

Iniciativas de Ensino das Tecnologias Digitais de Informação e Comunicação e Segurança Cibernética na Educação Básica

Eduardo H. Teixeira^{1,2}, Ítalo A. de S. Tacca¹, Patrícia G. da Silva²,
Guilherme P. Aquino¹, Evandro C. Vilas Boas¹

¹Centro de Segurança Cibernética (CxSC Telecom)
Instituto Nacional de Telecomunicações (Inatel)
Caixa Postal 37540-000 – Santa Rita do Sapucaí – MG – Brazil

²Programa de Pós-Graduação em Ensino Profissional e Tecnológico (PPG EPT)
Instituto Federal do Rio de Janeiro (IFRJ)
Caixa Postal 17250-000 – Rio de Janeiro – RJ – Brasil

{eduardo.teixeira, italo.augusto, guilhermeaquino, evandro.cesar}@inatel.br,
patricia.grasel@ifrj.edu.br

Abstract. *This paper describes the development of courses on Digital Information and Communication Technologies (TDICs) and cybersecurity, developed by the Cybersecurity Center of the Inatel. With the rapid advance of TDICs, it has become essential to understand the operation and principles of these technologies to enable human resources to develop safer systems. Courses developed and applied, covering areas such as computer networks, telephony, internet of things, network management and cybersecurity, providing an understanding of fundamentals and practical applications. The paper also highlights the importance of systems and data protection, in addition to discussing the contributions of DICTs in the educational context.*

Resumo. *Este artigo descreve a elaboração de cursos sobre Tecnologias Digitais de Informação e Comunicação (TDICs) e segurança cibernética, desenvolvidos pelo Centro de Segurança Cibernética do Inatel. Com o rápido avanço das TDICs, tornou-se fundamental compreender o funcionamento e os princípios dessas tecnologias para capacitar recursos humanos no desenvolvimento de sistemas mais seguros. Os cursos desenvolvidos e aplicados, abrangem áreas como redes de computadores, telefonia, internet das coisas, gerenciamento de rede e segurança cibernética, fornecendo uma compreensão dos fundamentos e aplicações práticas. O artigo também destaca a importância da proteção de sistemas e dados, além de discutir as contribuições das TDICs no contexto educacional.*

1. Introdução

Os avanços tecnológicos e o uso das Tecnologias Digitais de Informação e Comunicação (TDICs) têm transformado a forma como a sociedade se comunica. No entanto, esse aumento no uso de novas tecnologias também está acompanhado por um crescente número de ameaças e ataques cibernéticos em todo o mundo. Em 2021, estimou-se que os crimes cibernéticos tenham causado prejuízos econômicos superiores a 6 trilhões de dólares, afetando desde grandes corporações até instituições de ensino [Damaševičius et al. 2021].

Diante dessa realidade, a proteção de sistemas e dados tornou-se uma prioridade fundamental [Chinedu et al. 2021].

Este artigo tem como objetivo explorar em detalhes a iniciativa do Instituto Nacional de Telecomunicações (Inatel) no ensino das TDICs e segurança cibernética, áreas essenciais para que os alunos possam atuar futuramente no desenvolvimento de sistemas mais seguros e na prevenção ou mitigação de ataques cibernéticos. Para capacitar os alunos em desempenhar tais tarefas, é necessário que eles compreendam o funcionamento e os princípios dessas tecnologias. Com base nessa premissa, o Inatel, por meio do Centro de Segurança Cibernética do Inatel (CxSC Telecom), desenvolveu uma série de cursos direcionados a estudantes da educação básica, especialmente de escolas de nível médio e médio/técnico.

A elaboração de cursos didáticos requer uma abordagem cuidadosa para garantir que os conteúdos sejam relevantes e atendam aos objetivos educacionais [Molenda 2015]. Com o intuito de ensinar os princípios e demonstrar o funcionamento das tecnologias por trás das TDICs, elaboraram-se os cursos utilizando uma combinação de atividades teóricas, práticas, de pesquisa e extensão. Para isso, foi adotado o modelo ADDIE (*Analysis, Design, Development, Implementation, and Evaluation*) durante a criação e desenvolvimento dos cursos. Esse modelo é amplamente utilizado no campo da educação e fornece uma estrutura sistemática para a concepção e implementação de programas educacionais eficazes [Molenda 2003].

