Revista ARACÊ
ISSN: 2358-2472

METODOLOGIAS ATIVAS NO ENSINO DE CIBERSEGURANÇA: EXPERIÊNCIAS COM DEFESA CONTRA ATAQUES DE CANAL LATERAL EM AMBIENTES EDUCACIONAIS

ACTIVE METHODOLOGIES IN CYBERSECURITY EDUCATION: EXPERIENCES WITH DEFENSE AGAINST SIDE-CHANNEL ATTACKS IN EDUCATIONAL ENVIRONMENTS

METODOLOGÍAS ACTIVAS EN LA EDUCACIÓN EN CIBERSEGURIDAD: EXPERIENCIAS DE DEFENSA CONTRA ATAQUES DE CANAL LATERAL EN ENTORNOS EDUCATIVOS

https://doi.org/10.56238/arev8n4-007

Data de submissão: 08/03/2026 **Data de publicação:** 08/04/2026

Jonas da Silva Aquino
Mestrando em Engenharia da Computação
Instituição: Universade de Pernambuco (UPE)
E-mail: jsa2@ecomp.poli.br
Lattes: https://lattes.cnpq.br/4688542305121924
ORCID: https://orcid.org/0009-0006-2363-4198

José Paulo Goncalves de Oliveira
Doutor em Engenharia Eletrica
Instituição: Universidade Federal de Pernambuco (UFPE)
E-mail: jpgo@ecomp.poli.br
Lattes: http://lattes.cnpq.br/2174091280358934
ORCID: https://orcid.org/0000-0001-9438-6829

Wagner Franceschini
Mestrando em Engenharia da Computação
Instituição: Universade de Pernambuco (UPE)
E-mail: wf@ecomp.poli.br
Lattes: http://lattes.cnpq.br/6202363569597502
ORCID: https://orcid.org/0009-0009-2932-2373

RESUMO
Considerando a expansão dos sistemas embarcados, Internet das Coisas e infraestruturas digitais críticas, a formação em cibersegurança torna-se cada vez mais relevante. Contudo, em muitos cursos técnicos e superiores, o ensino de segurança da informação ainda apresenta predominância conteúdo teórico, com pouca exploração prática das vulnerabilidades físicas presentes em dispositivos computacionais. Essa limitação dificulta a compreensão de como algoritmos criptográficos podem apresentar vulnerabilidades quando implementados em hardware real, especialmente em ataques de canal lateral. Nessa conjuntura, este estudo tem como objetivo investigar como a aplicação de metodologias ativas pode contribuir para o ensino de cibersegurança por meio da defesa prática contra ataques de canal lateral em sistemas embarcados. Para esse caso, foi implementada uma metodologia ativa baseada em aprendizagem por projetos em duas turmas da área tecnológica do Senac Garanhuns, no total de quarenta e dois alunos. As atividades foram desenvolvidas ao longo de quatro meses com

Revista ARACÊ
ISSN: 2358-2472

utilização de microcontroladores, placas de prototipagem, instrumentos de medição eletrônica e desenvolvimento de firmware na plataforma STM32CubeIDE, permitindo aos estudantes explorar experimentalmente conceitos relacionados à segurança física. Os resultados indicaram maior engajamento discente, fortalecimento do pensamento analítico e melhor compreensão das relações entre execução de software, comportamento do hardware e exposição de dados sensíveis. Além disso, a experiência demonstrou viabilidade institucional ao ser registrada na Plataforma Gênesis do Senac Pernambuco, evidenciando o potencial das metodologias ativas para o ensino aplicado de cibersegurança em sistemas embarcados.

Palavras-chave: Metodologias Ativas. Ciberseguraça. Ataque de Canal Lateral. Sistemas Embarcados. Ensino Prático.

ABSTRACT

Considering the expansion of embedded systems, the Internet of Things, and critical digital infrastructures, cybersecurity training is becoming increasingly relevant. However, in many technical and higher education courses, information security education still predominantly focuses on theoretical content, with little practical exploration of the physical vulnerabilities present in computing devices. This limitation hinders the understanding of how cryptographic algorithms can present vulnerabilities when implemented in real hardware, especially in side-channel attacks. In this context, this study aims to investigate how the application of active methodologies can contribute to cybersecurity education through practical defense against side-channel attacks in embedded systems. For this purpose, an active methodology based on project-based learning was implemented in two classes in the technological area of Senac Garanhuns, totaling forty-two students. The activities were developed over four months using microcontrollers, prototyping boards, electronic measuring instruments, and firmware development on the STM32CubeIDE platform, allowing students to experimentally explore concepts related to physical security. The results indicated greater student engagement, strengthened analytical thinking, and a better understanding of the relationships between software execution, hardware behavior, and the exposure of sensitive data. Furthermore, the experience demonstrated institutional viability by being registered on the Senac Pernambuco Genesis Platform, highlighting the potential of active methodologies for applied cybersecurity education in embedded systems.

Keywords: Active Methodologies. Cybersecurity. Side-Channel Attack. Embedded Systems. Practical Teaching.

