits over the network, ensuring user privacy.
KEYWORDS: Computer networks, wireless networks, Wi-Fi, networks security, vulnerability, VPN.

1 | INTRODUÇÃO

As redes sem fio proporcionam mobilidade, flexibilidade, e muitas outras vantagens em relação às redes com cabeamento, por isso o seu uso se tornou cada vez mais presente no cotidiano das pessoas, estando presentes em diversas áreas, na saúde, na educação, no ambiente empresarial, entre outras. E as redes Wi-Fi, padronizadas pelo IEEE 802.11, passam por crescimento desde a sua criação e proporcionam um padrão de comunicação wireless para os diversos dispositivos. Com o grande aumento de sua utilização, a qualidade da segurança das redes Wi-Fi passou a ser questionada.

A maior das desvantagens das redes sem fio está justamente relacionada ao seu

meio de transmissão, o ar. Uma vez que o sinal wireless não é um sinal confinado, fica exposto e pode ser interceptado por qualquer dispositivo capaz de captar sinais sem fio. Deste modo, a segurança dessas redes fica comprometida e se torna motivo de muita preocupação para os seus utilizadores. E uma rede para ser considerada segura tem que oferecer alguns parâmetros, sendo alguns deles: confidencialidade, autenticidade e integridade. Estes e outros serviços são considerados fatores primordiais para garantir segurança às informações que trafegam na rede, sendo indispensáveis para usuários que possuem informações sigilosas na rede.

O objetivo fundamental da segurança das redes sem fio é impedir os acessos não autorizados e a leitura, alteração ou destruição de qualquer informação contida nessas redes, por isso foram criados protocolos de segurança que seriam capazes de garantir esse objetivo. Porém, esses protocolos possuem vulnerabilidades que podem comprometer toda segurança da rede, que uma vez comprometida, se torna passível a ataques de pessoas mal-intencionadas que podem causar dano a algo ou alguém. Além disso, o trabalho tem como intuito apresentar as vulnerabilidades presentes nas redes Wi-Fi, realizando a quebra das chaves de segurança dessas redes utilizando ferramentas livres, e como objetivo específico oferecer uma solução para a privacidade das informações trafegadas na rede, uma vez que é necessário ter os dados protegidos caso algum invasor consiga obter acesso à rede. Essa solução para a privacidade dar-se-á através da criação de redes privadas virtuais com o software livre *OpenVPN*.

E foram realizados testes na segurança de redes Wi-Fi espalhadas pela cidade de Porto Velho/RO (Brasil), onde foi verificado que a vulnerabilidade dos métodos de criptografia utilizados em redes wireless estava presente em todas as redes analisadas. A partir dessas lacunas foi possível obter o acesso à rede e realizar diversas análises na rede, onde pode ser possível encontrar senhas particulares, fotos pessoais, entre outros arquivos.

Por exemplo, em 2024, o grupo de hackers estatais russos APT28 utilizou uma técnica chamada **"ataque ao vizinho mais próximo"** para ataques cibernéticos na rede Wi-Fi corporativa de uma empresa nos EUA a partir de milhares de quilômetros de distância (CISOADVISOR, 2024).

Por fim, foi feita a implementação da segurança com a utilização de redes privadas virtuais, que têm a função de criar um túnel virtual dentro de redes públicas compartilhadas que garante segurança às informações trafegadas nessas redes. Foi possível então verificar que as informações antes legíveis a qualquer um que invadisse a rede, não estavam mais disponíveis para um intruso. Vale ressaltar que esse método garante uma segurança à informação trafegada, mas também possui vulnerabilidades que podem ser exploradas.

2 | METODOLOGIA APLICADA

A metodologia aplicada neste trabalho compreende uma pesquisa exploratória com abordagem quantitativa, onde será realizada uma pesquisa bibliográfica e um estudo de caso. E a pesquisa exploratória é realizada sobre um problema onde é proporcionada maior familiarização com o mesmo, podendo utilizar um levantamento bibliográfico, e geralmente, assumindo a forma de um estudo de caso com resultados de dados quantitativos ou qualitativos. E tem foco em proporcionar uma visão geral do uso de redes Wi-Fi, concebendo uma maior compreensão e precisão, permitindo uma avaliação de quais conceitos existentes podem ser aplicados ao problema em questão.

Destarte, o processo de pesquisa se realizará por meio da pesquisa bibliográfica, a qual abrange a leitura e interpretação de livros, artigos, documentos, trabalhos acadêmicos, entre outros. A pesquisa bibliográfica é o passo inicial para a construção de um trabalho, de onde é tirada a fundamentação teórica do estudo. Ela auxilia na definição da justificativa e do problema, assim como na determinação dos objetivos e do produto final do trabalho. E a pesquisa bibliográfica tem como objetivo identificar as diferentes contribuições científicas disponíveis para determinado tema, este trabalho teve como referência bibliográfica de maior relevância os livros: Redes de Computadores, TANENBAUM (2003); Redes Sem Fio, MORAES (2011); Segurança de Redes Sem Fio, RUFINO (2011); e Criptografia e Segurança de Redes, STALLINGS (2012).

E por fim, o estudo de caso pode ser entendido como uma pesquisa específica de um problema, onde é realizado um amplo e detalhado estudo. Neste trabalho será realizado um estudo de caso explicativo na localidade de Porto Velho/RO, onde serão analisadas as redes Wi-Fi, de diversos lugares espalhados pela cidade, por meio de ferramentas livres utilizando o *software* livre Linux – Ubuntu 13.10. As ferramentas utilizadas para as coletas e análises de dados são: *aircrack-ng*, *inSSIDer*, *tcpdump* e *OpenVPN*.

3 | FUNDAMENTOS DE REDES DE COMPUTADORES

Segundo Miranda (2008), as redes de computadores vieram da imprescindibilidade de se compartilhar recursos entre comunidades de usuários geograficamente espalhados. São dadas como um conjunto de computadores e periféricos conectados, localmente e remotamente, com a possibilidade de se comunicarem uns com os outros. E para Alves (1998), a rede de computadores é formada pela interconexão de um conjunto de computadores autônomos, onde não existe relação de mestre/escravo entre eles, o que significa dizer que um não pode controlar o outro. E somente dois computadores já são o suficiente para que seja formada uma rede, não existindo um número máximo predeterminado (MIRANDA, 2008). Dois ou mais computadores devem ser conectados em rede através de algum meio de comunicação (AMORIM, 2011). São utilizados, basicamente, três meios de comunicação: fios ou cabos de cobre, fibras ópticas e transmissão por ondas

de rádio (MARX, 2008), conforme Figura 1.

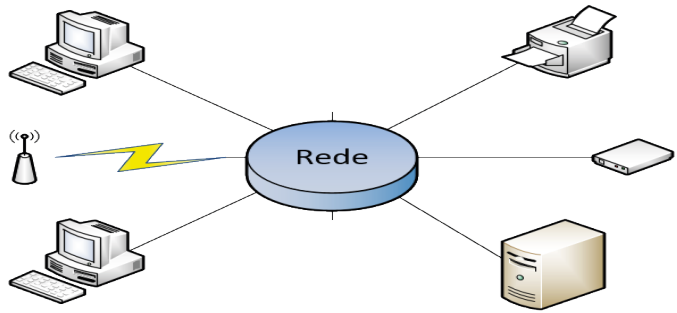


Figura 1: Exemplo de Rede de Computadores. Fonte: Elaboração Própria.

De acordo com Alves (1998), uma rede não precisa ser formada unicamente por computadores, sendo comum a presença de outros dispositivos de rede. Segundo Miranda (2008), as redes de computadores tem como finalidade um meio de comunicação com a disponibilidade de compartilhamento de dados, programas e outros recursos com devida confiabilidade. Com o aumento significativo do conhecimento em redes, foram feitas classificações dividindo-as e fazendo com que a troca de informação entre elas variasse agora de acordo com essa classificação. Foram classificadas de acordo com as tecnologias empregadas, a cobertura geográfica e a velocidade.

Atualmente, há vários tipos específicos, as mais conhecidas são: PAN (*Personal Area Network*), LAN (*Local Area Network*), MAN (*Metropolitan Area Network*) e WAN (*Wide Area Network*) (JARA; AUGUSTO, 2011). (a) PAN (*Personal Area Network*) - Rede de Área Pessoal: A PAN é uma rede doméstica que liga recursos diversos ao longo de uma residência. Um exemplo dela é a tecnologia Bluetooth. A LAN (*Local Area Network*) - Rede de Área Local: são redes de área local ou redes locais, conhecidas também como LANs, são redes de pequena cobertura geográfica que têm como objetivo o compartilhamento de recursos e a troca de informações. São redes privadas utilizando um conjunto de hardware e software que permite conectar computadores individuais e estações de trabalho em escritórios, empresas, escolas, edifícios, contidas numa mesma sala, prédio, ou campus com até alguns quilômetros de extensão. As redes locais tradicionais operam em velocidades entre 10 e 100 Mbps. As mais modernas conseguem atingir velocidades de até 10 Gbps. Essa rede tem baixo retardo (micro/nanossegundos) e são encontradas poucas taxas de erros de transmissão, 10^{-8} a 10^{-11}, (TANENBAUM, 2003).

E MAN (*Metropolitan Area Network*) - Rede de Área Metropolitana: As redes de área metropolitana ou redes metropolitanas, também conhecidas como MANs, são redes que ocupam aproximadamente o espaço de uma cidade e são constituídas de uma ou mais redes LANs, podendo ser uma rede privada ou pública. Por utilizarem tecnologias semelhantes, a rede MAN pode ser entendida como uma versão ampliada de uma LAN,

onde os dispositivos em rede podem se comunicar como se fizessem parte de uma mesma rede local. Comparada a LAN, apresenta uma taxa de erro maior, já que possui um maior alcance. São redes comumente encontradas em universidades, hospitais e em organizações com várias delegações espalhadas pela cidade capazes de transportar voz e dados (MIRANDA, 2008). Segundo Tanenbaum (2003), a rede de televisão a cabo é um exemplo de uma rede MAN, a qual abrange mais de uma cidade. Outra MAN surgiu como resultado do desenvolvimento no acesso à Internet sem fio com altas velocidades, padronizada como IEEE 802.16 e denominada de WiMAX.

Para WAN (*Wide Area Network*) - Rede de Área Geograficamente Distribuída: Redes de área geograficamente distribuídas ou redes geograficamente distribuídas, também conhecidas como WANs, são redes de comunicação de dados que abrangem uma grande área geográfica como um país ou um continente. Oferecem transmissão de dados provida por operadoras, como empresas de telefonia e telecomunicações. Devido ao custo elevado na comunicação, essas redes são públicas em sua maioria. A Internet é um exemplo de rede WAN, considerada a maior existente atualmente. Conecta milhões de redes LANs no mundo todo formando uma WAN. Surgiram com a necessidade de ampliação da rede devido ao crescimento das corporações, onde LANs já não eram suficientes para atender a necessidade demandada de informações e recursos compartilhados. Essas redes são formadas por conjuntos de servidores que formam grandes sub-redes que têm como função transportar dados entre os dispositivos de rede, sendo eles computadores ou outros dispositivos, de um ponto geográfico para outro (MIRANDA, 2008).

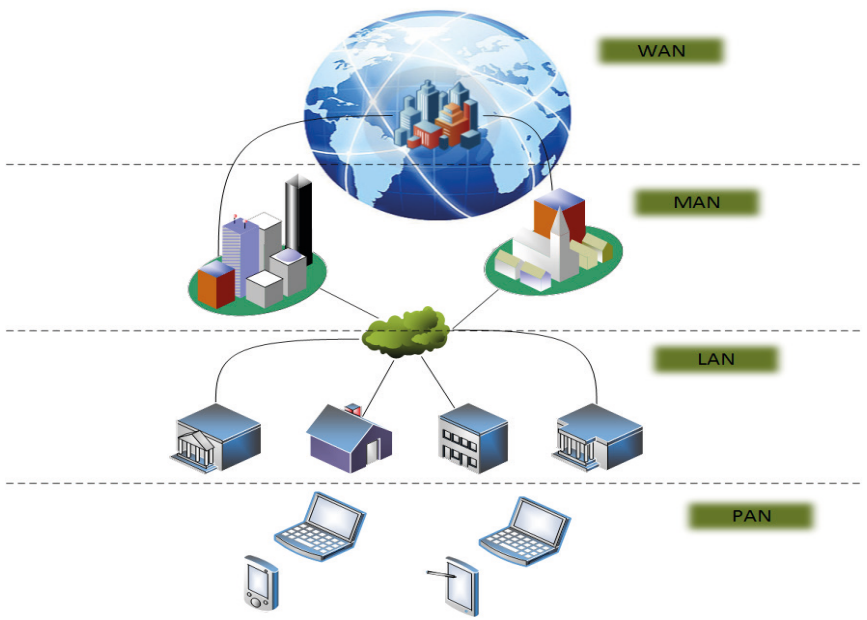


Figura 2: Representação das Redes LAN, MAN e WAN. Fonte: Elaboração Própria.2014/2024.

Devido ao crescimento das redes, o compartilhamento de recursos entre os usuários não estava sendo possível. Isso aconteceu com ausência de compatibilidade existente entre as diferentes tecnologias de plataformas de hardware e software das redes que foram criadas, dificultando ou impossibilitando a comunicação entre elas (MIRANDA, 2008). Cada fabricante possuía a sua tecnologia e a mesma só tinha suporte com quem a fabricou, sem a possibilidade de utilizá-la de forma conjunta às diferentes tecnologias. E com o avanço da tecnologia, houve a necessidade de melhorar essa incompatibilidade existente entre as diferentes tecnologias de rede. Assim, teve início uma busca por padrões para que houvesse uma integração entre os produtos dos diferentes fabricantes. E a padronização seria muito bem-vinda já que significaria maior lucratividade e mais oportunidades de negócios. Percebendo a importância de tal ação, surgiram organizações para realizar essa padronização, que definiram regras e modelos a serem seguidas pelas empresas para a fabricação de seus produtos (GOMES, 2004).

Além disso, as redes sem fio estão cada vez mais ganhando espaço, estando presentes em ambientes residenciais, empresariais, hospitalares, e muitos outros. Requerem assim, um alto grau de confiabilidade para os clientes dessas redes, fazendo com que o tema segurança de redes sem fio seja cada vez mais discutido e desenvolvido nessas redes. Então, foram criados protocolos de segurança com o intuito de proteger o acesso de pessoas não autorizadas e proteger os dados trafegados na rede, mantendo assim a autenticidade, a integridade e a confidencialidade da rede.

Segundo Rufino (2011), os métodos de segurança mais utilizados em redes sem fio são: Filtragem do endereço MAC (*Media Access Control*), os protocolos de segurança WEP, WPA (*Wi-Fi Protected Access*) e WPA2. Outro método de segurança que também tem sido bastante utilizado é a VPN (*Virtual Private Network*), que será abordado neste trabalho como a implementação de segurança para garantir a privacidade e a segurança das informações trafegadas em uma rede sem fio. O endereço MAC é um número único presente na interface física dos dispositivos definido pelo seu fabricante e controlado pelo IEEE. Foi criado para permitir a identificação única de um equipamento em relação a qualquer outro endereçamento.

A partir disso, foi criada uma forma de restringir o acesso ao AP de uma rede sem fio aos endereços MAC previamente cadastrado nesse concentrador. E onde somente seria permitida a autenticação de dispositivos possuindo endereços MAC conhecidos e cadastrados pelo AP. O que pode servir como um grande recurso para evitar pessoas não autorizadas de acessarem sua rede, mas que falha na restrição do equipamento, e não do usuário. Isso significa que um usuário que não necessariamente é o portador do equipamento com o endereço MAC cadastrado, pode facilmente, através de técnicas de escuta de tráfego, descobrir um endereço MAC registrado e realizar a clonagem desse endereço, conseguindo assim a autenticação no concentrador. Ainda que possua essa vulnerabilidade, é um método de segurança recomendado e que ajuda na defesa contra

acessos não autorizados (RUFINO, 2011).

O protocolo WEP surgiu como uma forma de garantir a segurança das redes sem fio, uma vez que, diferente das redes cabeadas, as redes wireless podem ter seu sinal facilmente interceptado. Portanto, surgiu a necessidade de cifrar os dados trafegados na rede. Esse é o protocolo mais antigo desenvolvido para garantir a segurança do padrão IEEE 802.11. Esse padrão possui dois modos de autenticação, um chamado de *Open System* e o outro de *Shared Key*. O primeiro modo, como o próprio nome sugere, é um sistema aberto, onde a autenticação é feita sem nenhuma forma de segurança. O segundo modo é baseado em uma chave compartilhada que é realizada na forma *challenge-response*. Uma estação que deseja se conectar a um AP solicita autenticação, então esse concentrador gera e envia um *challenge* para a estação que solicitou a autenticação, onde esse *challenge* é um texto desafio com informações pseudorrandômicas. Após receber o *challenge*, a estação requerente envia para o AP uma *response*, para que a autenticação seja autorizada ou não. A *response* é uma resposta ao AP, contendo as informações recebidas do *challenge* cifradas com o segredo compartilhado. Após o AP receber a *response*, caso a criptografia tenha sido feita com o segredo correto, o acesso é autorizado. A criptografia padrão utilizada nesse modo de chave compartilhada era o WEP. (AMORAS; BRABO; PEREIRA, 2004).

O WEP trabalha com o algoritmo simétrico de criptografia de fluxo denominado de RC4. O RC4 pode possuir 64 *bits* ou 128 *bits*, sendo que, no primeiro caso, 40 *bits* são de chave e os outros 24 *bits* são de um vetor de inicialização (IV – *Initialization Vector*), e, no segundo caso, 104 *bits* são de chave e os outros 24 *bits* são do vetor IV. Utiliza criptografia de chave simétrica, onde existe uma chave secreta para cifrar e decifras os dados trafegados, que deve ser compartilhada entre os dispositivos que querem se conectar a rede e o concentrador.

A chave do protocolo WEP é então composta de uma chave estática e um componente dinâmico (IV), onde esse componente é adicionado à chave para dificultar a descoberta da mesma. É feita então a concatenação desses dois componentes em um primeiro plano. A partir daí é gerado um fluxo de dados pseudorrandômico, que é somado à mensagem a ser transmitida através de uma operação XOR. Finalmente, essa mensagem cifrada é concatenada ao vetor de inicialização e transmitida. O receptor faz o processo reverso para decifrar a mensagem transmitida (MORAES, 2011).

No protocolo WEP, para garantir a integridade de um dado, é realizada a técnica de CRC, a qual gera um ICV (*Integrity Check Value*) para cada dado enviado. Na recepção de um dado, deve-se executar essa técnica CRC e comparar o valor ICV recebido com o gerado, para a verificação da integridade da mensagem, onde caso o ICV seja igual, a mensagem está integra, e caso contrário, sofreu alguma alteração.

Esse protocolo possui algumas vulnerabilidades que fizeram com que novas soluções para a segurança das redes sem fio fossem desenvolvidas. Serão tratadas neste trabalho algumas dessas vulnerabilidades, as quais serão citadas como alguns dos riscos

e ameaças à segurança das redes wireless (AMORAS; BRABO; PEREIRA, 2004).

A nova solução para eliminar as vulnerabilidades do protocolo WEP foi o protocolo WPA. Este novo protocolo foi desenvolvido pela Wi-Fi Alliance e lançado um pouco antes do padrão IEEE 802.11i, com a promessa de melhorar os problemas de segurança do antigo protocolo. O protocolo WPA utiliza um novo protocolo para gerenciamento de chaves dinâmicas, o TKIP, que agora gera chaves por pacotes, com o mesmo algoritmo de criptografia utilizado no WEP, o RC4. Porém, o vetor IV antes de 24 *bits* do WEP agora conta com 48 *bits* agregado a novas regras de sequenciamento, o que permite uma melhor e mais segura criptografia dos dados. Também foi inserido o código MIC (*Message Integrity Code*) para realizar as trocas dos números de sequência dos pacotes, melhorando a integridade das mensagens.

O WPA pode funcionar em dois modos, WPA *Personal* e WPA *Enterprise*. No primeiro modo, utiliza uma chave (WPA-PSK (*Pre-Shared Key*)) preestabelecida compartilhada entre o concentrador e as estações que vão se conectar ao mesmo. Foi feito para utilização em pequenas redes. No segundo modo, utiliza o padrão 802.1x para autenticação, que utiliza o protocolo EAP e um servidor RADIUS. Foi feito para utilização em redes de porte maior, empresariais, e necessita de mais um equipamento para a utilização do servidor. O protocolo de segurança WPA também possui vulnerabilidades, as quais serão comentadas como riscos e ameaças à segurança das redes wireless (MORAES, 2011).

O protocolo WPA2 surge então com a homologação do padrão IEEEE 802.11i, sendo baseado nesse padrão e desenvolvido pela Wi-Fi Alliance para aumentar a segurança do protocolo WPA em relação a criptografia e a integridade. Utiliza o protocolo CCMP e não mais o algoritmo RC4, mas sim o algoritmo AES, o qual é considerado mais robusto e faz a criptografia dos dados na forma de blocos ao invés da cifra de byte por byte. Mesmo com o protocolo diferente, foi mantida compatibilidade com o protocolo TKIP e o padrão 802.1x.

Modo	Tipo	WPA	WPA2
Personal Mode	Autenticação	WPA-PSK	IEEE 802.1X/EAP
	Encriptação	TKIP/MIC	AES
Enterprise Mode	Autenticação	IEEE 802.1X/EAP	IEEE 802.1X/EAP
	Encriptação	TKIP/MIC	AES

Quadro 1: Comparação dos Protocolos WPA x WPA2.

Fonte: MORAES (2011).

O WPA2 exige hardwares mais modernos e robustos, já que exige muito mais processamento que os outros protocolos de segurança. O algoritmo AES desse protocolo pode possuir uma chave de até 256 *bits*, que tem um grau de segurança elevado, tornando o padrão WPA2 o padrão atual mais seguro para redes Wi-Fi (MORAES, 2011).

Dessa forma, foi encontrada uma vulnerabilidade nesse protocolo, mas para um

usuário já autenticado na rede, onde o mesmo é capaz de realizar a captura dos dados trafegados na rede. Essa vulnerabilidade foi chamada de *Hole 196* (Buraco 196), que tem esse nome pelo fato de ter sido encontrada na página 196 do padrão IEEE 802.11.