Nos cursos desenvolvidos, exploraram-se conceitos como redes de computadores, telefonia, Internet das coisas, gerenciamento de rede e segurança cibernética. Essas áreas são fundamentais dentro do contexto das TDICs e formação de futuros profissionais, preparando-os para os desafios e oportunidades de suas áreas em um ambiente de convergência tecnológica. Dessa forma, a iniciativa proporciona uma compreensão aprofundada das TDICs aos alunos, incluindo princípios básicos e aplicações práticas para teste de hipóteses com acompanhamento e orientação de professores com base em metodologias para buscar soluções.

Nesse artigo, descrevem-se todos os cursos ministrados dentro de espectro proposto. A discussão está organizada em cinco seções. Na Seção 2, apresenta-se a importância de compreender os conceitos de operação e funcionamento das TDICs, abordando a metodologia de ensino utilizada e os recursos empregados nos cursos. Na Seção 3, discute-se cada curso desenvolvido sobre a óptica de fatores como o número de alunos, a abordagem didática e as atividades práticas. Na seção 4, apresentam-se conclusões e apontam-se trabalhos futuros.

2. Metodologia da Exploração dos Conteúdos

Nesta seção, discute-se a importância de compreender o funcionamento das TDICs e os princípios de segurança cibernética no contexto educacional. Além disso, a metodologia adotada na elaboração dos cursos é apresentada com destaque para o uso de recursos tecnológicos e estratégias pedagógicas que estimulam a participação ativa dos alunos.

A evolução exponencial das TDICs molda a comunicação e interação entre pessoas, trazendo inúmeros benefícios para a sociedade. Entretanto, a exposição digital traz novos desafios relacionados à segurança cibernética que transcendem aqueles relacionados a segurança física. Compreender o funcionamento dessas tecnologias é fundamental

para que educadores e alunos possam explorar seu potencial máximo no ambiente educacional, contribuindo para a formação de jovens digitalmente conscientes.

Os cursos desenvolvidos pelo CxSC Telecom foram elaborados com base em uma metodologia abrangente por meio da união de conceitos teóricos, princípios das TDICs, ferramentas computacionais e equipamentos. As aulas foram ministradas com o uso de recursos tecnológicos físicos e virtuais, como equipamentos de redes e telefonia, programas de computadores capazes de simular o gerenciamento de redes e dispositivos, além de interfaces de desenvolvimento que permitiram aos alunos projetar e programar seus próprios sistemas.

A integração entre teoria e prática permite aos alunos aplicar aprendizados conceituais de forma tangível. Por meio de simulações e experimentações práticas, os participantes validaram os conceitos discutidos em sala de aula, desenvolveram habilidades técnicas e adquiriram experiências em todas as áreas abordadas nos cursos. Foram aplicados alguns preceitos da aprendizagem ativa, onde o aluno atua como agente central do seu próprio processo de aprendizagem, incentivando sua participação ativa nas atividades propostas. O uso de recursos tecnológicos trouxe benefícios significativos ao longo do aprendizado em TDICs e segurança cibernética. Oportunamente, os alunos experimentaram um ambiente propício ao aprendizado ao trabalhar em projetos práticos, desenvolvendo soluções concretas e aprimorando suas habilidades de resolução de problemas.

A abordagem adotada nos cursos ofereceu aos alunos uma experiência completa, preparando-os para enfrentar os desafios do mercado de trabalho e fornecendo uma base sólida para sua atuação futura no desenvolvimento de sistemas seguros e na prevenção de ataques cibernéticos. Com isso, os alunos foram estimulados a um nível maior de pensamento crítico, o que facilita a retenção de conhecimento [Pedaste et al. 2023]. Ao explorar a importância de compreender o funcionamento das TDICs e os princípios de segurança cibernética, bem como apresentar a metodologia inovadora que integra conceitos teóricos, ferramentas computacionais e equipamentos, esta seção forneceu uma visão abrangente da abordagem adotada nos cursos desenvolvidos pelo CxSC Telecom do Inatel.