RESUMEN

Considerando la expansión de los sistemas embebidos, el Internet de las Cosas y las infraestructuras digitales críticas, la formación en ciberseguridad cobra cada vez mayor relevancia. Sin embargo, en muchos cursos técnicos y de educación superior, la formación en seguridad de la información aún se centra predominantemente en el contenido teórico, con escasa exploración práctica de las vulnerabilidades físicas presentes en los dispositivos informáticos. Esta limitación dificulta la comprensión de cómo los algoritmos criptográficos pueden presentar vulnerabilidades al implementarse en hardware real, especialmente en ataques de canal lateral. En este contexto, este estudio tiene como objetivo investigar cómo la aplicación de metodologías activas puede contribuir a la formación en ciberseguridad mediante la defensa práctica contra ataques de canal lateral en sistemas embebidos. Para ello, se implementó una metodología activa basada en el aprendizaje por proyectos en dos clases del área tecnológica de Senac Garanhuns, con un total de cuarenta y dos estudiantes. Las actividades se desarrollaron durante cuatro meses utilizando microcontroladores, placas de prototipado, instrumentos de medición electrónicos y desarrollo de firmware en la plataforma

Revista ARACÊ
ISSN: 2358-2472

STM32CubeIDE, lo que permitió a los estudiantes explorar experimentalmente conceptos relacionados con la seguridad física. Los resultados indicaron una mayor participación estudiantil, un fortalecimiento del pensamiento analítico y una mejor comprensión de las relaciones entre la ejecución del software, el comportamiento del hardware y la exposición de datos sensibles. Además, la experiencia demostró su viabilidad institucional al estar registrada en la Plataforma Génesis de Senac Pernambuco, lo que resalta el potencial de las metodologías activas para la enseñanza aplicada de la ciberseguridad en sistemas embebidos.

Palabras clave: Metodologías Activas. Ciberseguridad. Ataque de Canal Lateral. Sistemas Embebidos. Enseñanza Práctica.

Revista ARACÊ
ISSN: 2358-2472

1 INTRODUÇÃO

A proteção no ambiente digital se tornou fundamental na era atual da tecnologia, vários setores tecnológicos mostram sua preocupação com esse tema em diferentes níveis de complexidade. Levando em conta sistemas de computação de maneira geral, é possível refletir sobre aspectos de segurança que abrangem tanto *software* quanto *hardware* (Koeune; Standaert, 2005).

De forma simples, segurança de *software* aborda ameaças mal-intencionadas direcionadas ao mesmo, que aproveitam diversas vulnerabilidades, como erros na implementação, manejo inadequado de falhas e transbordamentos de *buffer* (Koeune; Standaert, 2005).

Quanto ao *hardware*, as dificuldades estão ligadas à parte eletrônica, envolvendo arquitetura, execução, verificação, distribuição e forma de acesso aos dispositivos, considerando os próprios elementos como circuitos integrados, resistores, capacitores, indutores e placas de circuito impresso, além dos segredos que residem dentro desses elementos, tais como chaves de criptografia, informações confidenciais dos usuários, *software* instalado e configurações de dados (Tehranipoor; Koushanfar, 2010).

O primeiro caso de ataques a canais laterais (*Side Channel Attacks* – SCAs) que tem como objetivo reunir dados ou afetar a operação do software de um dispositivo, avaliando ou aproveitando impactos secundários do sistema ou de seu equipamento, foi apresentado à comunidade acadêmica por Kocher, onde provou ser possível relacionar a chave criptográfica com o tempo de execução do algoritmo, também chamado de ataque por análise de tempo (*Timing Attack* – TA) (Kocher, 2001).

Ainda Kocher demonstra que existe uma relação entre a potência consumida por um circuito digital e os dados que estão sendo processados pelo mesmo (Kocher; Jaffe; Jun, 1999).

> A formação em segurança cibernética tem se tornado cada vez mais importante devido ao crescimento de sistemas embarcados, dispositivos internet das Coisas (Iot) e estruturas essenciais, onde técnicas de criptografia são utilizados em grande medida para assegurar a privacidade e a integridade dos dados (Fontoura, 2016; Lellis, 2017, Kaur; Singh; Kaur, 2021).

A falta de experiências práticas costuma limitar o crescimento de habilidades aplicadas, tais como a análise de padrões de consumo, identificação de vulnerabilidades concretas e a verificação de medidas de segurança criptográficas em equipamentos de baixo custo. (Fontoura, 2016; Lellis, 2017; Kaur; Singh; Kaur, 2021).

Pesquisas indicam que a proteção de sistemas ciberfísicos necessitam de uma metodologia que una teoria e prática, permitindo que o estudante enfrente situações reais, estimulando o pensamento crítico. Assim, é essencial implementar métodos de ensino que vão além do formato clássico,

Revista ARACÊ
ISSN: 2358-2472

conectando a educação com a tecnologia atual e com as necessidades do mercado e da investigação científica (Fontoura, 2016; Lellis, 2017; Kaur; Singh; Kaur, 2021).

1.1 PROBLEMA E JUSTIFICATIVA

A principal problemática da pesquisa resulta que em cursos técnicos e superiores, a segurança da informação tende a ter uma abordagem baseada em teoria e conceitos, enquanto a investigação prática de vulnerabilidades físicas reais é muitas vezes negligenciada (Fell; Pham; Lam, 2019; Ramos, 2024).