3.1 RISCOS E AMEAÇAS À REDE SEM FIO

Manter a segurança de uma rede sem fio tem sido um grande desafio desde o seu surgimento. Como o meio de transmissão é o ar, fica fácil de um sinal wireless ser interceptado, e uma vez interceptado, pode trazer grandes riscos à segurança dessa rede e de grandes consequências.

As redes sem fio são vítimas de muitos ataques realizados de diversas formas, tornando não seguro o tráfego de informações em uma rede wireless, uma vez que quando a rede é vítima de acessos indevidos, se torna sujeita à leitura e alteração dos dados trafegados na rede, o que é uma grande ameaça a quem utiliza essa rede.

Os ataques às redes wireless miram nas fraquezas presentes nas mesmas, nas falhas de segurança que podem apresentar. Essa vulnerabilidade proporciona às pessoas mal-intencionadas a invasão e a realização de algum dano a quem utiliza a rede, como roubo de informações, adulteração de dados, e até mesmo, em alguns casos, a destruição de algo que pode comprometer e inutilizar todo um sistema. Tornando assim o utilizador da rede passível de crimes como espionagem industrial, furto em transações bancárias, exposição de informações e conteúdos pessoais (calúnia, difamação e pornografia), entre outros (AGUIAR, 2009).

Assim, fica a necessidade de uma maior garantia na segurança dessas redes por parte dos administradores das mesmas, seja em uma residência ou em uma empresa. É importante também saber que não é uma ferramenta ou tecnologia que protege da melhor forma a rede, devem ser aplicadas mais de uma solução para a melhoria da segurança.

Segundo Rufino (2011), entre os riscos e ameaças à segurança das redes sem fio mais presentes, podem ser citados: segurança física, envio e recepção de sinal, interceptação de sinal, mapeamento do ambiente, captura de tráfego, DoS (*Denial of Service*), configurações de fábrica e vulnerabilidade dos protocolos WEP e WPA.A segurança física está relacionada à segurança quanto à área de abrangência do sinal da rede sem fio, uma vez que o sinal pode alcançar lugares que ultrapassam os limites desejáveis. Sendo assim, é importante ser feito um estudo da área que o sinal pode alcançar que depende do padrão utilizado, da potência de transmissão do AP e também do seu posicionamento (ALBUQUERQUE, 2008). E o posicionamento do AP afeta diretamente na área de envio do sinal, uma vez que ele é o ponto central da transmissão. Assim, é importante posicionar ele de maneira que proporcione um bom desempenho para o cliente levando em conta que a área de abrangência do sinal não deve ultrapassar os limites de utilização do usuário, para evitar que algum intruso receba o sinal e tente invadir a rede (ALBUQUERQUE, 2008).

Além disso, a interceptação do sinal é um grande problema para as redes sem fio, já que o meio de transmissão não é um meio guiado e pode ser facilmente sintonizado, uma vez que não é possível controlar quem recebe o sinal. Essa interceptação pode ocorrer próximo do aparelho concentrador (AP) ou mesmo realizada a uma grande distância com o uso de equipamentos implementados para melhor captação do sinal do AP. A partir da interceptação, pode ser realizada uma série de ataques à rede (RUFINO, 2011). Já o mapeamento do ambiente é uma ação realizada para identificar as redes sem fio, tentando assim, obter o maior número possível de informações sobre as redes identificadas, para que um ataque seja bem-sucedido e que o intruso não seja detectado. Pode ser considerado o primeiro procedimento para alguém que vai invadir uma rede (ALBUQUERQUE, 2008).

A captura de tráfego se realiza a partir da interceptação do sinal, sem a necessidade de associação à rede, onde, por meio de alguma ferramenta para captura de tráfego, o tráfego de informações de um AP pode ser capturado e copiado. Em uma situação em que não exista segurança nos dados trafegados, é possível obter as informações dos conteúdos trafegados na rede (RUFINO, 2011).

O DoS é uma ameaça que afeta os serviços utilizados na rede, fazendo que eles se tornem indisponíveis. Pode ser feito a partir de um equipamento gerador de frequências na mesma faixa de utilização do AP da rede sem fio, causando assim uma interferência no sinal, ou a partir de uma técnica que sobrecarrega o sistema tornando os recursos indisponíveis para o usuário (RUFINO, 2011).

As configurações de fábrica são um problema que ameaçam a segurança se não forem configuradas pelos administradores da rede. Os equipamentos para as redes wireless vêm de fábrica com mecanismos de seguranças implementados, visto o risco que é uma rede sem segurança, porém eles vêm com configurações padrões, ou seja, podem ser vítimas de ataques facilmente por quem conhece os padrões daquele fabricante (RUFINO, 2011).

O protocolo WEP foi condenado como inseguro após a quebra de seu algoritmo. Ele possui três pontos conhecidos de vulnerabilidade, o compartilhamento de chave, o uso do algoritmo RC4 e o vetor de inicialização (IV). O compartilhamento de chave consiste na distribuição de chaves para os dispositivos que queiram se comunicar, onde devem deter o conhecimento dessa chave. Essa situação se torna inviável em redes de grande porte dada a necessidade de todos os dispositivos conhecerem a chave, o que torna o segredo da chave menos seguro, e dificulta a administração da rede. O algoritmo RC4 ao realizar uma técnica de equivalência numérica, permite que a informação do tamanho da mensagem original seja descoberta, já que a informação gerada no processamento dessa técnica possui o mesmo número de bytes que a original.

O IV utilizado no protocolo WEP tem tamanho de 24 *bits*, que é associado à chave desse padrão, que tem o tamanho padrão de 64 *bits* ou 128 *bits*, onde somente 40 *bits* ou 104 *bits* representam a chave, e os outros 24 *bits* representam o IV. Devido ao tamanho

reduzido desse IV, ele se repete várias vezes durante um dia, o que permite a descoberta do IV e a identificação da chave WEP (ALBUQUERQUE, 2008).

O protocolo WPA é considerado mais seguro que o protocolo WEP, já que não tem as mesmas vulnerabilidades. E possui dificuldade maior para ter sua chave quebrada. Mas esse protocolo também tem vulnerabilidades, isto é, está sujeito a ataques de força bruta, onde através de tentativas de diversas senhas, um atacante pode descobrir a chave WPA. No entanto, esses ataques somente são viáveis para chaves com menos de 20 caracteres (RUFINO, 2011).

Outra vulnerabilidade encontrada nesse tipo de protocolo é o ataque de força bruta realizado no WPS (Wi-Fi *Protected Setup*) PIN, que é uma facilidade de configuração para a rede sem fio desenvolvida pela *Wi-Fi Alliance*. Consiste em descobrir o PIN por força bruta, aonde é possível a descoberta da chave WPA. Entretanto, atualmente, muitos fabricantes já desenvolveram métodos para dificultar e até mesmo impossibilitar esse tipo de ataque, que vai desde a desativação dessa configuração WPS, ao desenvolvimento de defesas aos ataques de força bruta. Esse método pode ser realizado tanto para o protocolo de segurança WPA como para o WPA2 (REAVER SYSTEM, 2014).

Dada as vulnerabilidades das redes sem fio, é preciso no mínimo garantir segurança às informações trafegadas na rede, para que a privacidade e a integridade dos dados sejam mantidas. Neste trabalho será tratada uma forma de prevenir o acesso às informações trafegadas na rede, e acesso ao seu conteúdo, por meio da criação de uma VPN através do software livre OpenVPN.

3.2 IMPLEMENTAÇÃO DE REDES VPN

A VPN é uma rede de comunicação privada virtual, como o próprio nome sugere, criada entre dois pontos, entre redes corporativas e usuários remotos, para que haja segurança na transferência de dados entre esses pontos. Tem algumas das vantagens de um link dedicado e mesma aparência, podendo substituí-lo onde o alto custo para a aplicação do link se torne inviável, porém levando algumas desvantagens, por exemplo, na segurança e no desempenho (CYSCO SYSTEMS, 2004).

Além disso, é uma rede virtual criada no ambiente de uma rede pública, por exemplo, a Internet, com tecnologias de criptografia por tunelamento, onde o tráfego de dados é feito por uma rota dessa rede, criando um túnel privado simulando uma conexão do tipo ponto-a-ponto, com a utilização de protocolos que garantam a confidencialidade, a autenticidade e a integridade dos dados (CYSCO SYSTEMS, 2014). Não são todas as VPNs que são seguras e garantem de fato a privacidade do usuário, existindo assim a necessidade de saber quais os protocolos utilizados pela VPN e saber se a ferramenta a ser utilizada para a sua criação é de confiança.

As VPNs oferecem recursos de autenticação, criptografia e também integridade,

sendo uma alternativa econômica e segura para a transmissão de dados entre redes, podendo até tornar seguro o tráfego de informações em redes inseguras. Sistemas de comunicação por VPN têm sido frequentemente encontrados em redes empresariais por sua boa relação de custo/benefício e facilidade de implantação (BORGES; CUNHA; FAGUNDES, 2008).

A autenticação pode ser oferecida por uma verificação de credenciais, *login* e *password*, requisitada para os usuários da rede, para garantir que pessoas não autorizadas não tenham acesso e não possam trocar informações na rede privada. Essa autenticação geralmente é feita a partir de certificados digitais ou chaves públicas. A criptografia é feita para tornar o dado trafegado ilegível para uma situação na qual essa informação seja interceptada em seu trajeto. Para a integridade, é realizada uma autenticação dos dados que verifica a integridade de cada pacote de dados e a origem dos mesmos, caso não seja proveniente de um usuário autorizado (AMORAS; BRABO; PEREIRA, 2004).

Para as redes VPNs podem ser utilizados os protocolos IPSec (IP *Security Protocol*), PPTP (*Point-to-Point Tunneling Protocol*), L2TP (*Layer 2 Tunneling Protocol*), SSL (*Secure Socket Layer*), entre outros (BORGES; CUNHA; FAGUNDES, 2008).

OpenVPN, como o próprio nome diz, é um software livre, Open Source, licenciado pela GPL (*Gerneral Public Licence*), que realiza a criação de VPNs para proporcionar segurança na transmissão de dados via redes públicas. Foi desenvolvido por James Yonan e é disponibilizado para diversos sistemas operacionais, como o Linux, Solaris, Mac OS X, OpenBSD, Microsoft Windows 2000/XP/Vista/7, entre outros.

O software foi baseado no protocolo SSL, implementando soluções de segurança por tunelamento nas camadas OSI 5 ou 6, tendo como ferramenta de recursos de criptografia e autenticação a biblioteca OpenSSL. Permite autenticação por diferentes modos, por credenciais, certificados digitais, chaves secretas compartilhadas, juntamente com suporte a *smart cards*. Consegue transmitir sobre UDP ou TCP, multiplexando toda comunicação em uma única porta TCP/UDP. Estabelece túneis criptografados com a capacidade de estabelecer conexões atrás de NAT (*Network Address Translation*) sem que seja necessária reconfiguração, sendo capaz de criar uma interface virtual para cada VPN baseada na interface genérica TUN/TAP (*Network Tunnel/Tap*), que cria túneis para carregar qualquer tipo de tráfego Ethernet (IP). O OpenVPN não é uma aplicação web e não possui compatibilidade com os protocolos IPSec, L2TP, PPTP. Possui como vantagens a fácil e simples instalação, configuração e utilização, facilidade na depuração de problemas de rede, a configuração de VPNs para IP fixos e dinâmicos, a compatibilidade com NAT, X.509 PKI, SSL/TLS, certificados RSA, entre outras (OPENVPN TECHNOLIGES, 2014).

Esse protocolo tem como versão mais atual a SSL 3.0 e é tido como antecessor do protocolo TLS (*Transport Layer Security*) padronizado pelo IETF (*Internet Engineering Task Force*), possuem pequenas diferenças, mas que os tornam não interoperacionais. São pronunciados como protocolos semelhantes também denominados de SSL/TLS.

O protocolo SSL utiliza o método de criptografia de chave pública, estabelecendo um canal de comunicação protegido entre o cliente e o servidor, garantindo a segurança e a privacidade dos dados transmitidos na Internet através de autenticação e criptografia (OPPLIGER, 2009). É um método de proteção transparente que estabelece uma sessão segura para os protocolos de aplicação HTTP, POP, SMTP, entre outros. Um exemplo de um servidor web protegido pode ser verificado com a presença do "s" no protocolo de aplicação como em "*https://*", demonstrando que é certificado pelo protocolo SSL.

O SSL utiliza subprotocolos para estabelecer e iniciar uma conexão segura, podendo ser dividido em *Record Layer Protocol*, *Change Cipher Spec Protocol*, *Alert Protocol*, e *Handshake Protocol*. O *Change Cipher Spec Protocol* é composto de uma mensagem que sinaliza o início de comunicações cliente/servidor, seguras e sinaliza possíveis alterações quanto à utilização da criptografia, caso seja necessária sua mudança. O *Alert Protocol* envia mensagens de erros, problemas ou alertas, a respeito da conexão entre cliente e servidor, mensagens estas que especificam o erro ou problema existente e, podem ou não, solicitar ou realizar, a desconexão entre as partes.

O *Handshake Protocol* é responsável pela autenticação cliente/servidor, sendo dividida em duas fases, uma fase para a escolha da chave a ser utilizada entre o cliente e o servidor, para a autenticação do servidor e a troca de chaves pré-mestre, e a outra fase, a qual é optativa, para a autenticação do cliente. No *handshake* é estabelecido uma séria de parâmetros para o protocolo *Record Layer Protocol* e utilizado um código MAC (*Message Authentication Code*) nas trocas de mensagem para maior segurança. E o funcionamento do *Handshake Protocol* é dividido em nove mensagens, *Client Hello, Server Hello*, *Server Key Exchange*, *Server Hello Done*, *Client Key Exchange*, *Change Cipher Spec*, *Finished*, *Change Cipher Spec* e *Finished* (STALLINGS, 2012).

4 | RESULTADOS E DISCUSSÕES

O procedimento inicial para a análise das falhas dos protocolos de segurança das redes Wi-Fi, foi realizado a partir da análise da região, com a ferramenta *inSSIDer*. Primeiramente foi necessário estar com o notebook na interface wireless ativada para executar o *inSSIDer*. Este software é capaz de realizar varreduras no espectro de frequência utilizado pela interface wireless do dispositivo, sendo capaz de gerar gráficos e algumas informações úteis para a análise das redes no alcance da placa wireless. Segue um exemplo de monitoração feita através do *inSSIDer*, conforme Figura 3.

SSID	SIGNAL ▼	CHANNEL	SECURITY	MAC ADDRESS	802.11	VENDOR
Wi-Fi	-35	1	WPA-Personal	5C:D9:98:75:46:D4	g	D-Link Corporation
Milena Reis	-85	11+7	WPA-Personal	00:1A:3F:A9:08:40	n	intelbras
MANTOVANI	-93	6+10	WEP	00:26:5A:1F:7F:36	n	D-Link Corporation
TP-LINK_CA2BEA	-93	6	WPA-Personal	00:27:19:CA:2B:EA	g	TP-LINK TECHNOLOGIES CO.,
WI-FI	-93	11+7	WPA-Personal	00:0A:EB:46:F6:80	n	Shenzhen Tp-Link Technology

Figura 3: Aproximação da Tela de Varredura do InSSIDer. Fonte: Elaboração Própria, 2014/2024.

Dentre as informações fornecidas pelo *inSSIDer*, as mais importantes e de maior interesse para a análise neste estudo são: SSID (*Service Set IDentifier*), *Signal* (Nível de Sinal), *Channel* (Canal do AP), *Security* (Protocolo de Segurança), MAC *Address* (Endereço MAC do AP), 802.11 (Padrão WLAN), *Vendor* (Fabricante do AP).

Com essas informações em mãos, já é possível ir para o próximo passo, que é realizar, por meio do software *aircrack-ng*, a quebra das redes que possuem o protocolo WEP. Com essa ferramenta também é possível realizar a análise da região, com a diferença de não tem na informação o tipo de fabricante. A Figura 3, é um exemplo de monitoramento através do *aircrack-ng*, conforme Figura 4.

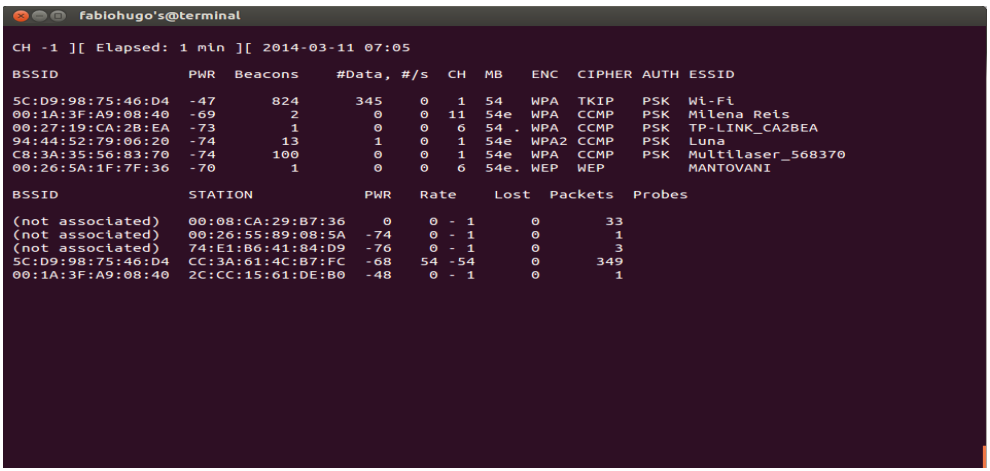


Figura 4: Tela de Captura do Aircrack-ng. Fonte: Elaboração Própria, 2014/2024.

O funcionamento do *aircrack-ng* se baseia em dois métodos, um deles parte da captura de pacotes na rede, para poder utilizar esses dados no outro método, o outro realiza ataques estatísticos e de força bruta para tentar descobrir a chave WEP, isso baseado na vulnerabilidade desse protocolo no que relaciona os vetores de inicialização.

O tempo médio para quebrar a senha da criptografia WEP 64 *bits* foi de aproximadamente 15 minutos e o tempo para a criptografia WEP 128 *bits* foi de um pouco mais, 25 minutos. Esse tempo varia de acordo com a dificuldade e tamanho da chave utilizada nas redes, mas que não chega a alcançar muito tempo, dada a facilidade de quebrar a chave de uma criptografia WEP, por ter um tamanho limite de chave pequeno, e pela capacidade do software *aircrack-ng* de fazer os cálculos com velocidade de processamento, alta.

E o procedimento realizado na plataforma Linux com a utilização do *aircrack-ng*: Identificação das redes no alcance da cobertura da placa wireless do notebook utilizado. Para esse procedimento é necessário primeiro que a placa wireless seja coloca em modo promiscuo, ou seja, em um modo de monitoração. Para isso, utiliza-se o comando no

terminal do sistema: airmon-ng start (interface de rede padrão wireless – ex: wlan0). Esse modo de monitoramento, também pode ser alcançado realizando os seguintes comandos: ifconfig (interface de rede wireless - ex: wlan0) down; iwconfig (interface de rede wireless - ex: wlan0) mode monitor; ifconfig (interface de rede wireless - ex: wlan0) up. A partir do momento em que a placa está em modo monitor, a identificação das redes pode ser feita com o comando: airodump-ng (interface de rede wireless modo monitor - ex: wlan0/mon0) e Captura de pacotes.

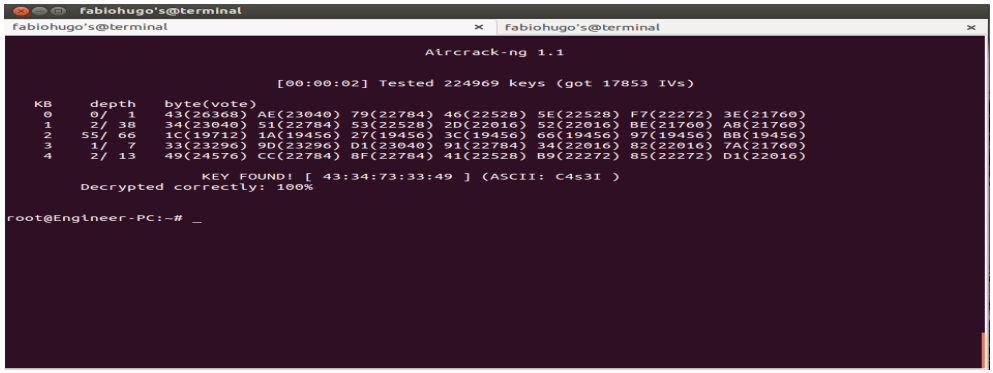


Figura 5: Aircrack-ng Chave WEP 64 Bits. Fonte: Elaboração Própria, 2014/2024.

E para realizar a captura dos pacotes é necessária a utilização do comando utilizado para a identificação, mas que agora será configurado para fazer captura de dados: airodump-ng -w (nome do arquivo) --bssid (MAC do AP a ser atacado) --ivs (interface de rede wireless). O w significa *write*, que será o comando para salvar o arquivo de texto; bssid é o endereço MAC do AP monitorado; e ivs indica que serão salvos somente dados dos IVs. O processo de quebra da senha é o último procedimento, onde será utilizado o comando *aircrack-ng* associado ao arquivo salvo na captura de pacotes, para que com os pacotes salvos, o software seja capaz de descobrir a senha WEP, isto é, ircrack-ng (arquivo salvo). ivs. Deste modo, dado o tempo necessário para a captura de pacotes na rede, o *aircrack-ng* será capaz de quebrar a chave. Vale lembrar que o *aircrack-ng* depende da captura de pacotes da rede e que esta depende do tráfego da rede, então o seu tempo varia conforme o grau de utilização da rede. Segue a figura com um exemplo de senha WEP 64 bits quebrada, conforme Figura 5.