3. Desenvolvimento e Detalhamento da Aplicação dos Cursos

Compreendendo a importância de explorar as TDICs em ambiente educacional e tecnológico, foram desenvolvidos cursos que visam aprofundar o conhecimento sobre o funcionamento dessas tecnologias. Nesse contexto, abordaram-se temas como o ecossistema de redes de computadores, telefonia analógica e *Voice over IP* (VoIP), redes de transporte de dados em hierarquia digital síncrona (*Synchronous Digital Hierarchy*, SDH) e óptica através da multiplexação por divisão de comprimentos de onda (*Wavelength Division Multiplexing*, WDM), conceitos, protocolos e aplicações dentro do ambiente de Internet das Coisas (*Internet of Things*, IoT), introdução ao gerenciamento de rede com Python e Python aplicado à segurança cibernética. Cada curso possui um foco específico, proporcionando aos alunos uma compreensão adequada de parte das TDICs e suas aplicações práticas em um ambiente educacional e tecnológico.

3.1. Telefonia Analógica e VoIP

O curso sobre telefonia analógica e VoIP foi ministrado para 16 alunos organizados em duplas, e objetivou a difusão de conhecimento sobre tecnologias telefônicas e o desper-

tar do interesse pela área de tecnologia e telecomunicações. Na introdução, a história da telefonia fixa foi apresentada como forma de contextualização, incluindo a invenção, a implementação no Brasil e a evolução tecnológica até os dias atuais. Em seguida, apresentaram-se às redes de telefonia analógicas, descrevendo os elementos de rede. As práticas posteriores foram realizadas em laboratório utilizando uma rede de telefonia analógica com duas centrais telefônicas e oito aparelhos telefônicos. Os alunos foram instruídos em configurar os equipamentos para estabelecer chamadas locais e remotas, também conhecidas como interurbanas. Ao fim da atividade, os alunos foram capazes de montar a rede telefônica da maneira esperada, e realizaram testes de chamadas locais e interurbanas entre suas bancadas em um experimento lúdico.

Com a parte analógica do curso concluída, os alunos foram apresentados às tecnologias modernas de VoIP, utilizadas para o estabelecimento de chamadas telefônicas em redes privadas empresariais e em redes de telefonia móvel [Goode 2002]. De forma análoga, os alunos implementaram uma rede de telefonia VoIP capaz de estabelecer chamadas locais e remotas com o auxílio das duas centrais telefônicas e oito telefones IP. Novamente, as duplas concluíram a atividade e comprovaram as funcionalidades da rede por meio de experimentos lúdicos de chamadas telefônicas.

3.2. Tecnologias de Redes de Transporte de Dados SDH e WDM

O curso de rede de transporte de dados em tecnologias SDH e DWDM foi ministrado para 16 alunos, difundindo conhecimentos sobre telecomunicações para provocar o despertar de interesse pela área de tecnologia. Inicialmente, os alunos foram introduzidos à história das redes de transporte de tráfego de telecomunicações e como as tecnologias habilitadoras evoluíram para se adaptarem à transição da era do tráfego telefônico analógico até o século XXI com o tráfego de dados da Internet. Em seguida, os alunos foram introduzidos às tecnologias SDH e DWDM, assim como às suas características, vantagens e cenários de uso [Dolma and Kiraz 2018, Alwayn 2004].

Iniciou-se, portanto, a fase prática do curso, na qual os alunos foram instruídos a implementarem redes SDH e DWDM por meio de enlaces de fibra óptica conectados a equipamentos apropriados para esse fim e dispostos em laboratório. Como resultado, os alunos foram capazes de estabelecer os enlaces ópticos propostos e de fazer o transporte de tráfegos telefônico e *Ethernet* por meio dos enlaces, simulando o que acontece em extensas redes de telecomunicações entre dois municípios. Observou-se que a prática em laboratório resultou em bom engajamento para cumprir com a proposta em configuração de equipamentos e manuseio de conexões ópticas.

3.3. Ecossistema de Redes de Computadores

No curso de Ecossistema de Redes de Computadores, um público de 20 alunos foi apresentado às principais tecnologias envolvidas no processo de envio e recepção de dados na Internet. O curso objetivou a difusão de conhecimento sobre Redes de Computadores, assim como o despertar do interesse dos alunos por essa área das telecomunicações. Em um primeiro momento, definiu-se para os alunos o que são Redes de Computadores e como as identificar em diferentes cenários. Em seguida apresentaram-se elementos básicos e suas configurações para constituir uma rede, incluindo dispositivos finais, comutadores de quadros, roteadores e pontos de acesso sem fio.