Essa limitação torna mais difícil para que estudantes entendam como algoritmos de criptografia amplamente empregados, como o AES (*Advanced Encryption Standard*) e RSA (*Rivest Shamir Adleman*), podem ser vulneráveis, mesmo quando implementados de maneira correta do ponto de vista lógico, por estarem sujeitos a vazamentos físicos inerentes ao hardware (Fell; Pham; Lam, 2019; Ramos, 2024).

Esse cenário demonstra a necessidade de métodos de ensino que facilitam a conexão entre teoria e a prática, possibilitando que o aluno experimente de maneira tangível, os desafios da segurança em sistemas embarcados (Fell; Pham; Lam, 2019; Ramos, 2024).

A justificativa do ponto de vista institucional e acadêmico, é que adotando atividades de ensino baseados em projetos práticos, auxiliam na formação de especialistas melhores capacitados para enfrentar os desafios do mercado e da pesquisa científica, incentivando a conexão entre aprendizado, investigação e extensão (Ramos, 2024).

Ao empregar plataformas acessíveis e laboratórios de aprendizado, é viável tornar o ensino de segurança física mais acessivel, permitindo sua aplicação em diversos cenários educacionais e reforçando a qualificação técnica e científica em cibersegurança de forma prática (Ramos, 2024).

> Esta pesquisa tem como proposta a utilização de metodologias ativas de aprendizagem no ensino de cibersegurança, através de atividades práticas que abordam a proteção contra ataques de canal lateral em sistemas embarcados (Fontoura, 2016; Kaur; Singh; Kaur, 2021; Ramos, 2024).

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Este estudo tem como objetivo principal investigar como a aplicação de metodologias ativas, através da defesa prática contra ataques de canal lateral em sistemas embarcados, promovendo o engajamento estudantil, aprimorando competências técnicas e solidificando o entendimento de conceitos de segurança física no ensino de cibersegurança.

Revista ARACÊ
ISSN: 2358-2472

1.2.2 Objetivos Especificos

- Desenvolvimento e validação de soluções para mitigar os ataques, focando na segurança de hardware de baixo custo.
- Monitorar o interesse e a evolução técnica/analítica dos alunos durante as atividades.
- Discutir a viabilidade e a replicabilidade da metodologia educacional em diferentes contextos institucionais e níveis de ensino.

2 REFERENCIAL TEÓRICO

A presença generalizada de sistemas embarcados e de outros tipos mais privativos como redes de sensores, faz com que esses sistemas assumam um papel crescente em tarefas essenciais, o que torna fundamental criar soluções de segurança apropriadas para eles (Wangham; Domenech; Mello, 2013).

A posição geográfica e a forma como se conectam tornam esses sistemas suscetíveis a investidas de ataques, que podem divergir tanto em suas modalidades de execução quanto em seus propósitos finais (Parameswaran; Wolf, 2008).

2.1 METODOLOGIAS ATIVAS NO ENSINO DE COMPUTAÇÃO E CIBERSEGURANÇA

A cibersegurança também conhecida como segurança digital, segurança cibernética ou *cybersecurity*, é um setor que une diversas áreas e se dedica à proteção de bens digitais, sistemas de computadores e redes de comunicação contra riscos que podem vir tanto de dentro como de fora. Este campo abrange um leque de métodos, tecnologias e diretrizes que buscam assegurar os fundamentos da confidencialidade, integridade, disponibilidade e veracidade das informações (Stallings, 2017).

As metodologias de ensino ativas se sobressaem como opções aos métodos convencionais de educação, particularmente em campos tecnológicos como a Informática e Engenharia, onde a conexão entre a teoria e a prática é fundamental (Ramos, 2024).

Ao colocar o aluno como protagonista do processo de aprendizado, essas abordagens facilitam a educação basedas em desafios, iniciativas e vivências práticas, estimulando o crescimento do raciocínio crítico, da independência e uso prático do conhecimento, habilidades essenciais para a formação na área de cibersegurança (Stallings, 2017).

No campo da cibersegurança, as abordagens ativas tem destaque por atenderem às características práticas e dinâmicas das ameaças digitais. Isso possibilita que os alunos entendam tanto os princípios teóricos quanto as restrições dos sistemas de proteção em situações reais, alinhando-se às exigências do setor e da pesquisa aplicada (Ramos, 2024).

Revista ARACÊ
ISSN: 2358-2472

2.2 ENSINO DE SEGURANÇA FÍSICA E ATAQUES DE CANAL LATERAL

A proteção física dos sistemas de computação representa um desafio crescente no contexto da cibersegurança, principalmente em sistemas embarcados e dispositivos ciberfísicos. Ataques de canal lateral tiram proveito de informações físicas não funcionais, como consumo elétrico, duração de execução e emissões eletromagnéticas, possibilitando a coleta de informações sensíveis mesmo quando os algoritmos criptográficos estão implementados corretamente em termos lógicos (Fontoura, 2016; Lellis, 2017; Kaur; Singh; Kaur, 2021).

Pesquisas indicam que esses ataques apresentam uma ameaça real e contínua, demandando soluções específicas tanto em *hardware* quanto em *software* (Fontoura, 2016; Lellis, 2017; Kaur; Singh; Kaur, 2021).