As informações que constam na Figura 5, significam: Aircrack-ng 1.1 – Versão utilizado; [00:00:02] – Tempo gasto para quebra da chave; Tested 224969 keys – Número de chaves testadas; (got 17853 IVs) – Número de vetores de inicialização capturados; (KB) – Byte da chave; (depth) –A quantidade de vezes que foram necessários as repetições naquele byte; (byte) – Bytes que vazaram dos IVs; Vote – Votos indicando que o byte está correto; KEY FOUND! – Informação da chave; [43:34:73:33:49] - Informação da chave em hexadecimal; (ASCII: C4s3I) – Informação da chave em ASCII e Decrypted correctly: -

Porcentagem de sucesso.

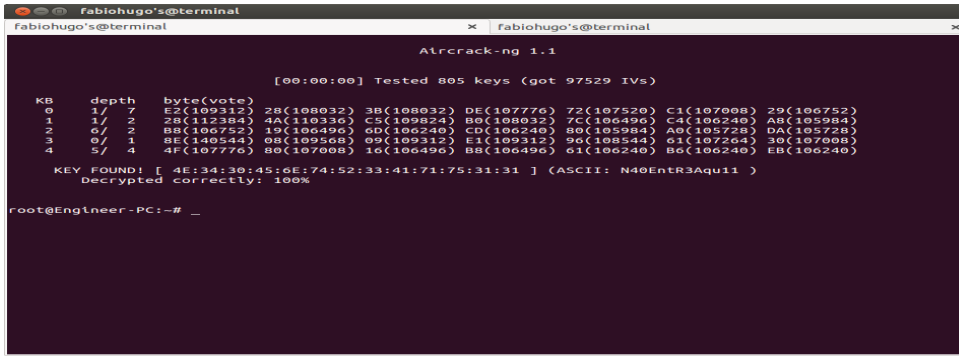


Figura 6: Aircrack-ng Chave WEP 128 Bits. Fonte: Elaboração Própria, 2014/2024.

A quantidade de pacotes necessários para a quebra da senha varia de acordo com a dificuldade da mesma. Para o protocolo WEP de 128 *bits* a quantidade de pacotes necessários aumenta bastante. Segue a Figura 6, como exemplo de senha WEP 128 *bits* quebrada. A primeira parte do estudo foi realizada com sucesso, onde foi testada e comprovada a vulnerabilidade dos protocolos WEP. Ao obter acesso nessas redes, foi possível verificar todo o tráfego de dados, concluindo assim que os usuários daquelas redes estão vulneráveis a ataque e que precisam de uma solução de melhoria, podendo optar por implementar outro método de segurança além do WEP.

Dessa forma, baseado na necessidade de implementação de segurança, este estudo propõe um método de segurança baseado na criação de redes privadas virtuais. Para realizar a criação de uma VPN será utilizado o software OpenVPN, onde será necessária a utilização de um servidor capaz de prover acesso à rede. Primeiramente será montada uma topologia com um servidor, um host e um intruso, onde serão realizados testes para comparação dos resultados obtidos anteriormente sem a utilização do servidor.

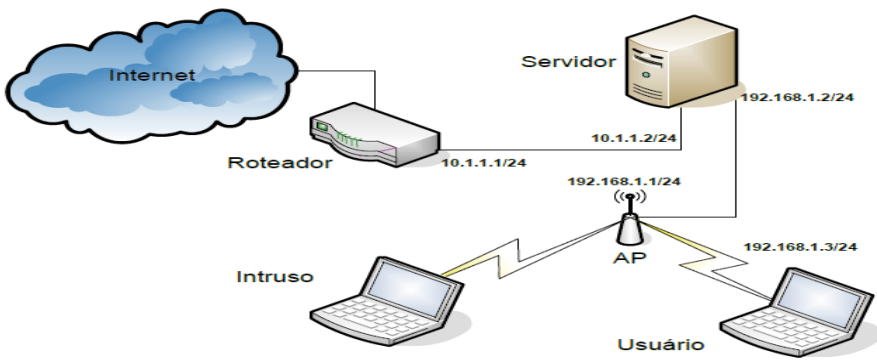


Figura 7: Ambiente de Teste. Fonte: Elaboração Própria, 2014/2024.

Para a realização dos testes foram utilizados os seguintes itens: Um intruso possuindo um notebook com interface de rede sem fio configurada em modo promíscuo; Um host com notebook com interface de rede sem fio configurada com o IP local 192.168.1.3; Um AP, configurado com o IP local 192.168.1.1. Um servidor com duas interfaces configuradas como: Interface de rede sem fio com o IP local 192.168.1.2; interface de rede LAN com o IP 10.1.1.2 - Internet; Um roteador configurado com o IP 10.1.1.1.

É necessária uma série de passos para a realização da configuração, segue um passo a passo, a começar pela instalação do software a ser utilizado: Instalando o sistema OpenVPN no servidor: # apt-get install openvpn; Criando certificados e chaves: Copiando os scripts do OpenVPN: (# cp -r /usr/share/doc/openvpn/examples/easy-rsa/2.0/. /etc/openvpn/); Acessando o diretório copiado: (# cd /etc/openvpn/easy-rsa/); Carregando as informações de configuração: (# source ./vars); Limpando todas as variáveis existentes: (# source ./clean-all); Criando uma autoridade certificadora: (# ./build-ca); A execução do comando resultará na criação dos arquivos: ca.crt - Certificado público da CA, ca.key - Certificado privado da CA, Serial - Controle do número serial das chaves geradas pela CA, index.txt - Controle das chaves geradas pela CA. (a) Criando o certificado e a chave do servidor: # ./build-key-server sever (nome do servidor), A execução do comando resultará na criação dos arquivos: server.crt - Certificado público do servidor, server.key - Certificado privado do servidor, Criando o certificado e a chave do cliente: # ./build-key client1 (nome do cliente). A execução do comando resultará na criação dos arquivos: client1.crt - Certificado público do cliente, client1.key - Certificado privado do cliente, Gerando os parâmetros necessários do Diffie Hellman. # ./build-dh.

A execução do comando resultará na criação dos arquivos: dh1024.pem - Arquivo que proporcionará a troca de informação entre o servidor e o cliente em um ambiente não seguro, sem comprometer a segurança. Além disso, configurando o OpenVPN Server: (a) Criar o arquivo de configuração do OpenVPN e de log, isto é, # touch /etc/openvpn/server.conf, # touch /var/log/openvpn.log e (b) Editar o arquivo inserindo as seguintes linhas de configurações: # vim /etc/openvpn/server.conf, server.conf, dev tun, tls-server, proto udp, ca /etc/openvpn/easy-rsa/keys/ca.crt, cert /etc/openvpn/easy-rsa/keys/server.crt, key /etc/openvpn/easy-rsa/keys/server.key, dh /etc/openvpn/easy-rsa/keys/dh1024.pem, ifconfig 192.168.11.1 255.255.255.0, ifconfig-pool 192.168.11.2 192.168.11.254 255.255.255.0, comp-lzo, persist-tun, persist-key, float, verb 3, log /var/log/openvpn.log. Onde: dev tup - Dispositivo virtual utilizado para vpn; tls-server - Permitir o uso de conexões SSL/TLS tipo servidor; proto udp – Utilização do protocolo UDP para transporte dos dados; ca - Certificado público da CA; cert - Certificado público do servidor; key - Certificado privado do servidor; dh - Diffie Hellman; ifconfig - IP utilizado no túnel da VPN; ifconfig-pool - Pools de ip reservados para os clientes; comp-lzo - Habilita a compressão dos dados; persist-tun - Mantém a interface tun configurada mesmo após um reset na aplicação OpenVPN; persist-key - Mantem a chave carregada mesmo após um reset na aplicação OpenVPN;

float - Caso ocorra alteração no IP o túnel permanecerá estabelecido; verb 3 - Nível de detalhes das conexões; log - Arquivo de log.

E configurando o OpenVPN client: (a) Para que seja possível a comunicação e configuração do OpenVPN client, é necessário que sejam copiados de modo seguro do servidor os arquivos: ca.crt, client1.crt, client1.key, dh1024.pem. Para criar o arquivo de configuração do OpenVPN client. E dentro do diretório c:/Arquivos de Programas/OpenVPN/config/, Inserir os arquivos de configuração copiados do servidor e criar um novo arquivo com o nome: client1.ovpn, dev tap, tls-client, proto udp, remote 10.1.1.2, ca ca.crt, cert client1.crt, key client1.key, dh dh1024.pem, comp-lzo, persist-tun, persist-key, float e verb 3. Onde: dev tap - Dispositivo virtual criado no Windows; tls-client - Permitir o uso de conexões SSL/TLS tipo cliente e remote - IP remoto do servidor.

Para criar a rota no servidor, temos que (a) Criar a rota de entrada via VPN para saída internet: # iptables -t nat -A POSTROUTING -s 192.168.11.0 -o wlan0 -j MASQUERADE; # echo “1” > /proc/sys/net/ipv4/ip_forward. Onde: iptables - Aplicação utilizada no linux 2.4.x, baseado em regras para realização de filtro dos pacotes trafegados pela rede; echo “1” > /proc/sys/net/ipv4/ip_forward - Comando utilizado para ativar o encaminhamento dos pacotes de uma interface para outra, conforme Figura 8.

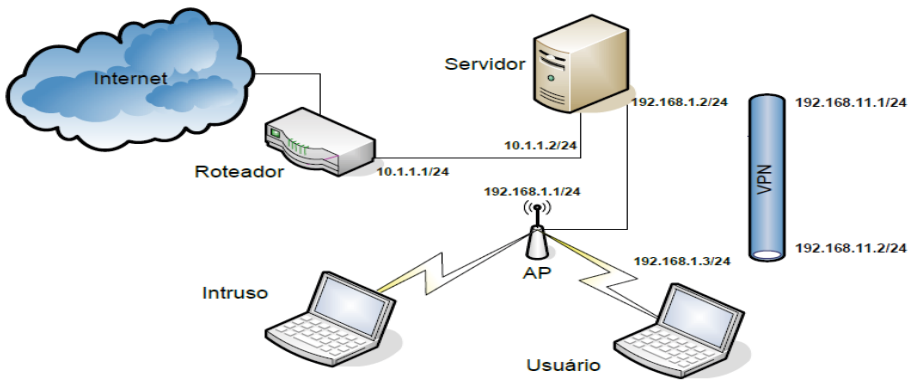


Figura 8: Ambiente de Teste com VPN – OpenVPN. Fonte: Elaboração Própria, 2014/2024.

E para iniciar o OpenVPN server + client. Iniciar o OpenVPN server no servidor: # /etc/init.d/openvpn restart; Iniciar o OpenVPN client no cliente: Acessar o diretório c:/Arquivos de Programa/OpenVPN/config/. E selecionar o arquivo client1.ovpn e executar: Start OpenVPN on This Config File. E acessar as configurações de rede padrão e inserir o gateway 192.168.11.1 (ip da vpn do servidor remoto), conforme mostrado na Figura 8.

E finalmente, depois de finalizar todo o processo de instalação e configuração do software OpenVPN, foram realizados testes onde foram utilizadas as mesmas ferramentas e os mesmos princípios para invadir a rede. O resultado da análise de tráfego realizada pela ferramenta *tcpdump* em uma rede WEP, onde antes era possível ler e capturar todo o

tráfego é mostrado na Figura 9.

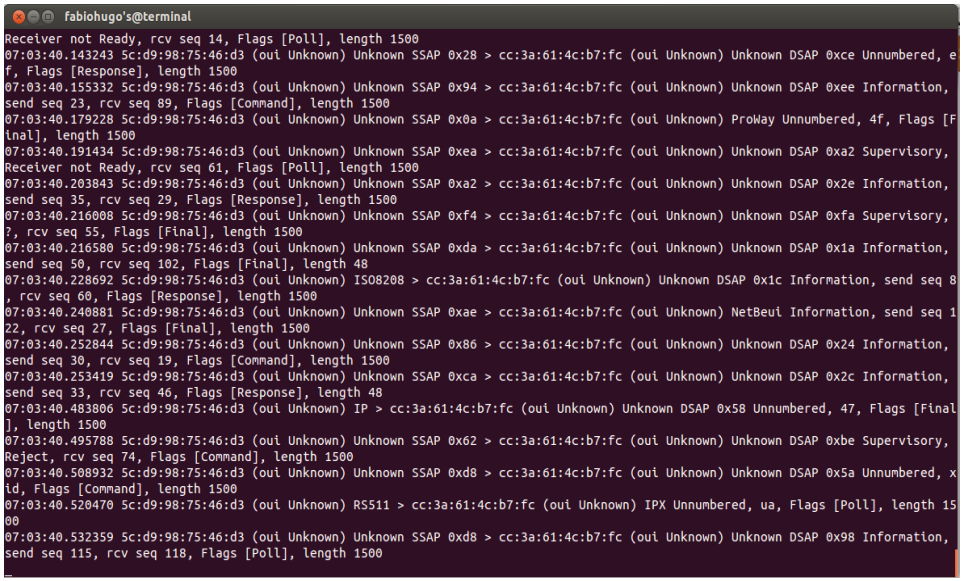


Figura 9: Tráfego na Rede Verificado com o Tcpdump. Fonte: Elaboração Própria, 2014/2024.

Nos testes acima, usou-se uma aplicação utilizado apenas um AP, dada a necessidade de teste com a presença do servidor, o que torna difícil a realização de testes com diferentes proprietários. Foi comprovado com os testes nas redes WEP que o sistema de VPN não é capaz de fornecer mais segurança quanto à quebra das chaves, porém em termos de privacidade as redes privadas virtuais alcançaram seu objetivo. Destarte, uma forma de identificar a privacidade são as aplicações *Unknown,* mostrando que não é possível localizar o tráfego trocado entre host/servidor.

Em 2021, por exemplo, 2 de cada 3 consumidores brasileiros, aproximadamente 68% afirmam ter adotado mais proteção em seus dispositivos e atividades online, o que representa um número bastante superior à média global, que é de 61%. Além disso, os brasileiros se conectam aos diversos tipos de redes, tais como: Wi-Fi público (48%), rede doméstica de amigos ou de casas alugadas (52%), Wi-Fi de carros (41%), redes hoteleiras (50%), Wi-Fi de aeroportos (47%) e smartTVs (42%) de acordo com CISOADVISOR (2023).

5 | CONSIDERAÇÕES FINAIS

De forma geral, com os avanços tecnológicos proporcionaram o desenvolvimento das redes sem fio, as quais rapidamente ganharam força no mercado e conquistaram os diversos utilizadores das redes com cabeamento, visto que proporcionam uma série de vantagens que as redes convencionais não podem oferecer, por exemplo, mobilidade, flexibilidade e abrangência, em que é possível o acesso à rede em locais de difícil acesso

físico. E com o desenvolvimento dessas redes, vários dispositivos incorporaram essa tecnologia, a qual tem crescido e se desenvolvido bastante, aprimorando sua capacidade e solucionando seus problemas, onde a segurança é o maior de seus problemas.

Dessa forma, os estudos realizados sobre os protocolos de segurança das redes sem fio, proporcionaram um melhor entendimento de como funcionam os diferentes métodos de criptografia utilizados para garantir o sigilo, a autenticidade e a integridade das informações trafegadas nessas redes. Com isso, foi possível entender os pontos de vulnerabilidade existentes nesses protocolos e entender também a necessidade de se desenvolver novos protocolos de segurança para eliminar as condições de riscos existentes nas redes Wi-Fi.

Nos testes, para o estudo de caso realizado, nos casos em que a segurança da rede possuía configuração padrão ou má configurada, foi possível observar que com pouco conhecimento de computação, uma pessoa poderia ser capaz de realizar a invasão da rede e, em algumas situações, conseguir fazer a captura de arquivos da rede. Nesse sentido, pode-se concluir que é indispensável à realização da configuração na segurança da rede diferente do padrão, melhor ajustada, e a utilização de outro método de segurança aplicado às redes Wi-Fi, além dos protocolos padrões oferecidos pela rede. E a solução utilizada, a criação de VPNs, não oferece maior segurança no acesso indevido à rede, porém teve resposta nos testes realizados para tentar obter algum tipo de informação na rede, demonstrando segurança adequada quanto à privacidade das informações trafegadas na rede. Porém, deve ser ressaltado, que não são todas as aplicações VPNs seguras, visto que esse método depende dos protocolos utilizados em sua implantação.

Portanto, nos testes, apesar das redes Wi-Fi apresentarem vulnerabilidades, não se pode dizer que essas redes são totalmente vulneráveis, uma vez que continuamente ocorrem avanços no desenvolvimento de soluções para cibersegurança. E por hipótese, uma pessoa com qualquer equipamento, não conseguiria realizar um ataque cibernético a rede, isto é, uma vez que a rede seja configurada de forma adequada em conformidade, pode proporcionar segurança adequada, restringindo a possibilidade de ataques cibernéticos às pessoas com alto grau de conhecimento em computação. Os vários relatos dos riscos e ameaças às redes Wi-Fi, fazem os engenheiro de redes e analisas de sistemas, dessas redes, disponibilizem maximização de atualizações e métodos, o que implica aumento da dificuldade para invadir uma rede. Daí, os sistemas e softwares para os ataques cibernéticos estão sendo desenvolvidos e aprimorados, constantemente. Além disso, a segurança das redes de forma ágil, desenvolvem soluções para mitigar os riscos e ameaças cibernéticas.

REFERÊNCIAS

AGUIAR, Daniel. **Estudo Sobre Crimes Praticados na Internet com o Uso do Computador**. 2009. 104 f. Trabalho de Conclusão de Curso (Tecnologia em Informática com Ênfase em Gestão de Negócio) – Faculdade de Tecnologia da Zona Leste, São Paulo. 2009.

AIRCRACK-NG. **Aircrack-ng Installation**. Disponível em: <http://www.aircrack-ng.org/install.html>. Acesso em: 25/01/2014.

ALBUQUERQUE, Alessandro. **Estudo de Métodos de Proteção de Redes Wireless**. 2008. 72 f. Trabalho de Conclusão de Curso (Pós-Graduação *Lato-Senso* em Redes de Computadores – Configuração e Gerenciamento de Ativos) – Universidade Tecnológica Federal do Paraná, Medianeira. 2008.

ALVES, Francinildo, et al. **Análise de Vulnerabilidades em Redes sem Fio**. 2010. 57 f. Trabalho de Conclusão de Curso – Faculdade Integrada do Ceará (Curso Tecnólogo em Rede de Computadores), Fortaleza. 2010.

ALVES, Nilton; BRAGA, Nilton; CARNEIRO, Leonardo. **Rede de Computadores**. 1998. 47 f. Nota Técnica.

AMORAS, Romulo; BRABO, Gustavo; PEREIRA, Carlos. **Segurança em Redes Wireless Padrão IEEE802.11b: Protocolos WEP, WPA e Análise de Desempenho**. 2004. 78f. Trabalho de Conclusão de Curso – Universidade da Amazônia UNAMA (Curso Ciência da Computação), Belém. 2004.

AMORIM, Fábio. **Implantação de Redes Wireless para Melhoria do Controle e Monitoramento de Automação Industrial.** 2011. 63 f. Trabalho de Conclusão de Curso (Curso de Tecnologia em Redes de Computadores) – Faculdade de Tecnologia de São José dos Campos FATEC, São José dos Campos, 2011.

BEZERRA, Dinarde; SOUSA, Gustavo. **Protocolos Criptográficos**. 2008. 74 f. Trabalho de Conclusão de Curso – Faculdade de Tecnologia Termomanica (Curso de Tecnologia em Análise e Desenvolvimento de Sistemas), São Bernardo do Campo. 2008.

BORGES, Fábio; CUNHA, Gerson; FAGUNDES, Bruno. **VPN: Protocolos e Segurança**. S/D. 10 f. Artigo Científico – Universidade Católica de Petrópolis, Rio de Janeiro. S/D.

BORTOLUZZI, Dayna; CUNHA, Erivelto; SPECIALSKI, Elizabeth. **An Extended Model for TCPIP Architecture**. 2004. 5 f. Artigo Científico – Universidade Federal de Santa Catarina, Santa Catarina. 2004.

BROWN, Edwin. **802.1X Port-Based Authentication**. Nova York. Auerbach publications, 2007.

CERT.BR. **Estatística de Incidentes Reportados ao Cert.br**. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em 10/12/2013.

CISOADVISOR. Brasileiro vê redes Wi-Fi como mais vulneráveis a ameaças. Disponível em: https://www.cisoadvisor.com.br/brasileiro-ve-redes-wi-fi-como-mais-vulneraveis-ameacas/. 2021. Acesso em dezembro de 2023.

CISOADVISOR. Rússia hackeia Wi-Fi nos EUA via Internet. Disponível em: https://www.cisoadvisor.com.br/russia-hackeia-wi-fi-nos-eua-via-internet/. Acesso em outubro de 2024.

CYSCO SYSTEMS. **Internetworking Technologies Handbook**, Cisco Press , 2004.

CYSCO SYSTEMS, INC. **VPN**. Disponível em: <http://www.cisco.com/web/BR/solucoes/pt_br/vpn/index.html>. Acesso em: 02/2014.

GOMES, Luís. **Fundamentos de Rede**. 2007. 85 f. Trabalho Acadêmico – Escola Agrotécnica Federal de São João Evangelista (Curso Técnico em Informática), São João Evangelista. 2004.

IEEE COMPUTER SOCIETY. **Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications**. Disponível em: <http://standards.ieee.org/getieee802/download/802.11-2012.pdf>. Acesso em: 12/01/2014. ISBN 978-0-7381-7245-3 STDPD97218.

JARA, Diego; AUGUSTO, Felipe. **Segurança em Redes Sem Fio.** 2011. 12 f. Artigo Científico – Universidade Nove de Julho, São Paulo, 2011.

KARNIK, Ankush; PASSERINI, Katia. **Wireless Network Security - A Discussion From a Business Perspective.** 2005. 7 f. Artigo Científico.

LINUX, UBUNTU. **Ubuntu 13.10 Saucy Salamander**. Disponível em: <http://www.ubuntu.com/download/desktop>. Acesso em: 11/2013.

MARX, Tiago. **Do Projeto à Implantação de Redes Sem Fio.** 2008. 50 f. Trabalho de Conclusão de Curso (Curso Sistemas de Informação) – Universidade do Oeste de Santa Catarina, São Miguel do Oeste, 2008.

MENDES, Douglas. **Redes de Computadores: Teoria e Prática**. São Paulo: Novatec, 2007.