Por fim, orientou-se a utilização de um programa de simulação de Redes de Computadores, com o qual os alunos puderam montar algumas topologias de rede propostas e testar os conceitos aprendidos. As topologias propostas incluíram desde redes simples com dois ou três computadores, até redes mais complexas com diversos roteadores e pontos de acesso sem fio. Como resultado, os alunos foram capazes de montar as topologias através de simulação, demonstrando facilidade na configuração dos elementos e engajamento na atividade ao interagirem com o instrutor para a resolução de dúvidas e de curiosidades.

3.4. Pilares da Comunicação Segura

No curso Pilares da Comunicação Segura, ministrado para um total de 20 alunos, apresentou-se conceitos fundamentais de segurança da informação. O objetivo do curso foi capacitar cidadãos e despertar o interesse para uma área que carece de profissionais no mercado de trabalho e cada vez mais relevante no contexto de uma sociedade tecnológica. Ao mesmo tempo, os alunos foram conscientizados sobre riscos cibernéticos e consequências negativas no cotidiano de uma pessoa, empresa ou instituição.

Introduziu-se o assunto para os alunos demonstrando o que são incidentes cibernéticos, como eles impactam os sistemas informatizados de corporações, governos e pessoas. Em seguida apresentou-se o conceito de segurança cibernética por meio dos pilares confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade. Exploraram-se esses tópicos individualmente para que os alunos pudessem compreender como cada um deles contribui para a segurança da informação. Por fim, apresentou-se como esses pilares podem ser combinados para prover modelos de comunicação segura, capazes de proteger dados durante o processo de transmissão por uma rede de computadores como a Internet. Os alunos participaram ainda de uma atividade prática, na qual foram instruídos a implementarem os modelos de comunicação segura apresentados pelo instrutor com o auxílio de softwares específicos. No experimento, eles foram capazes de implementar os modelos e de enviar mensagens seguras entre si, em um momento lúdico do final do curso.

3.5. Internet das Coisas

No curso de IoT, os alunos foram divididos em turmas de 20 integrantes que tiveram a oportunidade de explorar os conceitos e as tecnologias que habilitam esse cenário promissor. O curso é composto por fases que permutam entre a discussão de conhecimentos teóricos para formação do conhecimento, bem como de atividades práticas que estimulam a criatividade e fixação do conhecimento. Inicialmente, os alunos são aleatoriamente divididos em grupos e apresentados a um tema de projeto e provocados em propor uma solução inicial que é apresentada para todos em formato de *pith*. Essa atividade é caracterizada como uma competição para introduzir o elemento da gamificação e despertar o interesse por assimilar os conteúdos teóricos da IoT [Al-Fuqaha et al. 2015, Lu and Xu 2019, Meneghello et al. 2019].

Na exposição teórica, os alunos compreendem os princípios básicos da IoT relacionados à conexão de dispositivos, troca de dados e interação em um ecossistema interconectado. Além disso, foram apresentados os principais protocolos de comunicação utilizados no ambiente IoT, bem como as tecnologias de *hardware* e *software* necessárias para habilitar toda essa estrutura. Após a explanação teórica os alunos voltam a formação

de grupos inicial e são desafiados em redefinir a proposta de projeto de forma técnica aplicando o conhecimento adquirido. Nessa etapa, os alunos realizam experimentos práticos, utilizando kits de desenvolvimento IoT, sendo instigados em explorar as tecnologias disponíveis para habilitar essas soluções.

Durante o desenvolvimento da parte prática, o professor faz mentorias rápidas para provocar e estimular o pensamento crítico. Por outro lado, os grupos foram modificados com base em intervenções propostas pelo professor como forma de introduzir o elemento da surpresa com o dinamismo das relações ao mover participantes chaves entre projetos. Essa abordagem provou-se eficiente em estimular o engajamento contínuo do grupo, uma vez que a troca de alguns membros culmina em um processo de revisão e aprimoramento constante das propostas que surge naturalmente de um processo de confronto de ideias.