No âmbito educacional, a instrução sobre ataques de canal lateral traz desafios extras, pois exigem conhecimentos que cruzam áreas como criptografia, arquitetura de computadores, eletrônica e estudo de sinais. A escassez de materiais de laboratório e a dificuldade dos experimentos frequentemente resultam em uma abordagem que é apenas teórica ou rasa nos cursos de formação (Fontoura, 2016; Lellis, 2017).

Como resultado, os alunos muitas vezes desvalorizam a importância da segurança física e falham em entender completamente os perigos relacionados à aplicação de criptossistemas em dispositivos integrados (Fontoura, 2016; Lellis, 2017).

2.3 APRENDIZAGEM BASEADA EM PROJETOS COM SISTEMAS EMBARCADOS

A Aprendizagem Baseada em Projetos (*Project-Based Learning* – PBL) se torna cada vez mais reconhecida como uma metodologia eficiente para ensinar conteúdos desafiadores, possibilitando que os alunos trabalhem em soluções para questões do mundo real dentro de um processo organizado (STMicroelectronics, 2024).

Em disciplinas de Computação e Engenharia, a aplicação de sistemas embarcados como ferramenta de aprendizado amplifica essa estratégia, já que esses sistemas proporcionam um contexto tangível para a combinação de teoria e prática. A utilização de microcontroladores acessíveis torna viável a execução de experimentos que podem ser repetidos e que refletem as tecnologias atuais (STMicroelectronics, 2024).

No campo da cibersegurança, iniciativas fundamentadas em sistemas embarcados possibilitam que os estudantes experimentem de maneira prática todo o processo de ataque e defesa, começando pela identificação de falhas de segurança até a execução e análise de respostas (Kaur; Singh; Kaur, 2021).

Revista ARACÊ
ISSN: 2358-2472

A prática de métodos de prevenção contra ataques de canal lateral, como a adição de ruidos e variações de tempo, favorece uma compreensão mais abrangente dos métodos de segurança e seus efeitos no funcionamento do sistema. Essa metodologia fortalece o aprendizado ativo e incentiva a aquisição de habilidades técnicas essenciais para a atuação na segurança embarcada (Kaur; Singh; Kaur, 2021; Fell; Pham; Lam, 2019).

2.4 TRABALHOS RELACIONADOS

O posicionamento de uma pesquisa no cenário científico é importante fazer uma revisão cuidadosa dos estudos já realizados na área. Essa etapa é essencial para identificar as lacunas que a pesquisa pretende preencher, fortalecer a base teórica e mostrar o que torna seu trabalho original e importante para o avanço do conhecimento (Webster; Watson, 2002).

Com o propósito de fundamentar teoricamente a proposta deste projeto, foram analisados trabalhos relacionados que aplicam técnicas de metodologias ativas no ensino da computação e cibersegurança.

Uma das abordagens encontradas na literatura é a de Junior (2024), que usa de Inteligência Artificial e laboratórios virtuais como ferramentas pedagógicas para o ensino de Segurança da Informação no Ensino Fundamental I, com uma abordagem qualitativa, de caráter exploratório e bibliográfico, utilizando análise de literatura sobre o tema da pesquisa. Sua principal contribuição é apresentar uma abordagem pedagógica para o ensino de Segurança da Informação. A lacuna é a escassez de estudos que tratem do ensino estruturado de Segurança da Informação no Ensino Fundamental I no uso de Inteligência Artificial e laboratórios virtuais como recursos educacionais.

Em outra linha de pesquisa Goulart *et al*. (2024), é a Educação em Cibersegurança, com foco no desenvolvimento e avaliação de jogos sérios como ferramentas pedagógicas, utilizando uma abordagem qualitativa e exploratória, baseada em revisão bibliográfica e análise conceitual sobre o uso de jogos sérios no ensino de Segurança da Informação. Apesar de sua principal contribuição que é evidenciar os jogos como ensino para segurança, não existe uma metodologia de abordagem prática desenvolvida para os envolvidos.

A pesquisa de Fernandes *et al*. (2024), tem como linha a Educação em Computação e Tecnologias Digitais, com base em segurança digital, cidadania digital e metodologias ativas, trata-se de um relato de experiência qualitativa, baseado na utilização de metodologias ativas com alunos do primeiro ano do Ensino Fundamental, empregando atividades educativas apoiadas por ferramentas digitais e avaliação contínua, embora o estudo evidencia as metodologias, verifica-se a carência de recursos didáticos específicos e validados sobre *cyberbullying* e segurança digital.

Revista ARACÊ
ISSN: 2358-2472

Ainda, Leles *et al*. (2025), investigam inovações no ensino de cibersegurança através da colaboração entre universidades e indústria, empregando métodos ativos, com ênfase no aprendizado baseado em desafios e na educação orientada por competências. Tendo caráter qualitativo, utilizando uma abordagem de estudo de caso e combinando a aprendizagem autorregulada com avaliações diagnósticas, formativas e somativas. Sua principal contribuição é a apresentação de um modelo educacional que pode ser replicado para a formação em cibersegurança, ao mesmo tempo em que trata da falta de evidências empíricas relacionadas à aplicação conjunta dessas metodologias em cursos de pós-graduação.