METAGEEK LLC. **inSSIDer Home.** Disponível em: <http://www.metageek.net/products/inssider/>. Acesso em: 01/2014.

MIRANDA, Anibal. **Introdução às Redes de Computadores**. Vitória: ESAB, 2008.

MORAES, Alexandre Fernandes De. **Redes Sem Fio**. São Paulo: Erica, 2011.

OPENVPN TECHNOLIGES, INC. **OpenVPN Community Software**. Disponível em: <http://openvpn.net/index.php/open-source/overview.html/>. Acesso em: 01/2014.

OPPLIGER, Rolf. **SSL and TLS: Theory and Practice**. Norwood: Artech House, 2009.

RAMASWAMY, Raju. **A Security Architecture and Mechanism for Data Confidentiality in TCP/IP Protocols**. 1990. 11 f. Artigo Científico – University of Missouri, Kansas City, 1990.

RANJINI, T; YAMUNA, R. **Wireless Technology**. 2011. 4 f. Artigo Científico – Kongu Engineering College, Coimbatore, 2011.

REAVER SYSTEM SOLUTIONS. **WiFi Protected Setup**. Disponível em: <http://www.reaversystems.com/>. Acesso em: 02/2014.

RED LINE SOFTWARE. **Example of VPN Tunnel Configuration**. Disponível em: <http://www.redline-software.com/eng/support/docs/winroute/ch12s05.php>. Acesso em 09/01/2014.

RUFINO, Nelson Murilo De Oliveira. **Segurança em Redes Sem Fio**. São Paulo: NOVATEC, 2011.

STALLINGS, William. **Criptografia e Segurança de Redes**. São Paulo: Pearson, 2012.

STALLINGS, William. **IEEE 802.11: Moving Closer to Practical Wireless LANs**. 2001. 7 f. Artigo Científico. 2001.

TANENBAUM Andrew S. **Redes de Computadores**, Elsevier, 2003 – 4. Edição.

TCPDUMP & LIBPCAP. **Tcpdump Home**. Disponível em: <http://www.tcpdump.org/>. Acesso em 20/01/2014.

TELECO. **Redes WLAN de Alta Velocidade I: Características**. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialredeswlanI/default.asp>. Acesso em 11/2013.

TRINTA, MACEDO. **Um Estudo Sobre Criptografia e Assinatura Digital**. Disponível em: <http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm>. Acesso em 26/12/2013.

VISIO, MICROSOFT CORP. **Microsoft Visio Professional 2013**. Disponível em: <http://office.microsoft.com/en-us/visio/>. Acesso em: 02/2014.

VIVA O LINUX. **VPN em Linux com OpenVPN**. Disponível em: <http://www.vivaolinux.com.br/artigo/VPN-em-Linux-com-OpenVPN/>. Acesso em: 01/2014.

WI-FI ALLIANCE. **Wi-Fi**. Disponível em: <http://www.wi-fi.org/>. Acesso em: 01/2014.

WINDOWS 7, MICROSOFT CORP. **Windows 7 Home Premium**. Product Key: TC469 – PPBGY – 893DB – QDC6Q – 8C9Y7.

WINDOWS 8, MICROSOFT CORP. **Microsoft Windows 8**. Product ID: 00179 – 40493 – 83959 – AAOEM.

WORD, MICROSOFT CORP. **Microsoft Word 2013**. Disponível em: <http://office.microsoft.com/en-us/word/>. Acesso em: 10/2013.

ZHENG, Pei. et al. Wireless Networking Complete. Burlington. Morgan Kaufmann, 2009.

ZIMMERMANN, Hubert. **OS1 Reference Model-The IS0 Model of Architecture for Open Systems Interconnection**. 1980. 8 f. Artigo Científico. 1980.

PROPUESTA DE UN INVERNADERO INTELIGENTE AEROPÓNICO

Data de submissão: 29/10/2024 *Data de aceite: 02/12/2024*

Beatriz Eugenia Silva y Rodríguez García
Instituto Internacional de Aguascalientes Tecnológico Nacional de México – Instituto Tecnológico de San Luis Potosí San Luis Potosí – San Luis Potosí
https://orcid.org/0000-0002-0905-932X

Jorge Norberto Mondragón Reyes
Instituto Internacional de Aguascalientes Tecnológico Nacional de México – Instituto Tecnológico de Aguascalientes Aguascalientes – Aguascalientes
http://orcid.org/0009-0006-2372-0942

Marco Antonio Hernández Vargas
Instituto Internacional de Aguascalientes Tecnológico Nacional de México – Instituto Tecnológico de Aguascalientes Aguascalientes – Aguascalientes
https://orcid.org/0000-0002-8146-9307

César Dunay Acevedo Arreola
Tecnológico Nacional de México, Instituto Tecnológico de Aguascalientes Instituto Internacional de Aguascalientes Aguascalientes – México
https://orcid.org/0009-0001-9370-2997

RESUMEN: Las tecnologías de Internet abarcan una amplia gama de herramientas y sistemas que permiten la comunicación, el intercambio de información y la conectividad global. La integración del Internet de las Cosas (IoT) y la Inteligencia Artificial (IA) en la agricultura han revolucionado la manera en que se gestionan los recursos y se optimizan las prácticas agrícolas. Mediante el uso de sensores conectados, sistemas de monitorización en tiempo real y análisis de datos avanzados, los agricultores pueden tomar decisiones informadas que mejoran la eficiencia y la sostenibilidad de sus cultivos. La IA permite predecir condiciones climáticas, detectar plagas y enfermedades de manera temprana y ajustar automáticamente el riego y la fertilización, lo que reduce el desperdicio de recursos y aumenta la productividad. En conjunto, estas tecnologías no solo mejoran la rentabilidad, sino que también contribuyen a la seguridad alimentaria y a la protección del medio ambiente. El objetivo de este proyecto de investigación es gestionar las diferentes variables físicas tales como temperatura, humedad y luminosidad que intervienen en un invernadero aeropónico mediante el uso de Internet de las Cosas y Lógica Difusa. Esta propuesta se ha implementado en un prototipo de invernadero de bajo costo dónde se ha

colocado un banco de sensores gestionado a través de la plataforma de automatización de código abierto Home Assistant (HA). El invernadero aeropónico se puede controlar de manera local (Computación en la Niebla) o desde cualquier lugar con una conexión a Internet vía VPN (Computación en la Nube). Con este tipo de propuesta se pretende acelerar el proceso de crecimiento de los productos agrícolas que se coloquen dentro del invernadero. La implementación de este proyecto será en dos fases. La primera fase consistirá en la construcción del invernadero aeropónico junto con el banco de sensores, el sistema central de procesamiento, conectividad del banco de sensores a la plataforma Home Assistant y la conectividad remota al invernadero. En la segunda fase, se implementará la lógica difusa para la gestión automática del banco de sensores y el control de la luz ultravioleta para la germinación de diferentes tipos de productos agrícolas. En esta propuesta se muestran los resultados de la primera fase del proyecto.
PALABRAS-CLAVE: Invernadero aeropónico, Internet de las Cosas, Inteligencia Artificial, Lógica Difusa, Sensor.

PROPOSAL FOR AN AEROPONIC SMART GREENHOUSE

ABSTRACT: Internet technologies encompass a wide range of tools and systems that enable communication, information sharing and global connectivity. The integration of the Internet of Things (IoT) and Artificial Intelligence (AI) in agriculture has revolutionized the way resources are managed, and farming practices are optimized. Using connected sensors, real-time monitoring systems and advanced data analytics, farmers can make informed decisions that improve the efficiency and sustainability of their crops. AI makes it possible to predict weather conditions, detect pests and diseases early, and automatically adjust irrigation and fertilization, which reduces resource waste and increases productivity. Together, these technologies not only improve profitability, but also contribute to food safety and environmental protection. The objective of this research project is to manage the different physical variables involved in an aeroponics using Internet of Things and Fuzzy Logic such as, temperature and humidity. This proposal has been implemented in a low-cost greenhouse prototype where a bank of sensors has been placed and managed through the open-source automation platform Home Assistant (HA). The aeroponic greenhouse can be controlled locally (Fog Computing) or from anywhere with an Internet connection via VPN (Cloud Computing). This type of proposal is intended to accelerate the growth process of the agricultural products placed inside the greenhouse. The implementation of this project will be in two phases. The first phase will consist of the construction of the aeroponic greenhouse together with the sensor bank, the central processing system, connectivity of the sensor bank to the Home Assistant platform, remote connectivity to the greenhouse and the implementation of fuzzy logic in the management of the sensor bank. In the second phase, the growth time of an agricultural product inside the aeroponic greenhouse will be compared with the growth of the same product outside the greenhouse. This proposal shows the results of the first phase of the project.
KEYWORDS: Aeroponic greenhouse, Internet of Things, Artificial Intelligence, Fuzzy Logic, Sensor.

1 | INTRODUCCION

La agronomía ha evolucionado significativamente en las últimas décadas debido a la necesidad creciente de soluciones sostenibles para la producción de alimentos, dado el aumento poblacional y el cambio climático. Los enfoques tradicionales de la agricultura se han complementado con innovaciones tecnológicas, como la agricultura de precisión, los sistemas de riego avanzados y la utilización de nuevas técnicas de cultivo, como la hidroponía y la aeroponía (FAO, 2021).

Una tendencia destacada es el uso de sensores, drones y el procesamiento masivo de datos para mejorar la eficiencia de los cultivos y reducir el uso de recursos naturales. Estas tecnologías permiten un monitoreo más detallado de las condiciones del suelo, el clima y la salud de las plantas, lo que maximiza el rendimiento y minimiza el impacto ambiental (Brady & Weil, 2019).

La agricultura vertical y los sistemas de cultivo sin suelo, como la aeroponía, están ganando terreno en regiones donde la disponibilidad de tierra y agua es limitada. La aeroponía, en particular, ha demostrado ser una técnica prometedora para el cultivo de una amplia variedad de plantas, especialmente en entornos controlados, como invernaderos o instalaciones urbanas. Este método optimiza el uso del agua y los nutrientes, lo que lo convierte en una opción altamente eficiente para el futuro de la agricultura sostenible (Bailey- Serres et al., 2019).

Figura 1. Bustanica, la granja vertical más grande del mundo (Fuente: www.xataka.com).

En México, la agronomía también ha experimentado avances importantes, impulsados por la necesidad de mejorar la productividad agrícola y enfrentar los desafíos climáticos y de recursos hídricos. La agricultura de precisión ha empezado a implementarse en varias regiones del país con las técnicas como la aeroponía, aunque en sus primeras fases de adopción, han despertado interés tanto en la academia como en empresas agrícolas que buscan mejorar la eficiencia del uso del agua (Sánchez-Lizarraga & Carrillo-López, 2020).

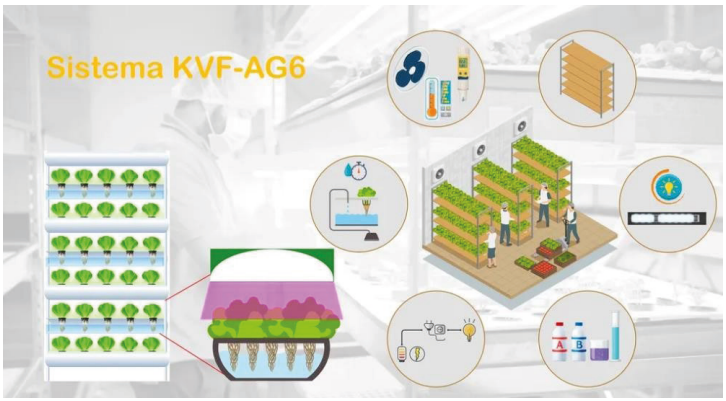


Figura 2. Karma Verde Fresh, un ejemplo de agricultura vertical en México (Fuente: https://karmaverdefresh.com/).

El gobierno y las instituciones académicas han fomentado la investigación y el desarrollo en áreas relacionadas con la agricultura sostenible, y la Secretaría de Agricultura y Desarrollo Rural (SADER) ha promovido proyectos de innovación tecnológica en el sector agrícola, incluidos los sistemas de cultivo sin suelo. Los estados con mayor adopción de estas técnicas son aquellos con escasez de agua o tierras agrícolas, como Baja California y Zacatecas, donde los sistemas aeropónicos se están considerando para cultivos de alto valor, como las hortalizas y plantas medicinales (Martínez & Pérez, 2021).

La propuesta del invernadero aeropónico basado en el Internet de las Cosas (IoT), es un prototipo de bajo costo que está compuesto por un banco de sensores, un microcontrolador y plataforma integradora Home Assistant (HA). El banco de sensores se utilizará para monitorizar las principales variables físicas del invernadero tales como temperatura, humedad y luminosidad del ambiente del entorno aeropónico. La función principal del microcontrolador será monitorizar y procesar las variables físicas anteriores y enviar el resultado al HA.

El HA permitirá mostrar en un entorno de aplicación móvil, el estado de cada uno de los sensores, actuadores y acceso remoto al invernadero.

2 | MARCO TEÓRICO

La aeroponía es un método avanzado de cultivo sin suelo en el cual las raíces de las plantas se suspenden en el aire y son rociadas con una solución rica en nutrientes. Esta técnica, que surge como una evolución de la hidroponía, ha ganado interés debido a su capacidad para maximizar el uso de agua y nutrientes, reducir el espacio requerido para el cultivo y evitar los problemas asociados al uso de suelo (Kozai et al., 2020; Sharma et al., 2019; Lakhiar et al., 2018; Zhang & Ling, 2021).

Figura 3. Torres de cultivo aeropónico (Fuente: www.agrohuerto.com)

El desarrollo de la aeroponía ha estado impulsado por la necesidad de encontrar soluciones agrícolas más sostenibles frente a los problemas derivados del cambio climático, la escasez de agua y la pérdida de tierras cultivables. Esta técnica es especialmente útil en ambientes controlados como invernaderos y sistemas de agricultura vertical, donde el uso eficiente de los recursos es prioritario.

Uno de los principales avances de la aeroponía es su capacidad para utilizar hasta un 95% menos agua que los métodos agrícolas tradicionales y su potencial para aumentar la velocidad de crecimiento de las plantas, debido a la alta oxigenación de las raíces. Además, los cultivos aeropónicos pueden producir alimentos durante todo el año independientemente de las condiciones climáticas externas, lo que los convierte en una opción viable para la producción en áreas urbanas y regiones con condiciones ambientales desfavorables.

A pesar de sus beneficios, la aeroponía enfrenta desafíos como el alto costo inicial de la infraestructura y el equipamiento necesario, así como la necesidad de un manejo técnico especializado para mantener los sistemas funcionando de manera óptima. La interrupción del suministro de nutrientes o del sistema de rociado puede causar daños rápidos a las plantas, lo que limita su adopción masiva.

Los avances en automatización y monitoreo han mejorado la viabilidad de la aeroponía, reduciendo la dependencia del manejo manual. Sin embargo, la falta de estandarización en la tecnología y la poca difusión de conocimientos sobre el tema en algunos países siguen siendo barreras para su implementación global (Medina & Gutiérrez, 2022).

Por otro lado, el Internet de las Cosas (IoT) ha crecido exponencialmente en la última década, transformando la manera en que interactuamos con el mundo digital y físico. IoT se refiere a la interconexión de dispositivos y objetos cotidianos a través de internet, lo que les permite recopilar, enviar y recibir datos sin intervención humana directa. El avance en sensores, redes inalámbricas y tecnologías de procesamiento ha facilitado esta expansión

(Atzori et al., 2020; Xu et al., 2019; Gubbi et al., 2021; Bello-Orgaz et al., 2021).

En la agricultura, el IoT ha permitido el monitoreo remoto de cultivos, e análisis del uso de agua y la automatización de sistemas de riego, lo que optimiza el rendimiento de las cosechas en un entorno donde el cambio climático y la escasez de recursos son problemas crecientes. Sin embargo, en México, los principales desafíos siguen siendo la infraestructura de telecomunicaciones y el alto costo de implementación de tecnologías IoT en comparación con otros países.

Por otro lado, Home Assistant (HA) es una plataforma de automatización de código abierto diseñada para monitorear, controlar y automatizar dispositivos inteligentes en un hogar. Desde su lanzamiento en 2013, ha ganado popularidad por su flexibilidad, amplia compatibilidad con una variedad de dispositivos y la posibilidad de operar de forma local, sin necesidad de depender de servicios en la nube. Esto proporciona una mayor privacidad y seguridad, una preocupación creciente en el ámbito del Internet de las Cosas (IoT) (Schneider, 2020; Gaur et al., 2021; Guo et al., 2021).

Con el objetivo de aumentar la velocidad de crecimiento de las plantas, este trabajo de investigación se centra, en su primera fase, en la implementación de un invernadero aeropónico de bajo costo basado en IoT.

3 | MATERIALES Y MÉTODOS

El diseño e implementación de la propuesta de invernadero inteligente ha sido orientado, en un principio, hacia el cultivo de rábanos, sin descartar la posibilidad de poder adaptarlo para otros cultivos incorporando nuevos sensores y actuadores.

El ciclo del cultivo del rábano depende de las condiciones climáticas, pudiendo encontrar desde 20 a más de 70 días. El desarrollo vegetativo tiene lugar entre los 6 y los 30º C. La temperatura óptima de germinación está entre 20 y 25º C (SIAP, 2023).

En la Figura 4 se presenta la arquitectura del invernadero inteligente indicando el alcance de procesamiento de las variables físicas involucradas, las herramientas tecnológicas utilizadas y los protocolos de comunicación inmersos en la transmisión de datos.

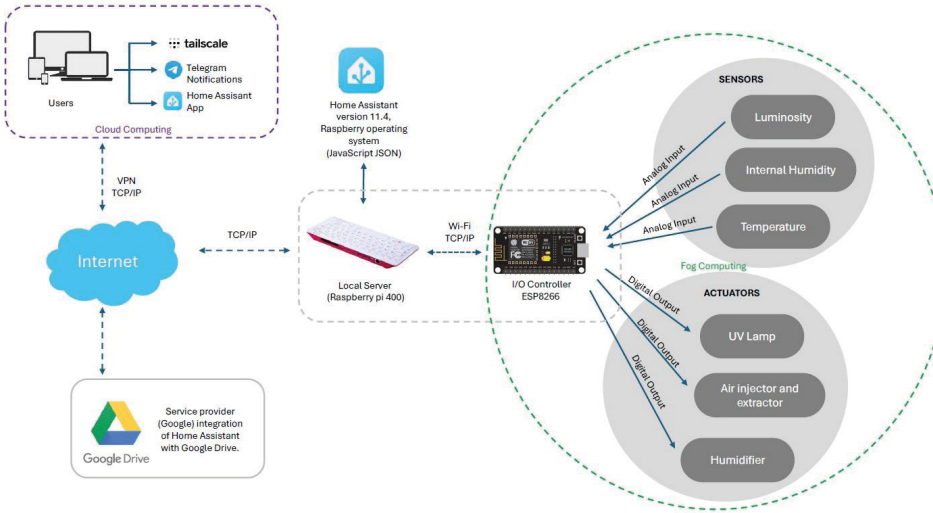
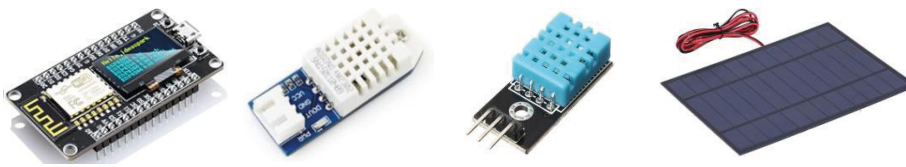


Figura 4. Arquitectura del Invernadero Inteligente basado en Lógica Difusa (Diseño propio).

En el extremo derecho de la Figura 4, se muestra el banco de sensores, actuadores gestionados por el microcontrolador ESP8266. En esta primera versión se han utilizado los sensores DHT22 para monitorizar la temperatura ambiental dentro del invernadero, el sensor DHT11 para monitorizar la humedad dentro de las torres aeropónicas y el panel solar PS-006 para monitorizar la intensidad de la luz. Con base en los valores obtenidos por los sensores anteriores, el invernadero podrá gestionar de manera automática la lámpara UV (λ=385-400 nm), el inyector y extractor de aire para mantener la temperatura interior entre 20 0C y 25 0C y los humidificadores de los tubos. La temperatura anterior se ha calibrado propiamente para los rábanos. La lámpara UV elegida es activada en caso de ausencia de luz natural.



a) Micro ESP8266 b) Sensor DHT22. c) Sensor DHT11. d) Panel solar PS-006.

Figura 5. Microcontrolador y banco de sensores utilizados en la primera fase del invernadero.

La instalación del Home Assistan en el microcontrolador Raspberry Pi 400 como plataforma operativa, permitirá tanto la gestión del banco de sensores y actuadores de manera local, así como el acceso a los mismos desde cualquier otro lugar de Internet con una interface gráfica hacia el usuario bastante intuitiva.

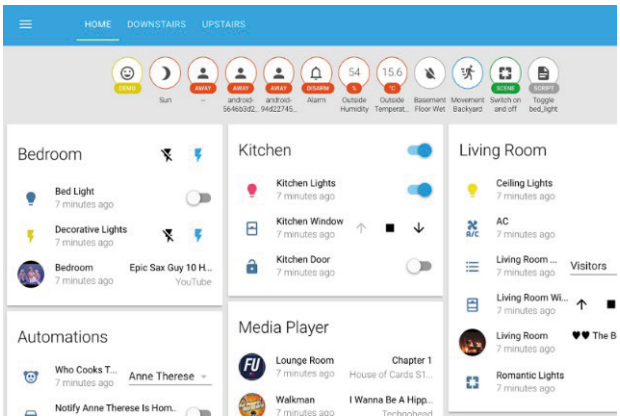


Figura 6. Ejemplo de una Interfaz Gráfica de Usuario (GUI) del Home Assistant personalizada (Fuente: https://magazine.odroid.com).