3.6. Introdução ao Gerenciamento de Rede com Python

O curso Introdução ao Gerenciamento de Redes com Python, foi ministrado para 20 alunos e demonstrou como essa linguagem de programação pode ser utilizada para o desenvolvimento de ferramentas para o gerenciamento de Redes de Computadores. O objetivo foi difundir conhecimentos mais avançados para os alunos e despertar o interesse pelas áreas de telecomunicações e programação. Inicialmente, os alunos foram introduzidos à linguagem Python. Foram demonstradas as estruturas básicas de decisão, repetição, criação de funções seguido pela utilização de módulos avançados, como *sockets*, *threads* e bibliotecas que permitem a navegação pelo sistema operacional.

Após uma base de conhecimento ter sido construída com os alunos, eles foram orientados a desenvolverem duas ferramentas. A primeira delas deveria executar uma varredura na rede procurando por outros computadores conectados a mesma. Já a segunda consistia em um *software* de bate-papo entre dois computadores. Ao final do curso os alunos foram capazes de desenvolver as ferramentas com a orientação do instrutor. Além disso, eles demonstraram engajamento na aprendizagem da linguagem de programação ao serem notavelmente participativos durante o curso.

3.7. Python aplicado à Segurança Cibernética

No curso de Python, os discentes foram divididos em turmas de 24 alunos com atividades realizadas por meio de acesso a um *notebook* exclusivo para realizar as experiências de forma individual e sob orientação do professor. Entretanto, os alunos foram incentivados a colaborar entre si, visando otimizar os códigos desenvolvidos. O curso se iniciou com a formação teórica para introduzir os alunos aos conceitos básicos de segurança cibernética, compreendendo a importância de proteger sistemas e dados contra ameaças e ataques [Xin et al. 2018].

Posteriormente, a linguagem Python e a plataforma *Google Colaboratory* foram exploradas como ferramentas práticas para aplicação no contexto da segurança cibernética. Os alunos iniciaram os estudos práticos lembrando ou aprendendo conceitos básicos de Python, como entrada e saída de dados, estruturas condicionais, estruturas de repetição, acesso a arquivos externos, criação de funções [Zanetti et al. 2022], e comunicação em rede através de *sockets* *User Datagram Protocol* (UDP) e *Transmission Control Protocol* (TCP). Durante o aprendizado de cada um desses conceitos, foram realizados experimentos voltados para o cenário da segurança cibernética.

Os experimentos propostos abrangeram diversos tópicos relacionados aos sistemas que possuem algum tipo de segurança contra ameaças cibernéticas. Os alunos aplicaram os conceitos para resolver problemas de criptografia, decifração, validação de números de Cadastro de Pessoas Físicas (CPF) por meio do cálculo dos dígitos verificadores, quebra de senhas utilizando métodos de força bruta, quebra de senhas com o auxílio de bibliotecas específicas do Python, manipulação de mensagens recebidas por meio de comunicação UDP e TCP, controle de acesso baseado no número de tentativas e temporização, entre outros.

Os alunos concluíram todas as atividades propostas e puderam comprovar, de forma prática, cada um dos conceitos teóricos aprendidos. Os desafios relacionados à quebra de senhas despertaram um grande engajamento por parte dos alunos, demonstrando o interesse e a motivação gerados pelo curso. Ao enfrentar esses desafios, os alunos puderam desenvolver habilidades de resolução de problemas e aplicar os conhecimentos adquiridos em um contexto real.

4. Conclusões e Trabalhos Futuros

Neste artigo, exploraram-se a importância do ensino do funcionamento das TDICs e da segurança cibernética no contexto educacional. Os cursos desenvolvidos pelo CxSc Telecom do Inatel proporcionaram aos alunos uma compreensão das TDICs por meio de atividades práticas para exploração e comprovação de conceitos e hipóteses. Adotou-se uma metodologia que integrou conceitos teóricos, ferramentas computacionais e equipamentos. Isso permitiu aos alunos aplicar aprendizados em situações práticas, validar conceitos e adquirir uma experiência completa em áreas como redes de computadores, telefonia, Internet das coisas, gerenciamento de rede e segurança cibernética. A interação constante entre professores e alunos desempenhou um papel fundamental no processo de ensino e aprendizagem, permitindo ajustes na metodologia e no conteúdo dos cursos com base no *feedback* contínuo dos alunos.