Ao analisar os estudos relacionados, embora todos utilizem abordagem qualitativa e metodologias ativas aplicadas a contextos da cibersegurança, a presente pesquisa aborda aspectos mais amplos e apresenta diferenciais importantes quanto ao foco, com atividades de ensino baseados em projetos práticos para desenvolvimento de competências técnicas, que permite uma compreensão mais detalhada dos fatores que comprometem a resolução eficiente de segurança embarcada, além de possibilitar o entendimento de conceitos de segurança física no ensino de cibersegurança.

3 METODOLOGIA

Esta seção detalha os procedimentos metodológicos adotados para a realização dos objetivos desta pesquisa. A metodologia desta pesquisa foi primeiramente criada e implementada na unidade do Senac em Garanhuns, envolvendo duas turmas da área de tecnologia, totalizando quarenta e dois estudantes, sendo uma turma com vinte e sete alunos e outra com quinze alunos.

As atividades foram realizadas de segunda a sexta-feira, com carga horária de 3 horas diárias**,** em um período inicial de 4 meses, dividida em etapas e envolvendo as turmas da área tecnológica, com a meta de facilitar o aprendizado em cibersegurança através de métodos ativos baseados em projetos reais (Prodanov; Freitas, 2013).

A primeira etapa foi realizada com a apresentação do projeto e da metodologia que seria empregada nas turmas de tecnologia do Senac, conforme ilustrado nas Figuras 1 e 2.

Revista ARACÊ
ISSN: 2358-2472

Figura 1 – Apresentação Projeto: Senac Garanhuns.

Fonte: Preparado pelos próprios autores.

Figura 2 – Turmas de Tecnologia: Senac Garanhuns.

Fonte: Preparado pelos próprios autores.

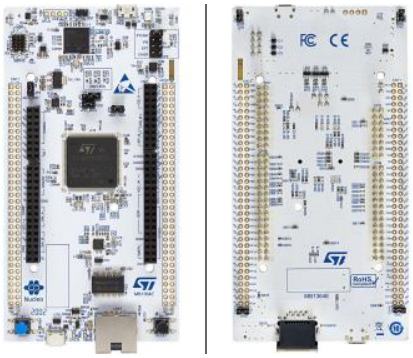
As figuras acimas demonstram que a proposta da pesquisa é conectar os alunos com situações práticas que envolvem a proteção física de sistemas embarcados, possibilitando a experiência em cenários reais, de acordo com as necessidades atuais do campo da segurança da informação.

A segunda etapa com base experimental consiste em utlizar o microcontrolador STM32H753ZI, presente na placa de desenvolvimento NUCLEO-H753ZI, que já possui inúmeros recursos avançados de *hardware* voltados a segurança, como aceleradores criptográficos, gerador de números aleatórios (RNG) e elevada capacidade de processamento, conforme figura 3 (STMicroelectronics, 2024).

A placa de desenvolvimento oferece baixo custo de aquisição, que faz parte do escopo do projeto e possibilitou a exploração de funcionalidades presentes em sistemas embarcados amplamente utilizados em contextos industriais e educacionais, conforme a Figura 3 (STMicroelectronics, 2024).

Revista ARACÊ
ISSN: 2358-2472

Figura 3 – Placa de desenvolvimento: NUCLEO-H753ZI.



Fonte: STMicroelectronics NUCLEO-H753ZI, 2024.

Durante as atividades práticas, os estudantes começaram recebendo uma explicação sobre o *hardware* e a plataforma de desenvolvimento STM32CubeIDE, abordando conceitos como arquitetura do microcontrolador, pinagem, alimentação elétrica e interfaces de entrada e saída.

Ainda nessa etapa, foram feitas atividades de configuração da placa de desenvolvimento, montagem de circuitos em uma *protoboard* e utilização de componentes simples, como LEDs, resistores e multímetros para um aprendizado inicial. Isso ajudou a visualizar e medir os sinais elétricos envolvidos no funcionamento do sistema embarcado, de acordo com a Figura 4.

Figura 4 – Materiais e componentes para o projeto.

Fonte: Preparado pelos próprios autores.