En el extremo izquierdo de la Figura 4, se observan las tecnologías que permiten la comunicación con el invernadero desde cualquier otro lugar utilizando la aplicación Home Assistant en cualquier dispositivo final tal como una computadora de escritorio, tableta o teléfono inteligente con acceso a Internet. La aplicación Telegram se usa como servicio de mensajería para enviar notificaciones sobre la operación del invernadero facilitando la comunicación inmediata y efectiva de cualquier evento relevante dentro del mismo y, finalmente, se utiliza la aplicación Tail para garantizar una comunicación segura via VPN con el microcontrolador Raspberry Pi 400 (Tailscale Inc, 2024).

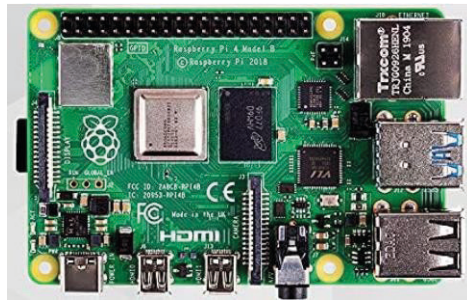


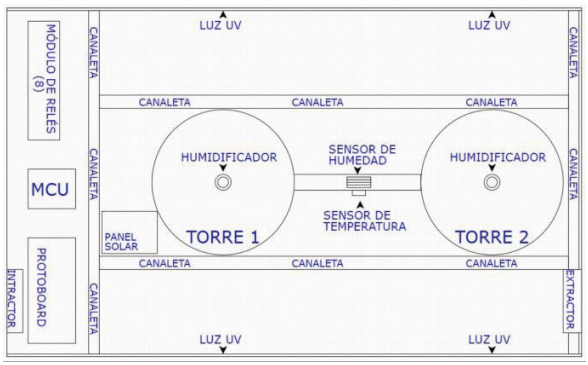
Figura 7. Microprocesador Raspberry Pi 4 utilizando a HA como sistema operativo.

Finalmente, mediante la integración de Home Assistant con Google Drive, permitirá hacer respaldos continuos de los datos generados por el invernadero.

4 | RESULTADOS Y DISCUSIÓN

Se han planificado varias fases para la implementación de este proyecto de investigación. En esta primera fase se construyó la maqueta con una base de madera, tubos aeropónicos de PVC y un techo de polietileno para permitir el paso de la luz natural

hacia las plántulas. Posteriormente se ha instalado todo el sistema de IoT conformado por el banco de sensores DHT12 y DHT11, el panel solar, los ventiladores (intractor y extractor), el microcontrolador ESP8266 y Raspberry Pi 4. En la Figura 8 se muestra tanto el diseño de la maqueta como del sistema IoT.

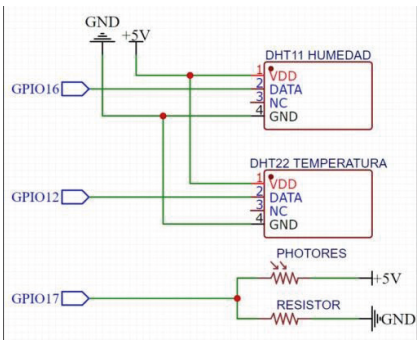


a) Diseño del Invernadero.

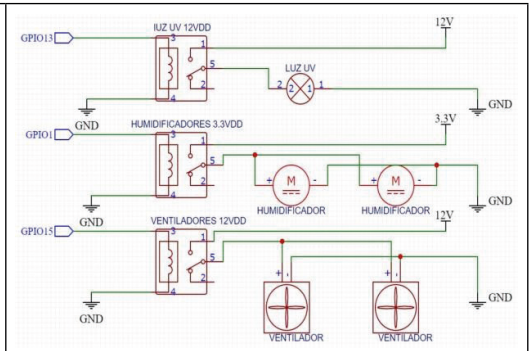
b) Implementación delInvernadero.

Figura 8. Diseño e implementación de la maqueta del invernadero.

Ahora, en la Figura 9 se muestra el diagrama eléctrico general del Invernadero derivado de la conexión de los sensores, los actuadores y los microcontroladores.



a) Conexión eléctrica de los sensores.



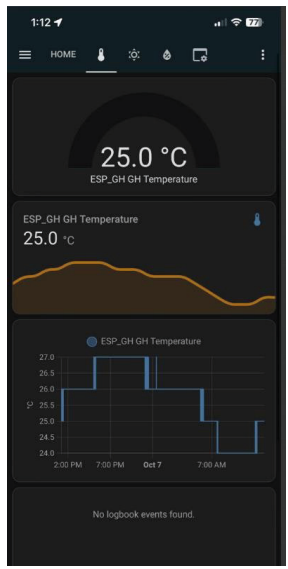
b) Conexión eléctrica de los actuadores.

Figura 9. Diagrama eléctrico general del Invernadero.

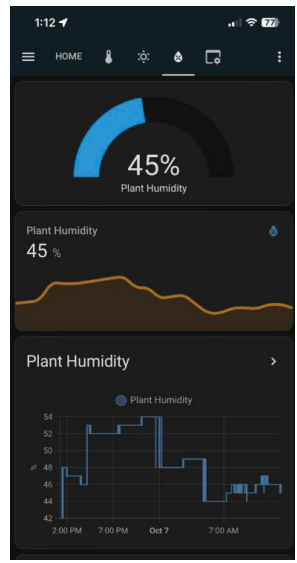
Para la gestión local o remota del invernadero, se ha utilizado como interfaz de usuario la plataforma Home Assistant (HA). El HA tiene la característica principal de ser una plataforma de código abierto diseñada para controlar y gestionar dispositivos inteligentes en el hogar. Justamente por ser de código abierto, en este proyecto se ha personalizado el HA para la gestión del invernadero. Otra de las principales características que ofrece HA es que permite la integración de una gran cantidad de dispositivos inteligentes de diferentes

fabricantes. Aunque en este proyecto HA hace la gestión de las variables físicas de humedad, luminosidad y temperatura del invernadero, asimismo permite escalar la gestión del invernadero en caso de aumentar y/o cambiar el control de las variables físicas para el manejo de otros tipos de semillas. En la siguiente figura se muestra el panel de control principal del Home Assistant junto con la gestión de las variables físicas del invernadero.

a) Panel principal del HA.



b) Registro de temperatura dentro del invernadero.



c) Registro de humedaddentro de los tubos.

Figura 10. Panel principal del Home Assistan para la gestión del invernadero.

Cabe la pena mencionar que la luz ultravioleta entra en acción de manera automática cuando se tiene una luz natural baja. En la Figura 11 se muestra el invernadero bajo la situación anterior.

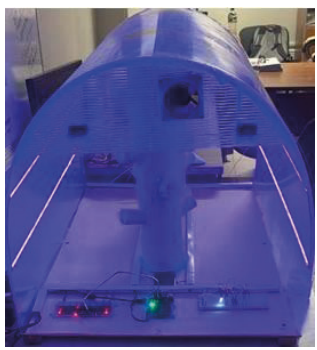


Figura 5. Funcionamiento automático de la luz UV y de la humidificación.

El usuario tiene la posibilidad de monitorizar constantemente la presencia de algún evento dentro del invernadero ya sea de manera local o remota via notificaciones del Telegram. En la siguiente figura se muestran algunos eventos tales como el estado de la temperatura, humedad, tiempo y calidad de exposición.

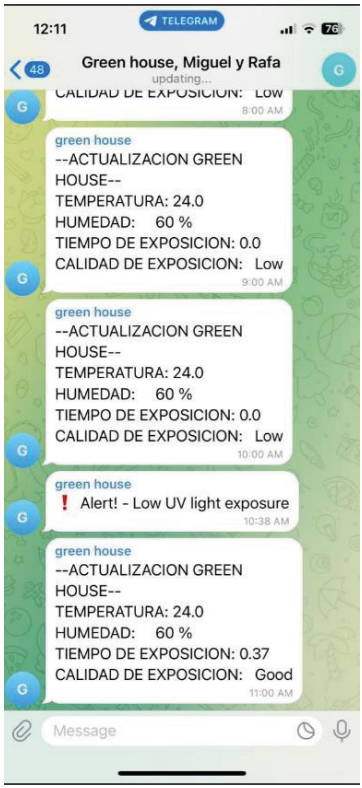


Figura 6. Interacción con el bot del Invernadero en Telegram para la monitorización de las principales variables físicas.

Como siguiente fase de este proyecto, se utilizará la lógica difusa para controlar todos los procesos de control generados dentro del invernadero. Por ejemplo, el proceso de control de temperatura interior, la sintonización de la luz ultravioleta dependiendo del tipo de germinación de semilla, la humedad de las torres, entre otras variables físicas.

5 | CONCLUSIONES

El uso del Internet de las Cosas en la agricultura ha revolucionado la manera en que gestionamos y optimizamos las operaciones agrícolas. Los sensores IoT permiten una monitorización en tiempo real de diversos parámetros críticos, como la humedad del suelo, la temperatura, la humedad ambiental. Esta capacidad de recopilación de datos precisa y continua facilita la toma de decisiones informadas, promoviendo prácticas agrícolas más

eficientes y sostenibles.

Implementar sensores IoT en la agricultura ofrece múltiples beneficios. Los agricultores pueden ajustar el riego y la temperatura con precisión, reduciendo el desperdicio de agua y nutrientes y mejorando el rendimiento de los cultivos. La siguiente fase de la implementación del Invernadero consistirá en la adopción de lógica difusa que, junto con el IoT, permitirá dar un gran paso hacia la agricultura de precisión; proporcionando herramientas avanzadas que ayudan a enfrentar los desafíos de la producción agrícola moderna y garantizando una gestión de recursos más responsable y eficaz.

REFERENCIAS

Atzori, L., Iera, A., & Morabito, G. (2020). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787-2805.

Bailey-Serres, J., Parker, J. E., Ainsworth, E. A., Oldroyd, G. E. D., & Schroeder, J. I. (2019). Genetic strategies for improving crop yields. *Nature*, 575(7781), 109- 118.

Bello-Orgaz, G., Jung, J. J., & Camacho, D. (2021). Social big data: Recent achievements and new challenges. *Information Fusion*, 28, 45-49.

Brady, N. C., & Weil, R. R. (2019). *The Nature and Properties of Soils*. Pearson. FAO (2021). The future of food and agriculture: Trends and challenges. Rome. *Food and Agriculture Organization of the United Nations*

Gaur, A., Scotney, B., Parr, G., & McClean, S. (2021). Smart home technologies: Overview, analysis, and challenges. *IEEE Access*, 7, 90945-90972.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2021). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645-1660.

Guo, X., Xu, L., & Li, S. (2021). Integration of IoT with Home Assistant for smart home automation. *Journal of Systems Architecture*, 104, 101713.

Kozai, T., Fujiwara, K., & Runkle, E. S. (2020). Plant Factory: An indoor vertical farming system for efficient quality food production. *Academic Press*.

Lakhiar, I. A., Gao, J., Syed, T. N., Chandio, F. A., & Buttar, N. A. (2018). Modern plant cultivation technologies in agriculture under controlled environment: A review on aeroponics. *Journal of Plant Interactions*, 13(1), 338-352.

Martínez, L., & Pérez, G. (2021). Sistemas hidropónicos y aeropónicos en México: Innovación y sostenibilidad en la producción agrícola. *Ciencia y Tecnología Agropecuaria*, 22(2), 45-58.

Medina, G., & Gutiérrez, F. (2022). Innovación en sistemas de cultivo aeropónico para mejorar la producción agrícola. *Ciencia y Tecnología Agropecuaria*, 12(3), 91-104.

Sánchez-Lizarraga, A. L., & Carrillo-López, A. (2020). Agricultura de precisión y su impacto en la producción agrícola en México. *Revista Mexicana de Agronegocios*, 24(3), 123-133.

Schneider, D. (2020). Home Assistant for smart home control: An open-source approach. *IEEE Consumer Electronics Magazine*, 9(5), 45-48.

Sharma, N., Acharya, S., Kumar, K., Singh, N., & Chaurasia, O. P. (2019). Hydroponics as an advanced technique for vegetable production: An overview. *Journal of Soil and Water Conservation*, 18(4), 364-371.

SIAP. (2023). RÁBANO. Consultado Junio 24, 2024, de https://www.gob.mx/cms/uploads/attachment/file/726314/Rabano.pdf

Tailscale Inc. (2024). Secure, remote access to. https://tailscale.com/

Xu, L. D., He, W., & Li, S. (2019). Internet of Things in industries: A survey. *IEEE Transactions on Industrial Informatics*, 10(4), 2233-2243.

Zhang, Y., & Ling, Q. (2021). Aeroponics: A tool for accelerated crop improvement. *Horticultural Science*, 26(2), 65-73.

INOVAÇÃO EM LABORATÓRIOS DIDÁTICOS COM A PLACA RASPBERRY PI

Data de submissão: 02/11/2024 *Data de aceite: 02/12/2024*

Thiago Corrêa Almeida
Universidade do Estado do Rio de Janeiro
Rio de Janeiro - RJ
http://lattes.cnpq.br/3266404381934797

Thiago Daboit Roberto
Universidade do Estado do Rio de Janeiro
Rio de Janeiro - RJ
http://lattes.cnpq.br/2694615438248688

RESUMO: Uma formação completa em qualquer área da ciência necessita de componente prática que complemente e signifique a componente teórica. Deste modo, escolas e universidades que possuem laboratórios didáticos bem equipados, saem na frente na função de fornecer ao estudante uma educação de qualidade. No entanto, nem todas as instituições de ensino, em especial as escolas da rede pública, possuem condições de garantir laboratórios didáticos bem equipados, devido ao alto valor de aquisição dos kits de empresas do ramo, como Pasco, Phywe e Cidepe. Deste modo, o presente trabalho propões a criação de um laboratório didático de baixo custo, e portátil, utilizando a placa *Raspberry Pi*, que consiste em um computador completo, pelo valor de US$35,00, e que permite interagir com o mundo ao redor utilizando sensores diversos. A placa, desenvolvida justamente para fins educacionais, tem sido amplamente utilizada mundo afora, devido ao baixo valor e facilidade no uso. Com a mesma, e um teclado, mouse e monitor, já é possível, com sensores baratos e outros materiais de baixo custo, elaborar experimentos diversos para o ensino de física em nível básico e superior. Apresentaremos dois experimentos que podem ser realizados, nos campos da Mecânica / Física Moderna, e da Termologia.

PALAVRAS-CHAVE: raspberry pi, laboratório portátil, TICs, experimentos.

INNOVATION IN DIDATIC LABORATORY WITH THE RASPBERRY PI BOARD

ABSTRACT: Complete training in any area of science requires a practical component that complements and signifies the theoretical component. In this way, schools and universities that have well-equipped teaching laboratories come out ahead in providing students with quality education. However, not all educational institutions, especially public schools, are able to guarantee well-equipped teaching laboratories, due to the high cost of

purchasing kits from companies in the sector, such as Pasco, Phywe and Cidepe. Therefore, the present work proposes the creation of a low-cost and portable teaching laboratory, using the Raspberry Pi board, which consists of a complete computer, for the value of US$35.00, and which allows you to interact with the world around you. using different sensors. The board, developed precisely for educational purposes, has been widely used around the world, due to its low cost and ease of use. With it, and a keyboard, mouse and monitor, it is now possible, with cheap sensors and other low-cost materials, to carry out various experiments for teaching physics at basic and higher levels. We will present two experiments that can be carried out, in the fields of Mechanics, Thermology and Modern Physics.
KEYWORDS: raspberry pi, portable laboratory, ICTs, experiments.

1 | INTRODUÇÃO

Uma das dificuldades enfrentadas pelo professor é a escassez de laboratórios, o que frequentemente faz com que estudantes concluam o ensino sem contato com atividades experimentais. Vários fatores contribuem para essa situação, como os altos custos de construção de laboratórios, a falta de recursos para manutenção, e até mesmo a falta de tempo ou conhecimento técnico para o uso adequado dos equipamentos. Nesse contexto, com o avanço dos computadores e smartphones, surgiram alternativas que utilizam essas tecnologias em substituição aos laboratórios tradicionais.

Entre essas ferramentas, o microcontrolador Arduino tem se destacado por suas aplicações em robótica e automação, permitindo a realização de experimentos acessíveis quando combinado com diversos sensores. Outra opção é o Raspberry Pi (UPTON, 2013), um microcomputador compacto e versátil, que se conecta a sensores através da porta GPIO. Diferentemente do Arduino, o Raspberry Pi (RPI) funciona como um computador completo, dispensando o uso de um dispositivo adicional para programação, armazenamento de dados e criação de gráficos. Sua principal linguagem de programação é o Python (MENEZES, 2014), conhecida pela simplicidade e vasta documentação disponível.

Neste artigo, propomos o uso do RPI na criação de um laboratório portátil e acessível, que possibilite a realização de experimentos em escolas sem laboratório disponível. Para exemplificar, compartilhamos nossa experiência com dois experimentos: estudo da transferência radiativa de calor e verificação da lei do inverso do quadrado da distância. O presente trabalho foi adaptado do trabalho produzido e apresentado por um dos autores em 2017 (Almeida et. al., 2017).

2 | MÉTODOS E MATERIAIS

A fim de resolver o problema da execução de um laboratório de baixo custo, analisamos o mercado e a literatura a fim de encontrar possibilidades viáveis e de baixo custo. Deste modo encontramos a placa RPI, muito utilizada no ensino de programação (Eberman, 2017), e a partir das possibilidades permitidas pela sua porta GPIO (*general*

purpose input/output), buscamos pesquisar que experimentos seriam viáveis e de fácil execução, de modo que a reprodução fosse tarefa simples até para pessoas que não tivessem conhecimento da área. Deste modo, selecionamos os experimentos, ouvindo professores de física, nas áreas de Mecânica / Física Moderna, e da Termologia. Abaixo apresentamos os materiais que foram utilizados.

2.1 Raspberry Pi

Em 2012 a placa RPI foi criada pela *Raspberry Pi Foundation* (RASPBERRY PI FOUNDATION, 2019), buscando baratear, democratizar e popularizar a robótica e computação – em uma ideia que tem os mesmos alicerces que a criação da placa micro controladora Arduino (Arduino, 2021), criada em 2005 na Itália, no Instituto Ivrea. O hardware da placa é do tamanho de um cartão de crédito, e é semelhante àquele dos smartphones, de modo que seu consumo de energia é baixo, e não sofre grande aumento na temperatura durante o uso. Pode ser usado como um *desktop*, com algumas limitações, e pode ser utilizada para vários projetos, como automação residencial, estações meteorológicas, sistemas de armazenamento pessoal, dentre outros. Seu potencial educativo foi pensado já em sua concepção, mas sua versatilidade fez com que a comunidade *maker* abraçasse a placa e logo passamos a ter muitos usuários, compartilhando ideias em fóruns na internet. Manuais de uso existem em abundância, como o livro de Richardson e Wallace (2015). A placa conta com um sistema operacional próprio, o Raspbian, que pode ser adquirido na página da criadora. O sistema é uma distribuição Linux baseada em debian. O armazenamento da placa é todo feito em um cartão micro SD. Embarcado, já temos alguns programas para aprendizado, como *scratch, Wolfram Mathematica,* e compiladores de *python.* Para programar e usar a porta GPIO, podemos programar em C++ ou *Python.* Na Figura 1 temos a primeira placa lançada, e no momento já estamos na 5ª versão, muito mais robusta e poderosa em processamento.

Figura 1: Placa Raspberry Pi B.

2.2 Light Dependent Resistor (LDR)

O LDR nada mais é que um resistor cuja resistência é sensível à luz recebida, de modo que pode funcionar como um “sensor de luminosidade”, seja qualitativamente, ou quantitativamente, caso se realize calibração com outra referência. É apresentando na Figura 2a. Sua resistência interna pode variar de algumas centenas de ohms à ordem de mega ohms, sendo bastante sensível a pequenas variações. Para uso do sensor, é preciso realizar uma pequena adaptação: a RPI realiza leitura apenas digital, e o sensor é analógico, de modo que precisa ser utilizado em conjunto com um capacitor, em um circuito RC. A montagem utilizada pode ser vista na Figura 3.

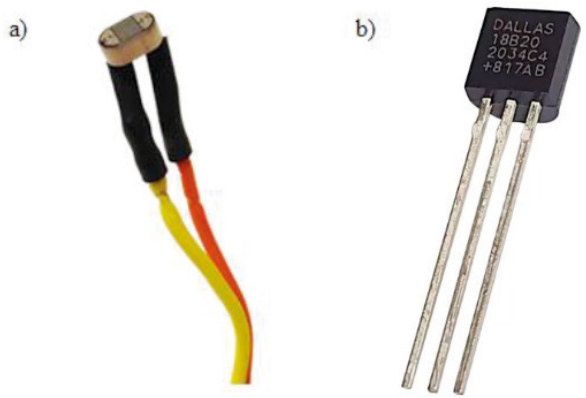


Figura 2: sensor LDR à esquerda (a) e o sensor DS18B20 à direita (b).

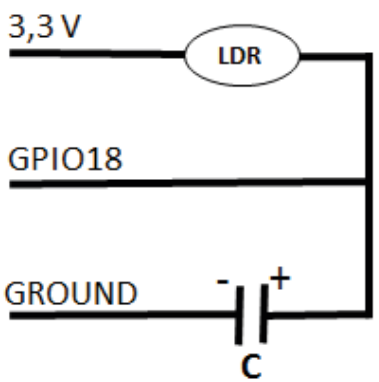


Figura 3: esquema de montagem do sensor LDR.

2.3 DS18B20

O sensor DS18B20, apresentado na Figura 2b, é um sensor do tipo *one-wire* que realiza aferição da temperatura por sinal digital. A facilidade do sensor é poder ser utilizado

em conjunto com vários outros sensores do mesmo tipo, bastando uma única ligação de todos eles à placa, visto que eles possuem um número que os identifica (ID). A ligação à placa, é simples, olhando o sensor de frente, o pino da direita é ligado à alimentação (3,3V), enquanto o da esquerda é ligado ao GND, e o do meio à porta GPIO escolhida para coletar as informações.