A compreensão do funcionamento das TDICs e dos princípios de segurança cibernética é crucial no processo de conscientização tecnológica e digital de jovens, permitindo o uso responsável e a atuação no desenvolvimento de sistemas seguros e na prevenção de ataques cibernéticos. Além disso, as TDICs têm um impacto significativo no contexto educacional, promovendo a qualidade do ensino e aprendizagem, ampliando o acesso à educação e desenvolvendo habilidades digitais essenciais para os alunos em uma sociedade tecnológica.

No entanto, é importante destacar que a evolução tecnológica e as ameaças cibernéticas estão em constante mudança. Portanto, é fundamental que as instituições de ensino continuem atualizando seus currículos e metodologias para acompanhar esse ritmo acelerado. Além disso, é necessário investir em capacitação e formação contínua dos professores, a fim de garantir a capacidade de transmissão de conhecimentos atualizados e preparar os alunos para os desafios futuros. Nesse contexto, a iniciativa do CxSC Telecom do Inatel no desenvolvimento e aplicação de cursos em tecnologia demonstra a importância de abordagens inovadoras e integradoras no ensino das TDICs e segurança cibernética.

Em suma, através de cursos bem estruturados e metodologias inovadoras, é possível fornecer aos alunos uma base sólida de conhecimento e habilidades práticas,

capacitando-os para contribuir com o desenvolvimento de sistemas seguros e a promover a conscientização sobre a importância da segurança cibernética. A integração das TDICs no ambiente educacional tecnológico traz benefícios significativos para a qualidade do ensino, ampliação do acesso à educação e desenvolvimento de competências. Por isso, é fundamental que outras instituições de ensino também continuem investindo nessa área e se adaptando às mudanças tecnológicas, a fim de preparar os alunos para um futuro cada vez mais digital e seguro.

Dentro dessas premissas, trabalhos futuros compreendem estudos visando a ampliação da oferta de cursos com foco nas TDICs e segurança cibernética, com aplicação no período de 2023/2024. Além disso, existem iniciativas em andamento relacionados à formação de profissionais da educação básica para atuarem em atividades relacionadas à formação e conscientização tecnológica em segurança no mundo digital de público infantil e adolescente.

5. Agradecimentos

Os autores agradecem ao Inatel, a Huawei e ao Centro de Segurança Cibernética (CxSC Telecom) pelo incentivo a realização dessas atividades, bem como a Finep (0122060400) pelos recursos destinados a realização e divulgação desse projeto.

Referências

- Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4):2347–2376.
- Alwayn, V. (2004). *Optical network design and implementation*. Cisco Press.
- Chinedu, P. U., Nwankwo, W., Masajuwa, F. U., and Imoisi, S. (2021). Cybercrime detection and prevention efforts in the last decade: An overview of the possibilities of machine learning models. *Review of International Geographical Education Online*, 11(7).
- Damaševičius, R., Venčkauskas, A., Toldinas, J., and Grigaliūnas, (2021). Ensemble-based classification using neural networks and machine learning models for windows pe malware detection. *Electronics*, 10(4).
- Dolma, A. and Kiraz, M. (2018). Data transmission analysis of dwdm and sdh. In *2018 26th Signal Processing and Communications Applications Conference (SIU)*, pages 1–4.
- Goode, B. (2002). Voice over internet protocol (voip). *Proceedings of the IEEE*, 90(9):1495–1517.
- Lu, Y. and Xu, L. D. (2019). Internet of things (iot) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, 6(2):2103–2115.
- Meneghello, F., Calore, M., Zucchetto, D., Polese, M., and Zanella, A. (2019). Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices. *IEEE Internet of Things Journal*, 6(5):8182–8201.
- Molenda, M. (2003). In search of the elusive addie model. *Performance improvement*, 42(5):34–37.

- Molenda, M. (2015). In search of the elusive addie model. *Performance improvement*, 54(2):40–42.
- Pedaste, M., Kallas, K., and Baucal, A. (2023). Digital competence test for learning in schools: Development of items and scales. *Computers Education*, 203:104830.
- Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., and Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access*, 6:35365–35381.
- Zanetti, H., Borges, M., and Ricarte, I. (2022). A teoria de aprendizagem significativa no ensino de programação: um mapeamento sistemático da literatura. In *Anais do XXXIII Simpósio Brasileiro de Informática na Educação*, pages 01–14, Porto Alegre, RS, Brasil. SBC.