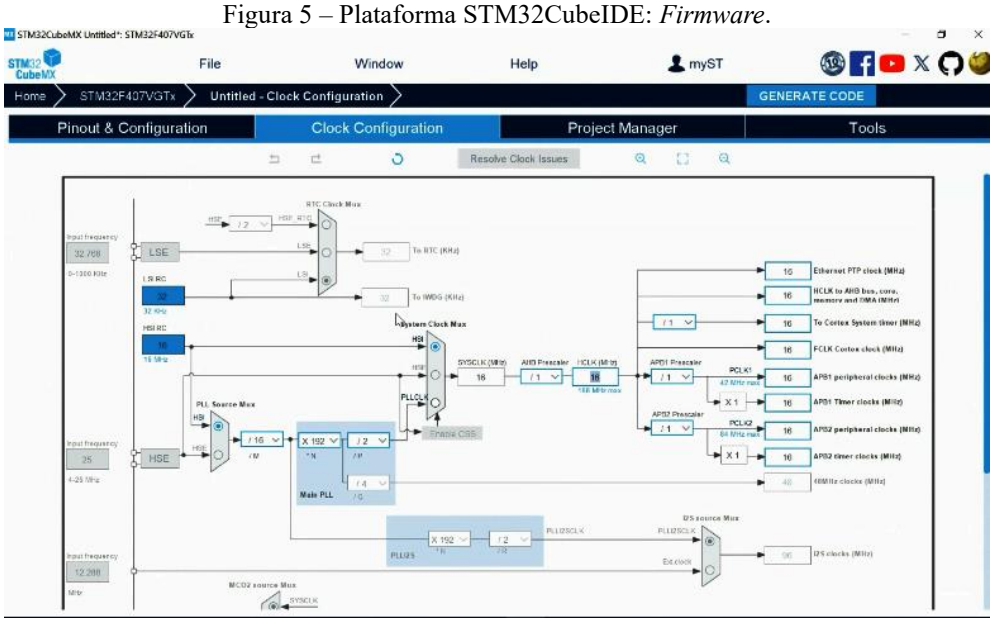
A plataforma STM32CubeIDE foi empregada para codificação das aplicações, com programação na sua maioria em linguagem C, complementada por trechos em *Assembly* quando necessário para um controle exato do *hardware* (STMicroelectronics, 2024).

Essa metodologia foi empregada particularmente em seções críticas ligadas ao consumo de energia, tempo de execução e comportamento do sistema, elementos fundamentais para entender os ataques de canal lateral (STMicroelectronics, 2024).

O *firmware* foi estruturado de maneira modular, incluindo a configuração de dispositivos periféricos, a utilização do RNG embarcado e a organização do código para facilitar a implementação, análise e avaliação de contramedidas de segurança, conforme a Figura 5 (STMicroelectronics, 2024).

Revista ARACÊ
ISSN: 2358-2472

Figura 5 – Plataforma STM32CubeIDE: *Firmware*.



Fonte: Preparado pelos próprios autores.

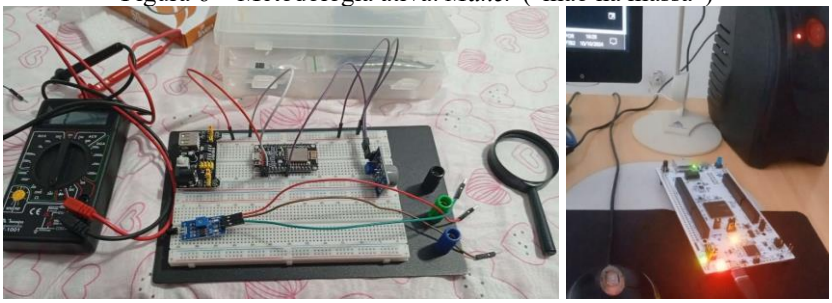
4 RESULTADOS E DISCUSSÕES

Antes da implementação da metodologia do projeto sugerido, os temas relacionados à cibersegurança eram predominantemente discutidos de maneira teórica através de conceitos e atividades sem aplicação em projetos, com pouca investigação prática sobre falhas físicas em equipamentos.

Nesse cenário, percebia-se que os alunos enfrentavam desafios para entender a conexão entre a execução de programas, consumo de energia e exposição de dados confidenciais. A interação dos estudantes era na sua maioria passiva, com raro envolvimento com ferramentas de medição e analise experimental (Fontoura, 2016; Lellis, 2017, Kaur; Singh; Kaur, 2021).

A aplicação da metodologia baseada em projeto permitiu as turmas de tecnologia cultivarem a cultura *Maker* (“mão na massa”), proporcionando aos alunos apriomirar os conhecimentos em laboratórios com componentes reais e bancadas de eletrônica em uma simulação de cenário de empresas do mercado, conforme a Figura 6 (Fontoura, 2016; Lellis, 2017, Kaur; Singh; Kaur, 2021).

Figura 6 – Metodologia ativa: *Maker* (“mão na massa”)



Fonte: Preparado pelos próprios autores.

Revista ARACÊ
ISSN: 2358-2472

Após a adoção da metodologia ativa com foco em problemas reais, foi notada uma transformação de forma significativa na participação e postura dos alunos. Durante os testes foram utilizados instrumentos como: Osciloscópio e multímetro para permitir a visualização das propriedades físicas do hardware enquanto as aplicações eram realizadas, conforme a Figura 7.

Figura 7 – Testes e utilização do osciloscópio.

Fonte: Preparado pelos próprios autores

Os alunos começaram a monitorar o funcionamento do sistema, desenvolver estratégias de montagem, configuração, proteção e examinar o efeito das medidas adotadas, levando em conta as mudanças nos sinais elétricos e no comportamento do dispositivo (STMicroelectronics, 2024).

A abordagem focou no objetivo educacional e da pesquisa, evitando a análise detalhada dos formalismos matemáticos e implementação mais técnica dos algoritmos de criptografia, destacando a noção prática dos fundamentos de segurança física em sistemas embarcados.

Do aspecto educacional, houve um crescimento na participação, independência e habilidade de análise dos alunos, demonstrado pela colaboração ativa nas montagens em *protoboard*, na configuração do circuito de desenvolvimento e na estruturação modular do *firmware* (Prodanov; Freitas, 2013).