3 I RESULTADOS E DISCUSSÃO

Os experimentos realizados não costumam estar presentes em kits prontos de grandes empresas para laboratórios didáticos, de modo que são inovadores, sendo viáveis com o uso das TICs. Ambos já foram realizados com uso da placa Arduino (Souza, 2011) e também utilizando smartphones (Vieira, 2014). É importante salientar que o experimento de transmissão de calor por radiação aborda um meio de transmissão que normalmente não abordamos em sala de aula, sendo apenas citado, de modo que o experimento apresentado possibilita ao estudante visualizar na prática o conteúdo. O experimento de estudo da lei do inverso do quadrado permite diversas abordagens e explorações, uma vez que é uma lei presente em diversos campos da natureza.

3.1 Estudo da transferência de calor por radiação

A fim de realizar este experimento, realizamos montagem de uma caixa cúbica de isopor com chapas de 5mm, e firmamos em duas paredes opostas fôrmas metálicas de cores distintas. As cores analisadas foram preta, branca e azul. No centro da caixa foi feita a instalação de um bocal de lâmpada, equidistante das fôrmas. O sensor que usamos foi o DS18B20, já apresentado anteriormente, que foi instalado entre a fôrma e a parede de isopor. O sensor fornece a temperatura em Celsius, com precisão de ±0,5ºC, na faixa de -10ºC a +85ºC. A montagem pode ser vista na Figura 4.

Figura 4: montagem experimental para estudo da transferência de calor por radiação.

O tempo de exposição foi de 30 minutos, e construímos gráficos utilizando o matpotlib. O gráfico da evolução da temperatura das fôrmas pode ser visto na Figura 5.

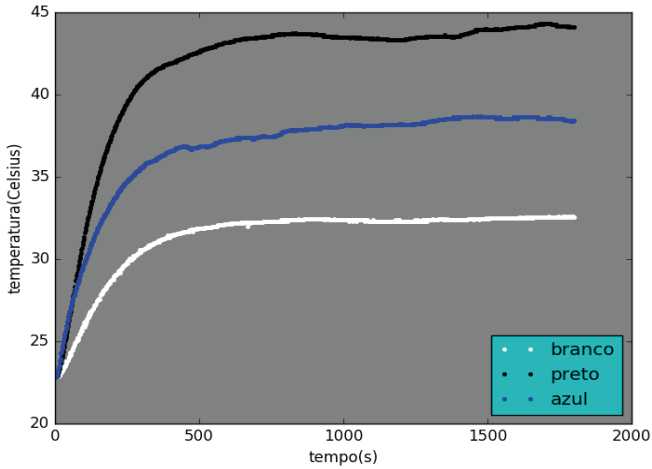


Figura 5: gráfico evolutivo da temperatura no tempo, das fôrmas branca, preta e azul.

É possível observar que todas as fôrmas evoluíram a temperatura de um valor comum, cerca de 24ºC, para valores terminais estáveis, que estão relacionados à cor de cada fôrma, sendo a branca a que obteve menor valor terminal, de 31ºC, a preta de maior valor terminal, de 43ºC, e a azul de valor intermediário, de 36ºC.

Este resultado permite a abordagem de diversos estudos, discutindo a absorção por cor, a refletância das diferentes cores, questões sobre tecnologias de refrigeração, etc.

3.2 Estudo da lei do inverso do quadrado

Este experimento é muito rico, e permite diversas abordagens, seja utilizando Arduino, Smartphone ou RPI. Isso torna interessante experimentar com os estudantes as diferentes abordagens e avaliar se o resultado é alterado caso se utilize tecnologias distintas.

Aqui utilizaremos o RPI ligado a um LDR como receptor, e uma lanterna como emissora de luz. Observaremos, com auxílio de uma trena, que a luminosidade decai com o inverso do quadrado da distância entre receptor e emissor. É simples executar o experimento, em uma aula curta, e compreende-se ricamente conceitos presentes na Lei de Coulomb e na Lei da Gravitação de Newton. A montagem pode ser vista na Figura 6.

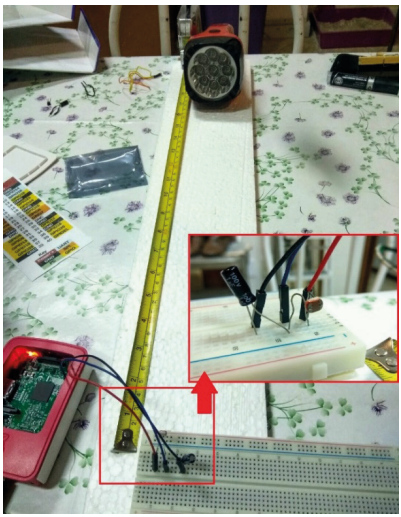


Figura 6: montagem do experimento. No detalhe, o circuito LDR.

Na Figura 7 é possível observar os dados obtidos e uma curva de ajuste, que segue a lei do inverso do quadrado, como era esperado.

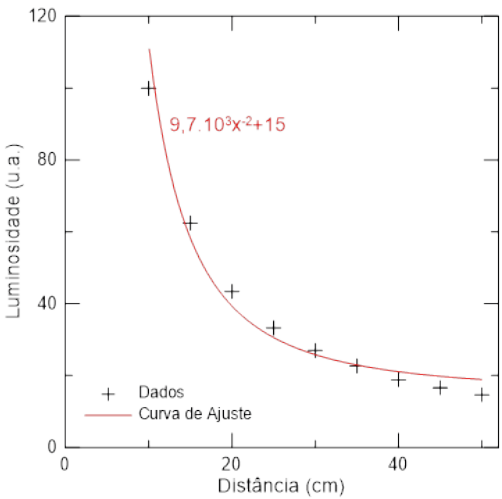


Figura 7: gráfico da luminosidade recebida no LDR contra a distância entre emissor e receptor.

4 | CONCLUSÕES

Concluímos que o Raspberry Pi é uma ferramenta potente para a realização de experimentos de física em sala de aula. Seu baixo custo, portabilidade e versatilidade são grandes atrativos, possibilitando estudos quantitativos e qualitativos de variados fenômenos por meio de códigos e montagens experimentais simples. Com pequeno investimento, é possível adquirir a placa e uma gama de sensores que permitirão realizar experimentos

para praticamente todos os conteúdos abordados na física, seja no ensino básico ou superior.

REFERÊNCIAS

ALMEIDA, T. C.; JULIÃO, A.; DIAS, E. C.; PORTO, M. B. **Uma proposta de laborátorio portátil de física de baixo custo utilizando o microcomputador raspberry pi**. Anais da VIII Jornada Científica do IFRJ campus Volta Redonda, v. 1. p. 286-300., 2017.

ARDUINO. **About Arduino**. 2021. Disponível em: <https://www.arduino.cc/en/about>. Acesso em 02 nov 2024.

EBERMAM, E.; PESENTE, G.; RIOS, R. O.; PULINI, G. C. **Programação para leigos com Raspberry PI**. João Pessoa: Editora IFPB, 2017

MENEZES, C.; NEY, N. **Introdução à Programação Com Python**, São Paulo: Novatec, 2014.

RASPBERRY PI FOUNDATION. **Raspberry Pi — Teach, Learn, and Make with Raspberry Pi**. 2019. Disponível em: <https://www.raspberrypi.org/>. Acesso em 02 nov 2024.

RICHARDSON, M.; WALLACE, S. **Make: Getting Started with Raspberry Pi.** California: Maker Media, 2015.

SOUSA, M. A.; SANTOS, A. A. **Absolute gravimetry on the Agulhas Negras calibration line**. Rev. Bras. Geof.,Rio de Janeiro, v. 28, n. 2, p. 165, abril 2010.

SOUZA, A. R. et al. **A placa arduino: uma opção de baixo custo para experiências de física assistidas pelo PC**. Revista Brasileira de Ensino de Física, São Paulo, v. 33, n. 1, p. 1702, jan. 2011.

UPTON, E.; HALFACREE, G. **Raspberry Pi: Manual do Usuário**, São Paulo: Novatec, 2013.

VIEIRA, L. P.; LARA, V. O. M.; AMARAL, D. F. **Demonstração da lei do inverso do quadrado com o auxílo de um tablet/smartphone**. Revista Brasileira de Ensino de Física, São Paulo, v. 36, n. 3, p. 3505, set. 2014.

ANEXOS: CÓDIGOS EM PYTHON UTILIZADOS

Código utilizado para os experimentos com o LDR.

```
#!/usr/bin/env python

import time
import RPi.GPIO as GPIO, time, os

DEBUG = 1
GPIO.setmode(GPIO.BCM)
luz = 0
tempo = 0

def RCtime (RCpin):
reading = 0
GPIO.setup(RCpin, GPIO.OUT)
GPIO.output(RCpin, GPIO.LOW)
time.sleep(0.01)
GPIO.setup(RCpin, GPIO.IN)
while (GPIO.input(RCpin) == GPIO.LOW):
reading += 1
return reading
while True:
f = open('Results.txt', 'a')
luz = RCtime(18)
tempo = time.time()
f.write('\t' + str(luz) + '\t' + str(tempo) + '\n')
f.close()
```

Código utilizado para o experimento com o DS18B20.

```
import os
import glob
import time

#inicializaçao do sistema

os.system('modprobe w1-gpio')
os.system('modprobe w1-therm')

#obtençao dos dados do sensor

base_dir = '/sys/bus/w1/devices/'
device_folder = glob.glob(base_dir + '28*')[0]
device_file = device_folder + '/w1_slave'

def read_temp_raw():
    f = open(device_file, 'r')
    lines = f.readlines()
    f.close()
    return lines

def read_temp():
    lines = read_temp_raw()
    while lines[0].strip()[-3:] != 'YES':
        time.sleep(0.2)
        lines = read_temp_raw()
    equals_pos = lines[1].find('t=')
    if equals_pos != -1:
        temp_string = lines[1][equals_pos+2:]
        temp_c = float(temp_string) / 1000.0
        return temp_c

r = open('preto.txt','w')
dtime = 0
start_time = time.time()
while dtime < 1800:
            dtime = time.time() - start_time
            r.write(str(read_temp()) + ',' +
str(dtime) + '\n')
            time.sleep(1)

r.close()
```

Código para a plotagem de gráficos com a biblioteca matpotlib. Para a utilização desse código é necessário a instalação dos pacotes numpy e matplotlib.

```
import matplotlib.pyplot as plt

#função para a leitura do arquivo

def ler_dados(arquivo):
        x = []
        y = []

        dados = open(arquivo, 'r')

        for line in dados:
                line = line.strip()
                X, Y = line.split('\t')
                x.append(X)
                y.append(Y)
        dados.close()

        return x, y

temp_b, tempo_b = ler_dados('branco.txt')
temp_p, tempo_p = ler_dados('preto.txt')

#características do gráfico

plt.axes(axisbg = 'grey')
plt.plot(tempo_b, temp_b, 'w.', label =
'branco')
plt.plot(tempo_p, temp_p, 'k.', label =
'preto')
legend_bk = get_frame().set_facecolor
plt.legend(loc = 'lower right').legend_bk('c')
plt.xlabel('tempo(s)')
plt.ylabel('temperatura(Celsius)')

plt.show()
```

CAPÍTULO 5

APRENDIZAGEM ATIVA UTILIZANDO ARDUINO: RELATOS DE PROJETOS DISCENTES

Data de submissão: 03/11/2024 *Data de aceite: 02/12/2024*

Thiago Corrêa Almeida
Universidade do Estado do Rio de Janeiro
Rio de Janeiro - RJ
http://lattes.cnpq.br/3266404381934797

Manoela Lopes Carvalho
Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro
Rio de Janeiro - RJ
http://lattes.cnpq.br/5302484744873241

Thiago Daboit Roberto
Universidade do Estado do Rio de Janeiro
Rio de Janeiro - RJ
http://lattes.cnpq.br/2694615438248688

RESUMO: Este trabalho apresenta dois projetos desenvolvidos no âmbito da aprendizagem ativa com foco em robótica e tecnologia, ambos realizados em colaboração com o grupo RoboCAp-UERJ, utilizando a robótica para o aprendizado indireto e significativo de física, apoiado na metodologia de Aprendizagem Baseada em Projetos (ABProj). O primeiro projeto foi conduzido no Instituto de Aplicação Fernando Rodrigues da Silveira (CAp-UERJ), dentro da Iniciação Científica Júnior (ICJr). Nele, os estudantes, após adquirirem conhecimentos sobre Arduino e eletrônica básica, são incentivados a aplicar o que aprenderam em projetos de impacto positivo para a comunidade escolar. Como exemplo, foi desenvolvida uma lâmpada inteligente, capaz de acender no escuro e apagar no claro, projetada para ser instalada nas dependências do CAp-UERJ. Durante o processo, os alunos exploraram conceitos de eletricidade e óptica. O segundo projeto, realizado em parceria com o IFRJ campus Maracanã, levou à criação do dispositivo chamado de Nature+, desenvolvido para facilitar o monitoramento de áreas de acesso difícil ou perigoso, sendo voltado a pesquisadores e professores. Inspirado nas sondas de exploração espacial da NASA, o Nature+ é um carrinho controlado via Bluetooth por smartphone e equipado com sensores de temperatura, pressão atmosférica, umidade e gases inflamáveis/fumaça. Os dois projetos utilizam a placa Arduino, e foram premiados em seminários e feiras de conhecimento. Esses projetos destacam a robótica como uma ferramenta eficaz para o aprendizado ativo e interdisciplinar, oferecendo aos estudantes uma oportunidade de aplicar teorias de física e biologia em situações reais, e desenvolver soluções tecnológicas úteis para a sociedade.

PALAVRAS-CHAVE: aprendizagem ativa, arduino, robótica, TICs.

ACTIVE LEARNING USING ARDUINO: REPORTS FROM STUDENT PROJECTS

ABSTRACT: This work presents two projects developed within the framework of active learning with a focus on robotics and technology, both conducted in collaboration with the RoboCAp-UERJ group, utilizing robotics as an indirect and meaningful way to learn physics, supported by the Project-Based Learning (PBL) methodology. The first project was carried out at the Instituto de Aplicação Fernando Rodrigues da Silveira (CAp-UERJ) within the Junior Scientific Initiation Program (ICJr). In this project, students, after gaining knowledge of Arduino and basic electronics, are encouraged to apply what they have learned in projects that positively impact the school community. For instance, a smart lamp was developed that turns on in the dark and off in the light, designed to be installed at CAp-UERJ facilities. During the process, students explored concepts of electricity and optics. The second project, conducted in partnership with IFRJ Maracanã campus, led to the creation of a device called Nature+, designed to facilitate the monitoring of hard-to-reach or hazardous areas and aimed at researchers and educators. Inspired by NASA's planetary exploration probes, Nature+ is a cart controlled via Bluetooth by a smartphone, equipped with sensors for temperature, atmospheric pressure, humidity, and flammable gases/smoke. Both projects use the Arduino platform and have been recognized at seminars and science fairs. These projects highlight robotics as an effective tool for active and interdisciplinary learning, offering students the opportunity to apply physics and biology theories in real-world situations and to develop technological solutions beneficial to society.
KEYWORDS: active learning, arduino, robotics, ICTs.

1 | INTRODUÇÃO

Atualmente, a robótica está cada vez mais presente em nossas vidas, tanto em ambientes urbanos quanto fora deles. Ela é amplamente utilizada em indústrias, linhas de produção e montagem, desde o setor alimentício até as montadoras de automóveis. Esse contexto torna o aprendizado em robótica uma competência importante para o exercício da cidadania. No entanto, muitos conceitos físicos estão embutidos nos sistemas robóticos, de modo que é essencial conhecer a física para entender como esses dispositivos funcionam. O ensino de ciências da natureza, no entanto, pode ser considerado maçante, devido à ênfase na "matematização", que nem sempre é necessária para a compreensão dos conceitos fundamentais.

Desta forma, a aprendizagem ativa se mostra como uma excelente opção para que o estudante aprenda "colocando a mão na massa", através, por exemplo, da Aprendizagem Baseada em Projetos (ABProj). Este trabalho propõe uma abordagem diferenciada para o aprendizado de física e biologia, de maneira prática e significativa. Através do desenvolvimento de projetos de robótica voltados à criação de soluções úteis para a sociedade, os conceitos são aprendidos na prática, tornando-se mais memoráveis e aplicáveis. Esta metodologia é baseada na aprendizagem ativa, que promove o engajamento

dos estudantes e facilita a retenção de conteúdo (Barbosa & Moura, 2013; Moura & Barbosa, 2011; Silberman, 1996). A plataforma Arduino foi escolhida por ser amplamente utilizada em atividades educacionais, sendo de fácil uso e acessível em termos de custo. Na literatura encontramos diversos trabalhos utilizando a placa (Cavalcante, Tavolaro & Molisani, 2011; Cordova & Tort, 2016; Souza, 2011).

Ao longo do trabalho, relatamos o desenvolvimento de dois projetos discentes, em duas instituições de ensino do Rio de Janeiro, uma no ensino médio, e outra em curso de graduação. O primeiro projeto consistiu no desenvolvimento de uma lâmpada inteligente, viabilizando economia de energia elétrica. O segundo projeto idealizou o dispositivo Nature+, projetado para monitorar parâmetros ecológicos em áreas de difícil acesso, com objetivos de pesquisa e educação ambiental (Dias, 2001; Cavalcanti, 1994). Esse dispositivo, de baixo custo e fácil construção, permite a coleta em tempo real de dados como temperatura, pressão atmosférica, umidade relativa e presença de gases inflamáveis, sendo controlado via Bluetooth por um smartphone.

O presente trabalho se baseia em resumos publicados nos anais da MNR 2018 pelos autores (Neto & Almeida, 2018; Marrucho et. al., 2018).

2 | METODOLOGIA

Os projetos discentes buscaram seguir sequência baseada em metodologia de aprendizagem ativa conhecida como Aprendizagem Baseada em Projetos – ABProj (Barbosa & Moura, 2013; Costa, 2010; Godoy, 2009). Para a realização do projeto foram pensados seis momentos a serem percorridos pelos estudantes, sendo estes os momentos de Motivação (M), Preparação (P), Exploração (E), Desenvolvimento (D), Apresentação (A) e Reflexão (R). Estes momentos foram pensados com base nas fases envolvidas na ABProj. Os estudantes incialmente tiveram encontros para **motivação (M)**, assistindo vídeos sobre a placa Arduino (Arduino, 2018) e sendo apresentados às possibilidades de desenvolvimento com a mesma. Em seguida, na **preparação (P)**, realizamos encontros para estudo de eletrônica e programação, aulas de circuitos, leis de kirchoff, lei de ohm e utilização do multímetro. Inicialmente foram realizadas atividades virtuais, na plataforma Tinkercad, e posteriormente no laboratório, práticas com a placa Arduino. A **exploração (E)** consistiu em verificarem todo o equipamento disponível no laboratório e levantar o que seria necessário adquirir para elaboração do projeto. Logo passamos ao **desenvolvimento (D)**, onde os estudantes iniciaram a execução dos protótipos, se deparando com vários problemas, e buscando autonomamente as soluções. Este é um momento de muita riqueza, onde acontece prioritariamente a aquisição indireta de conhecimentos de diversas disciplinas, a depender do projeto em específico que está sendo executado. Por fim, a culminância, se dá na **apresentação (A)**, onde os estudantes apresentam seus resultados ao público, neste caso, em eventos e feiras científicas. Por fim, na **reflexão (R)**, os

estudantes registram e rememoram tudo o que fizeram, normalmente apresentando o mesmo em eventos científicos.

3 | RESULTADOS E DISCUSSÃO

Apresentaremos nas seções seguintes o relato de cada um dos projetos, assim como materiais, custo estimado, imagens e esquema de montagem.

3.1 Projeto 1: Lâmpada Inteligente

A lâmpada inteligente é um dispositivo semelhante às lâmpadas de postes que acendem automaticamente à noite e apagam durante o dia. O foco de sua construção não foi tanto a inovação do dispositivo em si, mas o aprendizado proporcionado ao longo do processo. A Figura 1 mostra a lâmpada desenvolvida.

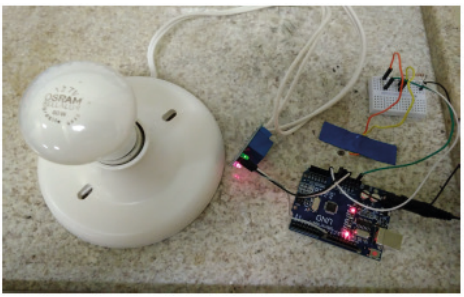


Figura 1: lâmpada inteligente no ambiente claro.

Optamos por confeccionar uma lâmpada que não fosse controlada por relógio, mas sim pela luminosidade captada, de modo que funcionaria bem mesmo em dias atípicos. Para construção da lâmpada utilizamos os seguintes materiais: Arduino UNO, 2x LDR, 2x Módulo RTC, Módulo SD, Relê de um canal, Plafonier, Lâmpada 60W, fios, protoboard e plug de tomada.

O primeiro passo para o desenvolvimento de nossa lâmpada foi registrar a curva de luminosidade do local onde ela seria instalada, a fim de definir o valor padrão de luminosidade que determinaria o acendimento e apagamento automáticos. Para isso, conectamos ao Arduino um sensor LDR, um módulo SD com cartão de memória e o módulo RTC, deixando o dispositivo posicionado no local da futura instalação da lâmpada. Durante alguns dias, o LDR registrou a curva de luminosidade, armazenando os dados no cartão SD. Na Figura 2, apresentamos a curva obtida em um dia específico. Observa-se um comportamento simétrico entre o amanhecer e o anoitecer, com uma transição rápida de escuro para claro entre cinco e sete da manhã, e de claro para escuro entre seis e oito da noite.

Com base nessa curva, definimos o valor de luminosidade 600 como o limite para ligar

ou desligar a lâmpada. Com esse parâmetro estabelecido, conectamos o relé ao Arduino, junto com a lâmpada e o plafonier, permitindo que o Arduino controle o acendimento e apagamento da lâmpada de acordo com a leitura do LDR. Retiramos os módulos SD e RTC, pois não seriam mais necessários.

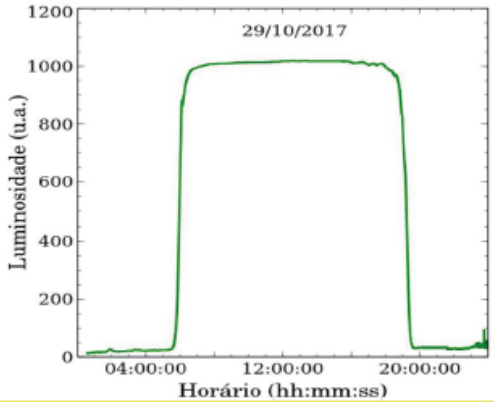


Figura 2: curva de luminosidade obtida no ambiente escolar.

Em testes práticos, nossa lâmpada funcionou perfeitamente, acendendo e apagando conforme a luminosidade, independentemente do horário. O custo estimado é de 60 reais, valor que consideramos adequado em vista da economia de energia e da praticidade que essa lâmpada pode oferecer. O projeto foi apresentado na 26ª Semana de Iniciação Científica da UERJ, onde recebeu o prêmio de primeiro lugar na categoria ICJr.

3.2 Projeto 2: Nature+

O dispositivo foi concebido como projeto para participar na XI Feira de Ciência, Tecnologia e Inovação do Rio de Janeiro, visando uma experiência prática de aprendizagem em biologia utilizando a robótica. Seria um dispositivo voltado a auxiliar professores e pesquisadores no monitoramento de áreas específicas, tanto para pesquisa quanto para fins educacionais. O resultado foi um veículo robótico controlado via Bluetooth, por meio de um smartphone, que coleta em tempo real dados sobre pressão atmosférica, temperatura, umidade relativa do ar e presença de gases inflamáveis ou fumaça. Esses dados são exibidos em gráficos no aplicativo Virtuino (Lamprou, 2021). O dispositivo pode ser visto na Figura 3.

Figura 3: dispositivo Nature+.

Na concepção do robô, nos inspiramos nas sondas de exploração planetária. Como o dispositivo se move sobre rodas, ele pode ser usado para medir parâmetros à distância em áreas de acesso difícil ou perigoso. A interface no aplicativo Virtuino é dividida em duas seções: controle e visualização de dados. No lado esquerdo (controle), é possível direcionar o movimento do robô em várias direções. Ao pressionar “start”, o movimento é interrompido, permitindo alternar para a seção de sensores, onde os dados monitorados são exibidos graficamente (à direita). A interface completa pode ser vista na Figura 4.

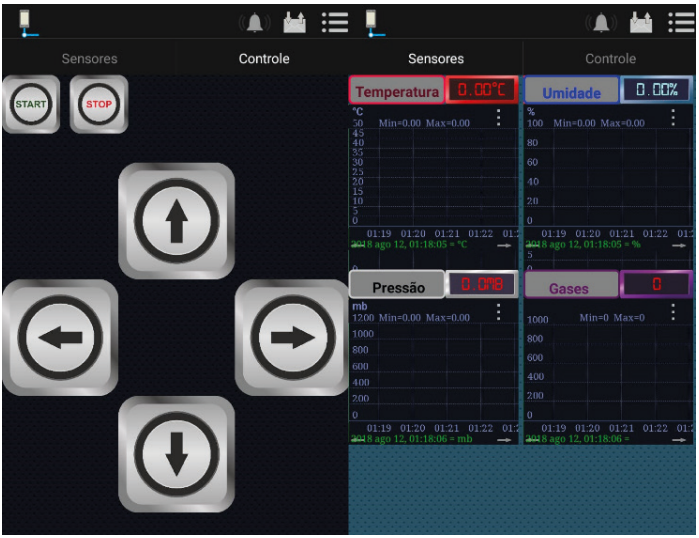


Figura 4: interface montada no aplicativo Virtuino.

Os materiais utilizados na montagem de nosso dispositivo foram os seguintes: Arduino Nano, Roda com caixa de redução (2x), Bateria 18650 de 3,7V (2x), Sensor DHT11, Sensor BMP280, Módulo Bluetooth HC-05, Leds, Ponte H L9110, Sensor de gás MQ-5.

Optamos pelo Arduino Nano em vez do mais popular Arduino UNO devido ao seu tamanho reduzido e menor consumo de energia. Além dos componentes mencionados, utilizamos uma placa universal para criar a placa de circuito na versão final do dispositivo,

conferindo maior robustez ao projeto. A estrutura do carro foi adaptada de um modelo de brinquedo de plástico encontrado em lojas de varejo. As Figuras 5, 6 e 7 mostram cada componente e indicam suas conexões na placa Arduino.

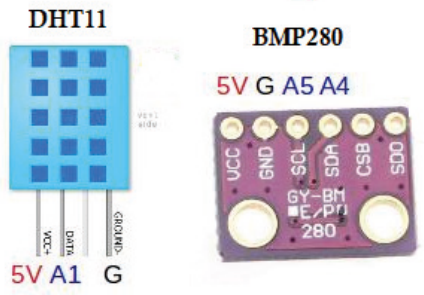


Figura 5: esquema de ligação dos sensores DHT11 e BMP280.

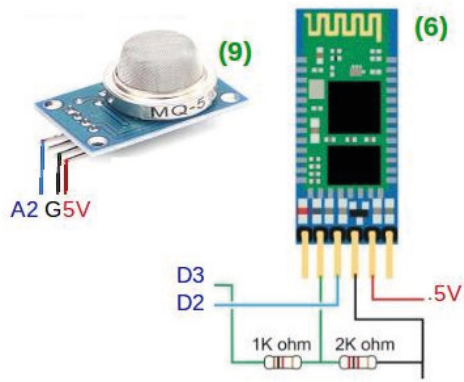


Figura 6: esquema de ligação do sensor MQ-5 e do módulo bluetooth.

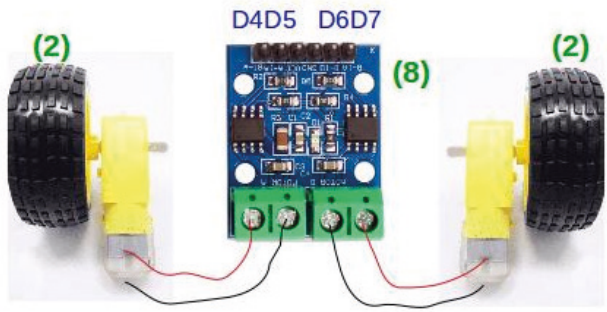


Figura 7: esquema de ligação das rodas e da ponte H.

Como mostrado na Figura 6, para a conexão do módulo Bluetooth, é necessário um divisor de tensão feito com resistores de 1k ohm e 2k ohm, sendo então ligado nas portas digitais D2 e D3 do Arduino, além do 5V e GND.

O código foi desenvolvido na ARDUINO IDE utilizando as bibliotecas Adafruit_ Sensor, Adafruit_BMP280, DHT, Wire, SPI e VirtuinoBluetooth. O trabalho foi exibido na XI FECTI, atraindo a atenção de centenas de visitantes, incluindo muitos professores que manifestaram interesse no uso do Nature+ para atividades de ensino e pesquisa, o que indicou que os objetivos foram atingidos.

Nos testes iniciais, verificamos que o Nature+ possui uma autonomia de cerca de duas horas com a alimentação utilizada e uso leve a moderado dos motores. O alcance do controle via Bluetooth chega a aproximadamente cinco metros. As medições de temperatura foram comparadas com termômetros convencionais e mostraram excelente precisão, com erro percentual inferior a 1%. Os dados de pressão atmosférica foram verificados com registros de um banco de dados (Daftlogic, 2009), apresentando excelente concordância, assim como as medições de umidade relativa. Em laboratório, testamos o sensor de gases inflamáveis, expondo-o a gás de isqueiro e fumaça a 5 cm de distância; em segundos, o sensor reagiu, aumentando os valores detectados em uma a duas ordens de grandeza.

4 I CONCLUSÕES

Neste trabalho relatamos dois projetos discentes inseridos na metodologia de aprendizagem ativa ABProj, onde estudantes de duas instituições de ensino, do ensino médio e da graduação, desenvolveram projetos tecnológicos utilizando o arduino para participação em eventos e feiras. O desenvolvimento levou os estudantes, de forma autônoma a adquirirem conhecimentos, de maneira significativa, nos campos da física, biologia, e outras competências. Além disso, habilidades como resolução de problemas, criatividade, autonomia e trabalho em equipe foram intensivamente trabalhadas, reforçando competências essenciais para a vida profissional.

A experiência foi enriquecedora e recompensadora. Com a conquista do primeiro lugar na 26ª Semana de Iniciação Científica da UERJ (Projeto 1), e com o prêmio de 3º lugar interdisciplinar na XI FECT (Projeto 2). Ambos os projetos atraíram grande interesse do público, especialmente de professores, muitos dos quais demonstraram intenção de replicar o projeto em suas atividades.

Segundo os discentes participantes, “essa experiência de aprendizagem ativa não só nos proporcionou uma aplicação prática dos conteúdos teóricos, mas também uma realização pessoal e profissional significativa, que certamente influenciará nossa trajetória futura”.

REFERÊNCIAS

ARDUINO. **Arduino**, 2018. Disponível em: <https://arduino.cc/>. Acesso em: 02 nov 2024.

BARBOSA, E. F.; MOURA, D. G. Metodologias ativas de aprendizagem na Educação Profissional e Tecnológica. **Boletim Técnico do Senac**. v. 39, n.2, p.48-67, 2013.

CAVALCANTE, M. A.; TAVOLARO, C. R. C.; MOLISANI, E. Física com arduino para iniciantes. **Revista Brasileira de Ensino de Física**, São Paulo, v. 33, n. 4, p. 4503, out. 2011.

CAVALCANTI, C. Desenvolvimento e natureza: estudos para uma sociedade sustentável. INPSO/ FUNDAJ, **Instituto de Pesquisas Sociais**, Fundação Joaquim Nabuco, Ministério da Educação, Governo Federal, Recife, Brasil. 1994.

CORDOVA, H.; TORT, A.C. Medida de g com a placa arduino em um experimento simples de queda livre. **Revista Brasileira de Ensino de Física**, São Paulo, v. 38, n. 2, p. 2308, maio 2016.

COSTA, A. R. P. **Metodologia de projetos: a percepção do aluno sobre os resultados da sua aplicação**. Dissertação (Mestrado em Educação Tecnológica) - CEFET-MG, Belo Horizonte, 2010.

DAFTLOGIC. **Google Maps Find Altitude**. 2009. Disponível em: <https://www.daftlogic.com/sandbox-google-maps-find-altitude.htm>. Acesso em: 02 nov 2024.

DIAS, Genebaldo Freire. **Educação ambiental: princípios e práticas**. 7.ed. São Paulo: Gaia, 2001.

GODOY, E. G. U. **Contribuições da metodologia de projetos na implantação das tecnologias de informação e comunicação – TIC nos processos educativos da educação básica**. Dissertação (Mestrado em Educação Tecnológica) – Cefet-MG, Belo Horizonte, 2009.

LAMPROU, I. **Virtuino 6**. 2021. Disponível em: < https://play.google.com/store/apps/details?id=com.virtuino_automations.virtuino>. Acesso em: 02 nov 2024.

MARRUCHO, C. da C.; ALHEIROS, S. F.; MACEDO, T. M. de; CARVALHO, M. L. Nature+, ferramenta de baixo custo para realização de monitoramento ambiental. **Anais da VIII Mostra Nacional de Robótica (MNR 2018)**. São Paulo, v. 1, n. 1, p. 241, 2018.

MOURA, D. G.; BARBOSA, E. F. **Trabalhando com projetos: planejamento e gestão de projetos educacionais**. Petrópolis: Vozes, 2011.

NETO, M. P. dos S.; ALMEIDA, T. C. Aprendendo Física por meio da Robótica, lâmpada Inteligente. **Anais da VIII Mostra Nacional de Robótica (MNR 2018)**. São Paulo, v. 1, n. 1, p. 43, 2018.

SILBERMAN, M. **Active learning: 101 strategies do teach any subject**. Massachusetts: Ed. Allyn and Bacon, 1996.

SOUZA, A. R. et al. A placa arduino: uma opção de baixo custo para experiências de física assistidas pelo PC. **Revista Brasileira de Ensino de Física**, São Paulo, v. 33, n. 1, p. 1702, jan. 2011.

CAPÍTULO 6

INTELIGÊNCIA ARTIFICIAL NO CONTEXTO DAS BIBLIOTECAS UNIVERSITÁRIAS: CONCEITOS E TENDÊNCIAS

Data de submissão: 08/10/2024 *Data de aceite: 02/12/2024*

Marcos Vinicius Mendonça Andrade
http://lattes.cnpq.br/0735082959494528

Ana Rosa dos Santos
http://lattes.cnpq.br/8478823303610041

RESUMO: Aborda a aplicação da Inteligência Artificial - IA - no contexto da Biblioteca Universitária. Traz um breve histórico, características e princípios atrelados à Inteligência Artificial, bem como suas pretensas aplicações em serviços de informação. Demonstra através de revisão de literatura um panorama sobre os estudos publicados na área, tendo como recorte temporal o período entre 2018 e 2023. Os resultados obtidos evidenciam que a aplicação da IA em Bibliotecas Universitárias é apontada como um tema emergente e descortina uma série de potencialidades e desafios exigindo uma nova postura por parte destas instituições e dos profissionais a elas vinculados, em especial, os bibliotecários. Ressalta que os estudos nesta temática ainda são incipientes.

PALAVRAS-CHAVE: Inteligência Artificial. Bibliotecas Universitárias. Inovação em Bibliotecas.

TRENDS IN THE APPLICATION OF ARTIFICIAL INTELLIGENCE IN THE UNIVERSITY LIBRARY: POSSIBILITIES AND LIMITATIONS

ABSTRACT: This paper approaches the application of Artificial Intelligence - AI - in the context of the University Library. It brings a brief history, characteristics and principles linked to Artificial Intelligence, as well as its alleged applications in information services. It demonstrates, through a literature review, an overview of the studies published in the area, having as a time frame the period between 2018 and 2023. The results obtained show that the application of AI in University Libraries is identified as an emerging theme and reveals a series of potentialities and challenges requiring a new posture on the part of these institutions and the professionals linked to them, especially librarians. It emphasizes that studies on this subject are still incipient.

KEYWORDS: Artificial Intelligence. University Library. Innovation in Libraries.

1 | INTRODUÇÃO

Muito se tem discutido, ao longo das últimas décadas, a ampla utilização das

Tecnologias da Informação e Comunicação – TIC[1], no contexto do ensino superior e, em especial, nas Bibliotecas universitárias. Indiscutivelmente, as TIC impactam diretamente nos processos de geração, tratamento e disseminação da informação, além do aumento exponencial no consumo de produtos e serviços de informação, alterando inclusive a compreensão de tempo e espaço que a biblioteca universitária tem oferecido.

Corroboram Andrade e Santos (2021) ao afirmarem que a revolução tecnológica conduziu o desenvolvimento da área de comunicação e gerenciamento de dados e informações gerando um volume de conhecimento sem precedentes na história. Em nenhuma outra época, segundo os autores, a produção e registo do conhecimento foram tão intensas como nos dias de hoje, como também em nenhuma outra época a sua aplicação assumiu papel tão preponderante.

Logo, viver na sociedade atual significa conviver com abundância e diversidade de informações, e a tecnologia é o instrumento que facilita o acesso a esse universo informacional amplo e complexo, bem como a seu uso para o acesso ao local e a distância dessas comunidades. E, a biblioteca universitária enquanto instância que possibilita à universidade atender às necessidades informacionais da comunidade acadêmica e da sociedade em geral, através do exercício de função educativa, ao orientar os usuários na utilização da informação, pode desempenhar papel preponderante no acesso amplo ao conhecimento que seja realmente útil em cada um dos contextos que se fizer necessário. (*op. cit.,* 2021)

Como consequência dos avanços tecnológicos, pode-se afirmar que a inteligência artificial (IA) é uma das mais recentes tendências tecnológicas de transformação digital que a biblioteca universitária pode se apropriar no sentido de agregar valor aos produtos e serviços ofertados, ou, dentro de um processo inovativo, oferecer novos serviços. Interessante como um *chatbot*, por exemplo, poderia remotamente simular uma conversa com um usuário como se fosse um ser humano, de forma que uma abordagem inicial seja mais prática e não deixe a impressão de estar falando com o robô, uma máquina. Ou explorar a potencialidade da IA para dar suporte às decisões para tratamento, recuperação e compartilhamento de informações voltadas para aprendizado para o desenvolvimento de coleções, ensino e pesquisa.

No entanto, a literatura existente demonstra uma baixa taxa de adoção pelas bibliotecas universitárias no uso de IA para fornecer produtos e serviços inovadores, agregar maior valor aos já existentes na Biblioteca, além de fomentar uma aprendizagem em rede com o foco em processos colaborativos de aprendizagem. (Adetayo, 2023). Percebe-se então uma lacuna a ser estudada.

Neste sentido, importante se faz necessário identificar os estudos sobre a aplicação

1 A terminologia Tecnologias de Informação e Comunicação (TIC), especificamente, envolve a aquisição, o armazenamento, o processamento e a distribuição da informação por meios eletrônicos e digitais, como rádio, televisão, telefone e computadores, entre outros. Resultou da fusão das tecnologias de informação, antes referenciadas como informática, e as tecnologias de comunicação, relativas às telecomunicações e mídia eletrônica (PRETTO, 2008).

da Inteligência artificial no contexto das Bibliotecas Universitárias. Para tanto, o presente trabalho procura identificar trabalhos relacionados à temática na próxima seção, descreve a revisão de literatura como princípio metodológico na seção 2; destaca resultados e primeiras discussões sobre o tema na seção 3, seguindo-se das primeiras aproximações ao final.

1.1 Fundamentação teórica e estudos relacionados

O termo "inteligência artificial" representa um software diferente dos demais, pois é inteligente e visa fazer os computadores realizarem funções que eram exclusivamente dos seres humanos, por exemplo, praticar a linguagem escrita ou falada, aprender, reconhecer expressões faciais, etc. Corroboram Silva; Lens; Freitas (2018) ao afirmarem que:

> [...]o termo "inteligência artificial" refere-se à capacidade de uma máquina digital executar tarefas comumente associadas a seres inteligentes, e suas tecnologias associadas são divididas em vários ramos, como visão computacional, fala, aprendizado de máquina, big data e processamento de linguagem natural. (p. 37)

A Inteligência Artificial (IA) pode ser amplamente entendida como o estudo de sistemas que atuam de maneira que, para um observador externo, aparentam ser inteligentes. O principal objetivo desses sistemas é executar tarefas que, se realizadas por humanos, seriam consideradas como demonstrando inteligência. Entre as capacidades-chave dos sistemas de IA, destacam-se:

- **Raciocínio**: a habilidade de aplicar regras lógicas a um conjunto de dados disponíveis para chegar a uma resposta.
- **Aprendizado**: a capacidade de aprender com os dados, ajustando-se com base em erros e acertos para melhorar seu desempenho futuro.
- **Reconhecimento de padrões**: identificar padrões visuais, sensoriais e comportamentais, permitindo uma melhor compreensão e resposta a diferentes situações.

As categorizações da inteligência artificial auxiliam a compreender seu grau de desenvolvimento. De forma geral, qualquer produto derivado de uma aplicação de IA pode ser classificado em três grandes categorias:

- **Inteligência Artificial Fraca** - uma corrente de pesquisa e desenvolvimento que defende que nunca será possível construir máquinas inteligentes no real sentido da palavra, pois inteligência demanda consciência e autopercepção, habilidades impossíveis de serem recriadas. Tudo que se pode fazer envolve imitar comportamentos inteligentes e emoções, bem como resolver problemas, mas nunca a consciência... um motor de inferência, *chatbot* por exemplo, nada mais é do que um vários *if-them* encadeados

- **Inteligência artificial forte** - acredita que um dia será possível recriar máquinas capazes de pensar, criar e exibir comportamento inteligente nos moldes humanos, a partir da criação de algoritmos cognitivos que possam executar em computadores.
- **Superinteligência** - Termo estabelecido por Nick Bostrom como "um intelecto que é muito mais inteligente do que o melhor cérebro humano em praticamente todas as áreas, incluindo criatividade científica, conhecimentos gerais e habilidades sociais" (Rosa, 2011)

Principais questões a serem contornadas pelo projetista do sistema de inteligência artificial são aquisição, representação e manipulação de conhecimento e, geralmente, uma estratégia de controle ou a máquina de inferência que determina os itens de conhecimento acessados, as deduções feitas e a ordem dos passos usados. Tal como representando no modelo a seguir:

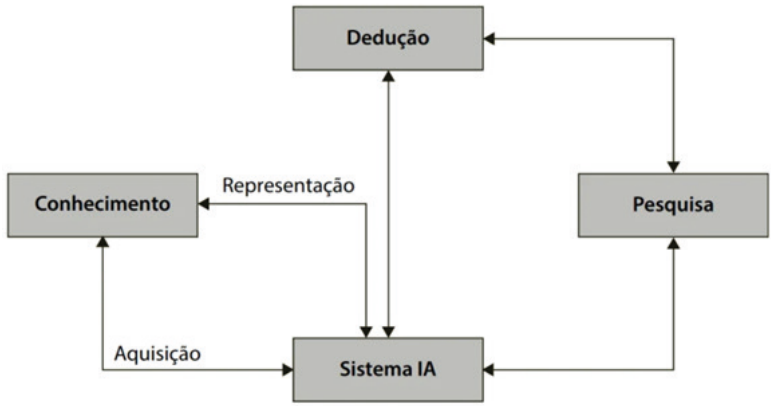


Figura 1: Visão conceitual dos sistemas baseados em inteligência artificial

Fonte: adaptada de Russel; Norvig (2003)

Os sistemas de Inteligência Artificial (IA) não se limitam apenas a armazenar e manipular dados, mas também são capazes de adquirir, representar e utilizar o conhecimento de maneira sofisticada. A IA abrange várias áreas, como:

- **Machine Learning**: Algoritmos que utilizam dados passados para identificar padrões e tomar decisões. Um subcampo importante é o **Deep Learning**, que envolve redes neurais profundas.
- **Redes Neurais**: Modelos matemáticos inspirados na estrutura dos neurônios humanos, capazes de aprender com a experiência e adquirir conhecimento ao longo do tempo.
- **Visão Computacional**: Sistemas que reproduzem a visão humana por meio de softwares e/ou hardwares, permitindo a interpretação visual de imagens e vídeos.