Ainda como resultado direto da metodologia, os projetos permanecerão em andamento, conduzidos pelos próprios estudantes, indicando continuidade do aprendizado dos conceitos trabalhados (Prodanov; Freitas, 2013).

No contexto institucional, após a validação da metodologia na Unidade do Senac Garanhuns, a experiência foi apresentada como um projeto inovador e integrada à plataforma Gênesis, que é um espaço institucional dedicado à incubação de projetos e divulgação de iniciativas inovadoras de todas as unidades Senac do estado de Pernambuco, conforme a Figura 8.

Revista ARACÊ
ISSN: 2358-2472

Figura 8 – Plataforma Gênesis: Tela inicial

Fonte: Preparado pelos próprios autores

A plataforma funciona como um sistema de administração e organização do conhecimento, possibilitando o registro organizado das fases do projeto, das ferramentas tecnológicas empregadas e dos resultados alcançados, garantindo uniformidade nos métodos e a capacidade de rastrear informações, conforme a Figura 9.

Figura 9 – Plataforma Gênesis: Projeto cadastrado

Fonte: Preparado pelos próprios autores

A adesão à plataforma Gênesis facilitou a conversão de uma experiência local em um formato institucional que pode ser replicado, tornando possível sua aplicação em outras unidades do Senac em Pernambuco.

Os resultados mostram que a união de métodos ativos, com uma infraestrutura apropriada e uma boa governança institucional ajuda significativamente a melhorar o ensino de cibersegurança aplicada em sistemas embarcados.

Apesar dos resultados positivos observados, este estudo possui algumas limitações como a metodologia que foi aplicada exclusivamente em uma instituição, com duas turmas específicas de tecnologia. Apesar da quantidade total de quarenta e dois alunos possibilitar uma análise preliminar

Revista ARACÊ
ISSN: 2358-2472

robusta, o contexto continua sendo limitado, o que impede a ampliação dos resultados para diferentes perfis de cursos, graus de formação ou instituições que tenham estruturas diferentes.

Além disso, a aplicação da metodologia depende de uma infraestrutura básica de laboratório, que abrange placas de desenvolvimento, equipamentos de medição como: Osciloscópios e analisadores lógicos, além de um espaço apropriado para a realização de experimentos. Em situações educacionais que enfrentam restrições financeiras ou limitações técnicas, a reprodução completa da proposta pode necessitar de ajustes.

Como trabalhos futuros desta pesquisa, busca-se expandir o uso da metodologia em diferentes unidades do Senac Pernambuco, monitorando sua execução através de indicadores pedagógicos e técnicos mais bem definidos. Essa ampliação contribuirá para uma maior solidez nas metodologias e uma validação prática dos efeitos percebidos na educação em segurança cibernética aplicada.

No campo técnico, investigações futuras podem expandir a avaliação das medidas de segurança aplicadas no microcontrolador STM32H753ZI, examinando a performance, consumo de energia e eficiência em diferentes ambientes experimentais.

5 CONCLUSÃO

Este artigo apresentou a aplicação de metodologias ativas no ensino de cibersegurança, especialmente para ajudar os alunos a compreenderem de forma prática os ataques de canal lateral em sistemas embarcados.

O objetivo foi explorar de que maneira as atividades práticas e o estudo de problemas reais em projetos podem tornar o aprendizado de segurança da informação mais envolvente e relevante em ambientes educacionais.

Os resultados obtidos demonstraram que a implementação de experimentos utilizando microcontroladores, placas de prototipação, componentes eletrônicos, sensores, aparelhos de medição e a criação de *firmware* aumentou a participação dos alunos e aprofundou os conceitos de segurança física aplicada ao *hardware*.

Além da contribuição educacional, a experiência na unidade do Senac Garanhuns revelou a viabilidade da abordagem como um método de inovação na educação. A inclusão do projeto na plataforma Gênesis viabilizou sua gravação e propagação dentro da instituição, permitindo que seja reproduzido em outras unidades do Senac em Pernambuco.

Dessa maneira, a pesquisa ajuda no desenvolvimento de métodos educacionais focados no aprendizado de cibersegurança prática, destacando a capacidade das abordagens ativas para conectar alunos a situações reais de segurança em sistemas embarcados.

Revista ARACÊ
ISSN: 2358-2472

REFERÊNCIAS

FELL, A.; PHAM, H. T.; LAM, S. **TAD: time side-channel attack defense of obfuscated source code.** ASPDAC '19: Proceedings of the 24th Asia and South Pacific Design Automation Conference, ACM, 2019. Disponível em: https://doi.org/10.1145/3287624.3287694. Acesso em: 25/05/2025.

FONTOURA, F. M. **Uma API criptográfica para aplicações embarcadas**. 155 f. Dissertação (Mestrado em Computação Aplicada) - Universidade Tecnológica Federal do Paraná, Curitiba, 2016. Disponível em: https://repositorio.utfpr.edu.br/jspui/handle/1/1813. Acesso em: 25/06/2025.

GOULART, G.; AMARAL, É.; CORDEIRO, M.; SOARES, M.; LEAL, T. **Proposta de uma ferramenta para o apoio ao processo de ensino-aprendizagem de cibersegurança.** Porto Alegre: Sociedade Brasileira de Computação, 2024. p. 166-171. Disponível em: DOI: https://doi.org/10.5753/errc.2024.4684. Acesso em: 25/08/2025.

JUNIOR, E. W. S. V. **Ensino de segurança da informação no fundamental 1: uso de ia e laboratórios virtuais como ferramentas.** Monumenta - Revista Científica Multidisciplinar, 10(10), 324–341. Disponível em: https://doi.org/10.57077/monumenta.v10i10.274. Acesso em: 25/08/2025.

KAUR, S.; SINGH, B.; KAUR, H. **Stratification of Hardware Attacks: Side Channel Attacks and Fault Injection Techniques.** Original Research Published: 31 March, Volume 2, article number 183, Springer Nature, 2021. Disponível em: https://link.springer.com/article/10.1007/s42979-021-00562-3. Acesso em: 25/06/2025.

KOCHER, P. C. **Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems.** In: 16th International Cryptology Conference on Advances in Cryptology. London, UK: (CRYPTO'96) Springer-Verlag, 2001. Disponível em: https://link.springer.com/chapter/10.1007/3-540-68697-5_9. Acesso em: 25/06/2025.

KOCHER, P. C.; JAFFE, J.; JUN, B. **Differential Power Analysis.** In: 19th International Cryptology Conference on Advances in Cryptology. Santa Barbara, USA: (CRYPTO'99) Springer-Verlag, 1999. Disponível em: https://link.springer.com/chapter/10.1007/3-540-48405-1_25. Acesso em: 25/06/2025.

KOEUNE, F.; STANDAERT, F.-X. **A tutorial on physical security and side-channel attacks**. Foundations of Security Analysis and Design III: FOSAD 2004/2005 Tutorial Lectures. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005. ISBN 978-3-540-31936-8. Disponível em: https://link.springer.com/chapter/10.1007/11554578_3. Acesso em: 25/07/2025.

LELLIS, R. N. **Fluxo de ataque DPA/DEMA baseado na energia dos traços para neutralizar contramedidas por desalinhamento temporal em criptosistemas.** 96f. Dissertação (Mestrado) – Programa de Pós-Graduação em Computação. Universidade Federal de Pelotas, Pelotas, 2017. Disponível em: https://bdtd.ibict.br/vufind/Record/UFPL_7aafafc0807f4c5cfa935076fdeeebbf. Acesso em: 25/06/2025.

PARAMESWARAN, S.; WOLF, T. **Embedded Systems Security — An Overview.** Design Automation for Embedded Systems, 12(3), 2008. Disponível em: https://www.researchgate.net/publication/220201340_Embedded_systems_security-an_overview. Acesso em: 25/06/2025.

Revista ARACÊ
ISSN: 2358-2472

PRODANOV, C. C.; FREITAS, E. C. de. **Metodologia do Trabalho Cientifico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico**. 2. ed. Novo Hamburgo, Rio Grande do Sul: Feevale, 2013. Disponível em: https://www.feevale.br/Comum/midias/0163c988-1f5d-496f-b118-a6e009a7a2f9/E-book%20Metodologia%20do%20Trabalho%20Cientifico.pdf. Acesso em: 25/06/2025.

RAMOS, R. B. **Metodologias de análise integrada de segurança crítica e segurança cibernética em sistemas ciber físicos.** Digital Library of Theses and Dissertations of USP, São Paulo, 2024. Disponível em: https://doi.org/10.11606/D.3.2024.tde-12072024-091247. Acesso em: 25/06/2025.

STALLINGS, W. **Cryptography and Network Security:Principles and Practice**. Ed. Pearson, 2017. Disponível em: https://www.scirp.org/reference/referencespapers?referenceid=4166016. Acesso em: 25/08/2025.

STMicroelectronics. UM2407 - **User manual, STM32H7 Nucleo-144 boards (MB1364)**. Genebra, Suíça, 2024. Disponível em: https://br.mouser.com/ProductDetail/STMicroelectronics/NUCLEO-H753ZI?qs=%252B6g0mu59x7JptTWmsgHt6Q%3D%3D. Acesso em: 25/05/25.

TEHRANIPOOR, M.; KOUSHANFAR, F. **A survey of hardware trojan taxonomy and detection.** IEEE Design Test of Computers, v. 27, n. 1, janeiro 2010. ISSN 1558-1918. Disponível em: https://ieeexplore.ieee.org/document/5406669. Acesso em: 25/06/2025.

WANGHAM, M. S.; DOMENECH, M. C.; MELLO, E. R. d. **Infraestruturas de Autenticação e de Autorização para Internet das Coisas.** In Minicursos do XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSeg, 2013. Disponível em: https://www.researchgate.net/publication/263161591_Infraestruturas_de_Autenticacao_e_de_Autorizacao_para_Internet_das_Coisas. Acesso em: 25/06/2025.

WEBSTER, J.; WATSON, R. T. **Analyzing the past to prepare for the future: Writing a literature review**. MIS Quarterly, v. 26, n. 2, p. xiii-xxiii, 2002. Disponível em: https://www.researchgate.net/publication/220259996_Analyzing_the_Past_to_Prepare_for_the_Future_Writing_a_Literature_Review. Acesso em: 25/06/2025.