- **Sistemas Cognitivos**: Softwares que simulam o processo de aprendizado humano, agindo, identificando, deduzindo e compreendendo com base em dados. Exemplos incluem o Watson da IBM, Siri, Alexa e Cortana.
- **Processamento de Linguagem Natural (NLP)**: Tecnologias que permitem que sistemas compreendam e interpretem a fala e a escrita humanas. Exemplos incluem tradutores em tempo real, chatbots, análise de sentimentos e detecção de spam em e-mails.
- **Robótica**: Integra a IA em dispositivos físicos, como carros autônomos, drones e aspiradores de pó autônomos.

A Inteligência Artificial pode ser compreendida por meio de uma taxonomia, figura 2, que descreve suas ramificações e possibilidades. Nessa estrutura hierárquica, a IA é dividida em vários ramos, como aprendizado de máquina (ML), processamento de linguagem natural, sistemas especialistas, entre outros. O ramo de aprendizado de máquina (ML), por sua vez, é subdividido em áreas como Análise Preditiva e Deep Learning.

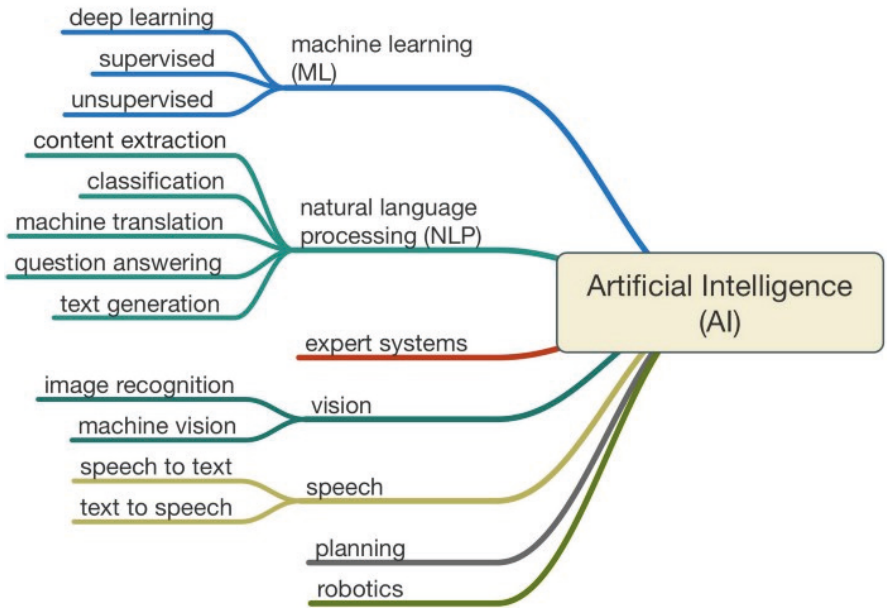


Figura 2: Taxonomia de Inteligência Artificial

Fonte: Adaptado de adaptada de Russel; Norvig (2003)

Todos esses ramos têm em comum o processamento de big data, utilizando algoritmos de aprendizado de máquina como o núcleo de sua proposta de valor. Eles atuam em campos tradicionalmente ligados à IA, como reconhecimento de padrões em vídeos, imagens e dados visuais, otimização do desempenho de algoritmos, processamento de grandes volumes de dados textuais para extrair insights ou gerar novos textos, análise de dados genéticos e criação de robôs.

A Inteligência Artificial está presente em nosso cotidiano e é amplamente utilizada na indústria, em jogos eletrônicos, em automóveis e em diversos dispositivos. Além de ser uma ferramenta valiosa em muitos sistemas computacionais, a IA também abre inúmeras possibilidades quando aplicada no contexto das bibliotecas universitárias.

De maneira geral, conforme identificado na literatura, o ciclo para aplicação da IA pelas organizações funciona da seguinte forma: quando uma organização desenvolve um produto ou serviço de qualidade satisfatória, ela consegue atrair usuários iniciais. Esses usuários, ao utilizarem o produto ou serviço, geram dados que são coletados e armazenados pela organização. Se esses dados forem tratados adequadamente com técnicas de Inteligência Artificial, especialmente Machine Learning, isso permitirá a melhoria do produto ou serviço. Com o aperfeiçoamento, a organização conseguirá atrair ainda mais usuários. Mais usuários resultarão em mais dados, e a maior quantidade de dados levará a melhorias contínuas no produto ou serviço, criando um ciclo que se repete. A cada iteração, o produto ou serviço se torna cada vez melhor, enquanto a organização conquista um número crescente de usuários.

Entretanto, em relação às Bibliotecas Universitárias, percebe-se que uma das mais profundas e indispensáveis mudanças no que tange ao papel destas instituições é a transferência do foco nos acervos para o foco no usuário e em seu comportamento que conduzam à autonomia em direção ao letramento informacional.

Demonstrando que poucos são os estudos científicos relacionados aos contextos de avaliação sobre a usabilidade destes portais e serviços virtuais ofertados por um Sistema de Bibliotecas Universitárias com foco na autonomia do usuário, bem como a falta de divulgação de trabalhos relacionados e experiências institucionais sobre este tipo de análise, dentre outras ponderações.

2 | PRINCÍPIOS METODOLÓGICOS

A presente pesquisa se inscreve no quadro das pesquisas qualitativas com objetivos exploratórios e descritivos, pois se tem a pretensão de investigar, analisar, refletir e interpretar a realidade à medida que se procure entendê-la. Este trabalho se caracteriza como uma pesquisa do tipo “estado da arte” que visa identificar, mapear e analisar os trabalhos sobre a utilização aplicação da Inteligência Artificial em produtos e serviços para Bibliotecas Universitárias.

Romanowski; Ens (2006) destacam que as pesquisas do tipo estado da arte:

> [...] são justificadas por possibilitarem uma visão geral do que vem sendo produzido na área e uma ordenação que permite aos interessados perceberem a evolução das pesquisas na área, bem como suas características e foco, além de identificar as lacunas ainda existentes (p. 41)

Para tanto, buscou-se organizar a revisão de literatura em quatro etapas: Identificação do Repositório de Informação; Definição das estratégias de Busca e Recuperação da

Informação; Classificação e extração dos dados; e Análise e categorização dos artigos.

Na primeira etapa, foi feita a opção Portal de Periódicos da CAPES como principal (e único) repositório de informações, pois este se caracteriza como uma biblioteca virtual que congrega a produção científica nacional e internacional. Disponibiliza um acervo de mais de 39 mil títulos com texto completo, 396 bases referenciais, 13 bases dedicadas exclusivamente a patentes, além de livros, enciclopédias e obras de referência, normas técnicas, estatísticas e conteúdo audiovisual[2].

2.1 Estratégias de Busca e Recuperação da Informação

Para selecionar os artigos científicos, utilizou-se, enquanto estratégia de busca, os descritores "**INTELIGÊNCIA ARTIFICIAL**" *or* (ou) "**Artificial Intelligence**" *and* (e) "**University library**", na interface de busca avançada do Portal Capes, tendo como recorte temporal o período de 2018 a 2023 – últimos 5 anos.

A busca foi direcionada para o campo "assunto" que contivesse os termos destacados acima.

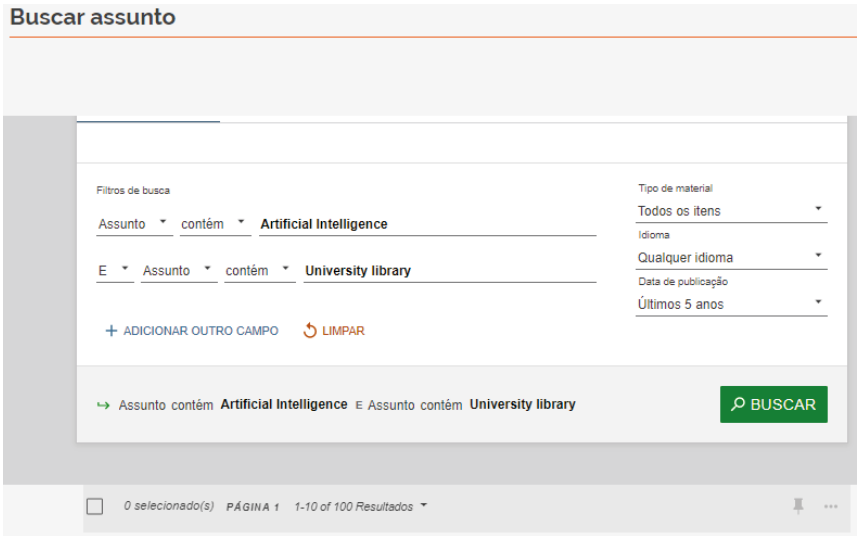


Figura 3 – Modelo da interface de busca avançada do Portal Capes

Fonte: os autores

Importante ressaltar que se optou pelos descritores na língua inglesa uma vez que a grande maioria das bases de dados que integram o Portal de Periódicos da Capes são internacionais. Inclusive, o próprio Portal recomenda que sejam utilizados termos em inglês considerando que a literatura científica é, em sua maioria, publicada em inglês, aumentando

2 PORTAL DE PERIÓDICOS: missão e objetivos. Disponível em: www.periodicos.capes.gov.br. Acesso em: 25 maio 2023.

a recuperação da informação. Não havendo, entretanto, restrição a outros idiomas.

As estratégias de busca adotadas na fase inicial deste mapeamento são fundamentais para o andamento pesquisa considerando que uma estratégia inconsistente pode trazer um grande número de trabalhos e possivelmente a pesquisa poderia ter outro direcionamento.

Os critérios utilizados para a seleção dos artigos permitiram refinar a busca e recuperar os estudos relevantes e pertinentes ao objeto da pesquisa sendo descartados os demais itens coletados. Não foram observados os itens duplicados.

2.2 Classificação e extração dos dados

Neste primeiro recorte, foram obtidos 101 artigos, distribuídos em 14 bases de dados. Em seguida, novos filtros e critérios de busca foram adotados para aumentar a precisão e a granularidade dos resultados. Para tal, foram selecionados os artigos revisados por pares, escritos em português, inglês ou espanhol que estivessem com os textos completos disponíveis, chegando ao quantitativo de 38 artigos conforme ilustrado no gráfico 1, a seguir:

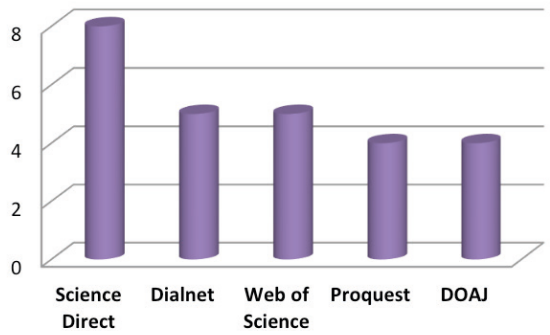


Gráfico 1: Recuperação da Informação das publicações por base de dados (maio/2023)

A base de dados "DOAJ" apresentou o resultado mais significativo (31%) em relação à quantidade de artigos recuperados, seguida das bases "Ovid" (18%), "Springer", "PubMed" e "Web of Science" (16% cada). Os resultados justificam-se uma vez que as bases listadas são de caráter multidisciplinar que abrangem trabalhos voltados para as áreas de Educação, Tecnologia Educacional, além de agregar artigos de periódicos relevantes nas áreas de Ciência da Computação e Tecnologias Emergentes.

Quando esses artigos são examinados em termos de seu alcance, tanto em relação às bases de dados, aos autores e aos títulos dos periódicos identificados, pode-se notar que eles abordaram diferentes aspectos da pesquisa Inteligência Artificial mesmo estando a busca restrita à Biblioteca Universitárias, fato que limita a comparação e padronização dos resultados.

3 | RESULTADOS E DISCUSSÕES: PRIMEIRAS APROXIMAÇÕES

Numa primeira análise, pode-se verificar que a maioria dos trabalhos sobre Inteligência Artificial está relacionada com os assuntos “produtos e serviços” e “modelos de aplicação”. Nota-se ainda que as instituições percebem a Inteligência Artificial como uma oportunidade, um novo “modelo de negócios” que exige adaptação das abordagens biblioteconômicas existentes, além dos processos de formação – inicial e continuada – dos bibliotecários.

Embora a IA esteja longe de se fazer presente nas bibliotecas no contexto atual, algumas Universidade e, consequentemente, suas bibliotecas tem apoiado iniciativas sobre o tema. Até por se tratar com um tema emergente e emergente para o desenvolvimento de aplicações e soluções baseadas em tecnologias no atual contexto das bibliotecas universitárias.

Percebe-se que a inteligência artificial pode transformar significativamente o ambiente das bibliotecas universitárias, automatizando processos e oferecendo novos serviços aos usuários. A revisão bibliográfica, ora desenvolvida, aponta que uma das principais aplicações da IA nesse contexto é a automação de tarefas rotineiras, como a catalogação e indexação de materiais, permitindo maior eficiência e precisão na organização dos acervos. Ferramentas de IA são capazes de analisar grandes volumes de dados rapidamente, proporcionando uma catalogação mais rápida e consistente, além de facilitar a recuperação da informação por parte dos estudantes e pesquisadores.

Um dos usos mais comuns identificados nos artigos mapeados são os *chatbots* de referência que usam aprendizado de máquina, conforme descrito no item 1.1, para fornecer aos usuários respostas a perguntas simples.

Como exemplo, pode-se destacar o *ChatGPT* (*chat generative pretrained transformer*) – que se constitui como chatbot “treinado” com textos disponíveis na internet e retroalimentado com suas interações com os usuários – pode oferecer respostas mais relevantes. Ele poderá, por exemplo, “orientar os usuários pelo site da biblioteca e até mesmo auxiliar nas pesquisas”. Podendo auxiliar na “referência, desenvolvimento de coleções e catalogação”. Mas apesar de oferecer respostas com maior qualidade, por ter acesso a uma quantidade maior de informações, estes tipos de chatbot também podem errar, e por suas respostas serem mais elaboradas, o usuário poderá não perceber (ADETAYO, 2023, tradução nossa).

Além disso, a IA pode otimizar o atendimento ao usuário nas bibliotecas universitárias. Assistentes virtuais e chatbots, baseados em processamento de linguagem natural, podem responder a perguntas frequentes e fornecer orientação sobre o uso de recursos bibliográficos, contribuindo para uma experiência mais acessível e personalizada. Isso permite que os bibliotecários se concentrem em tarefas mais complexas, como a curadoria de conteúdo especializado e o apoio a projetos de pesquisa avançados.

Assim, é importante lembrar que neste momento a inteligência artificial ainda precisa de acompanhamento humano para oferecer produtos e serviços de qualidade. Sendo assim, ela deve ser usada como um auxiliar ao trabalho humano.

Ao considerar a Biblioteca Universitária, é essencial levar em conta tanto a compreensão quanto a construção do conhecimento, além dos novos modelos de suporte informacional. A Inteligência Artificial (IA) promove uma ruptura significativa, abrindo diversas possibilidades para a oferta de novos produtos e serviços, bem como para a readequação dos já existentes nas bibliotecas. Na área da Biblioteconomia, é particularmente importante compreender não apenas o potencial da IA, mas também suas limitações. Essas tecnologias, por si só, não são suficientes para gerar mudanças transformadoras ou produzir conhecimento que resulte em aprendizagens significativas.

Em relação aos softwares de automação de Bibliotecas e Serviços de Informação, os recursos baseados em IA podem contribuir significativamente na análise e recomendação de conteúdos personalizados. Com base no histórico de pesquisa e comportamento de leitura dos usuários, algoritmos de machine learning podem sugerir materiais acadêmicos relevantes, artigos científicos ou livros, otimizando o processo de descoberta de informação. Isso não só melhora a experiência dos usuários, como também fortalece o papel das bibliotecas universitárias como facilitadoras de inovação e produção de conhecimento.

Nesse contexto, a celeridade é mais importante do que a alta qualidade no lançamento de produtos e serviços baseados em Inteligência Artificial. A rapidez é essencial para entrar no ciclo virtuoso, iniciando a jornada de iteração com os usuários, coletando e armazenando dados que serão utilizados para o aperfeiçoamento dos produtos e serviços já existentes na Biblioteca Universitária, sempre com base na identificação das necessidades dos usuários.

Outro ponto relevante é que o produto ou serviço deve ser concebido desde o início para ser habilitado para a coleta de dados. Isso precisa ser parte integrante do planejamento, que deve incluir respostas a questões como: Quais dados queremos obter? Como conseguiremos esses dados? Como iremos armazená-los? O que faremos com esses dados? Como imaginamos que o produto possa ser aprimorado com essas informações?

Portanto, o uso de recursos tecnológicos na mediação do conteúdo, embora importante, não garante o acesso pleno à informação. O foco deve estar no desenvolvimento de estratégias inovadoras que capacitem os profissionais a selecionar criticamente as informações mais relevantes para a construção de saberes, garantindo que as bibliotecas universitárias desempenhem um papel central na formação acadêmica.

4 | CONSIDERAÇÕES FINAIS

Destaca-se que a partir deste estudo, será possível identificar oportunidades além de desencadear uma Revisão sistemática da Literatura que conduzirá à categorização dos estudos desenvolvidos sobre Inteligência Artificial aplicada no contexto das Bibliotecas

Universitárias.

À medida que os aplicativos de inteligência artificial continuam a crescer no futuro, as bibliotecas precisam estar na vanguarda das mudanças que trarão. O objetivo deste projeto de pesquisa foi investigar as percepções e atitudes de bibliotecários em relação à inteligência artificial e, em pequena medida, aos assistentes virtuais. As descobertas trazem à tona a importância de desenvolver uma compreensão da IA dentro da profissão e a urgência de os bibliotecários educarem a si mesmos e a seus patronos sobre essa tecnologia. A inteligência artificial trará mudanças em todas as profissões e, embora os bibliotecários não pareçam preocupados que ela possa substituir seus cargos, ela pode muito bem mudar a maneira como trabalhamos para sempre.

Conforme as tecnologias que dão suporte às aplicações baseadas em IA, as pesquisas voltadas para as Bibliotecas Universitárias devem ser intensificadas na direção de investigar novas oportunidades e possibilidades que honrem princípios de da autonomia dos usuários, a aprendizagem autêntica, colaborativa e personalizada. Acredita-se que estudos similares a este podem fomentar "insights" críticos que apoiem e sustentem as possibilidades e o design de aplicações e recursos de voltados especificamente para as Bibliotecas Universitárias.

REFERÊNCIAS

ADETAYO, A. J. Artificial intelligence chatbots in academic libraries: the rise of ChatGPT**. Library Hi Tech News**, [S. l.], n. 3, p. 18–21, 2023. Disponível em: https://www-periodicos-capes-gov-br.ez24.periodicos.capes.gov.br/. Acesso 27 maio 2023

ANDRADE, M. V. M. Considerações sobre a cibercultura e a aplicação das tecnologias da informação e comunicação nos processos educativos. In: JORGE, W. J. (org). **Educação presencial a distância**: desafios e reflexões. Maringá (PR): Uniedusul, 2020. p. 23-52. Disponível em: https://app.uff.br/riuff/handle/1/22399

ANDRADE, M. V. M., SANTOS, A. R. Aplicação da gestão estratégica no contexto das bibliotecas universitárias: primeiras aproximações. In: **Ciências sociais aplicadas**: Desafios metodológicos e resultados empíricos. Ponta Grossa (PR): Atena Editora, 2021, p. 66-80.

ANDRADE, M. V. M.; SANTOS, A. R. Tendências da aplicação da inteligência artificial na Biblioteca Universitária: primeiras aproximações. In: Seminário Nacional de Bibliotecas Universitárias, 2023, Florianópolis. **Anais do 22º Seminário Nacional de Bibliotecas Universitárias (SNBU)**. Florianópolis: UFSC, 2023. Disponível em: https://portal.febab.org.br/snbu2023/article/view/2837/2813. Acesso em: 08 out. 2024.

EHRENPREIS, M.; DELOOPER, J. Implementing a Chatbot on a Library Website. **Journal of Web Librarianship**, [S. l.], v. 16, n. 2, p. 120–142, 2022. Disponível em: https://doi.org/10.1080/19322909.2022.2060893. Acesso 27 maio 2023.

LAKATOS, E. M.; MARCONI, M. de A. **Metodologia científica**. 6. ed. São Paulo: Atlas, 2011.

LUGER, G. Artificial **Intelligence**: Structures and Strategies for Complex Problem Solving. Addison-Wesley Pub Co, 2008.

PRETTO, N. L. **Além das redes de colaboração**: internet, diversidade cultural e tecnologias do poder. Salvador: EDUFBA, 2008.

ROMANOWSKI, J. P. ; ENS, R. T. As pesquisas denominadas do tipo “estado da arte” em educação. **Diálogo Educ**., Curitiba, v. 6, n. 19, 2006. p. 37-50. Disponível em: www.scielo.br/pdf/es/v23n79/10857.pdf

ROSA, J. L. G. **Fundamentos da Inteligência Artificial**, LTC, 2011.

RUSSEL, S.; NORVIG, P. **Inteligência Artificial**, Ed. Campus, 2003.

SILVA, F. M.; LENZ, M. L.; FREITAS, P. H C. **Inteligência artificial**. São Paulo: Grupo A, 2018.

FABRÍCIO MORAES DE ALMEIDA - É Doutor em Física pela UFC (2005) e Líder do grupo de pesquisa GEITEC/UFRO. Além disso, tem mais de 25 anos de experiência com Pesquisas Científicas/Consultorias, Gestão de Ciência e da Tecnologia. E para saber mais, acesse: http://lattes.cnpq.br/5959143194142131.

ÍNDICE REMISSIVO

ÍNDICE REMISSIVO

CIÊNCIA E TECNOLOGIA

CATALISADORES DA INOVAÇÃO 3

www.atenaeditora.com.br
contato@atenaeditora.com.br
@atenaeditora
www.facebook.com/atenaeditora.com.br

Atena Editora
Ano 2024

CIÊNCIA E TECNOLOGIA

CATALISADORES DA INOVAÇÃO 3

www.atenaeditora.com.br
contato@atenaeditora.com.br
@atenaeditora
www.facebook.com/atenaeditora.com.br

Atena Editora
Ano 2024