AVALIAÇÃO DO ENSINO DE CRIPTOGRAFIA APLICADA UTILIZANDO A METODOLOGIA MSEP E QUESTÕES DE CERTIFICAÇÕES PROFISSIONAIS

EVALUATING APPLIED CRYPTOGRAPHY EDUCATION USING MSEP METHODOLOGY AND PROFESSIONAL CERTIFICATION QUESTIONS

Hebert de Oliveira Silva[1], [i]
Caique Zaneti Kirilo[2], [ii]
Tiago Augusto Orcajo Demay Cordeiro [3], [iii]
Vivian de Oliveira Preto[4], [iv]
Emerson Costa Santos[5], [v]

Data de submissão: (13/03/2026) Data de aprovação: (29/10/2026)

RESUMO

Este trabalho apresenta uma avaliação do aprendizado de estudantes em uma disciplina de criptografia aplicada à segurança cibernética, conduzida com base na Metodologia SENAI de Educação Profissional (MSEP). Como instrumento de avaliação, foi aplicada uma prova composta por 50 questões de múltipla escolha provenientes de certificações profissionais da área de segurança da informação, com o objetivo de medir o domínio conceitual dos estudantes sobre os conteúdos abordados no curso. A análise dos resultados foi realizada por meio de métricas estatísticas educacionais, incluindo média, mediana, desvio padrão e distribuição das notas. Os resultados indicaram média de aproximadamente 66% de acertos, valor próximo ao nível geralmente exigido em exames de certificação profissional, que costuma variar entre 70% e 75%. Os resultados sugerem que a abordagem pedagógica adotada contribui para alinhar o processo de ensino às exigências do mercado, além de fornecer indicadores quantitativos para avaliação do aprendizado em criptografia.

Palavras-chave: criptografia; educação em cibersegurança; MSEP; avaliação educacional.

ABSTRACT

This paper presents an evaluation of student learning in an applied cryptography course for cybersecurity, conducted using the SENAI Professional Education Methodology (MSEP). As an assessment instrument, a 50-question multiple-choice exam based on professional cybersecurity certification questions was applied to measure students' conceptual understanding of the topics covered during the course. The results were analyzed using educational statistical metrics, including mean score, median, standard deviation, and score distribution. The analysis indicated an average performance of approximately 66% correct

[1]Doutorando e Docente de Segurança Cibernética no Centro Universitário SENAI-SP, e-mail: hebert.oliveira@sp.senai.br
[2]Doutorando e Docente e Coordenador de Curso de Segurança Cibernética no Centro Universitário SENAI-SP, e-mail: caique.zaneti@sp.senai.br
[3]Mestre e Docente de Segurança Cibernética no Centro Universitário SENAI-SP, e-mail: tiago.demay@sp.senai.br.
[4] Mestre e Coordenadora de área dos cursos superiores de Tecnologia da Informação no Centro Universitário SENAI-SP, e-mail: vpreto@sp.senai.br
[5] Doutorando e Diretor do Campus São Caetano do Sul - Centro, e-mail: emerson@sp.senai.br

answers, which is close to the typical passing threshold of professional cybersecurity certifications, usually ranging from 70% to 75%. The findings suggest that the pedagogical approach adopted helps align the teaching process with industry expectations while providing quantitative indicators for evaluating learning outcomes in cryptography.

Keywords: cryptography; cybersecurity education; MSEP; educational assessment.

1 INTRODUÇÃO

O crescimento da dependência de sistemas digitais, serviços em nuvem e comunicação online ampliou significativamente a superfície de ataque das organizações, tornando a segurança da informação um dos principais desafios tecnológicos contemporâneos. Nesse contexto, a criptografia ocupa papel central na proteção de dados, na garantia da confidencialidade, integridade e autenticidade das informações e na segurança das comunicações digitais (Menezes; Van Oorschot; Vanstone, 1997; Stallings, 2017). Protocolos criptográficos como TLS, sistemas de certificados digitais e infraestruturas de chave pública tornaram-se elementos fundamentais da arquitetura de segurança da internet moderna.

Paralelamente à crescente relevância da criptografia no ambiente tecnológico, a formação de profissionais qualificados em segurança cibernética tornou-se uma prioridade para instituições educacionais, governos e organizações privadas. Relatórios internacionais apontam um déficit significativo de profissionais especializados na área de cybersecurity, o que reforça a necessidade de programas educacionais capazes de desenvolver competências técnicas alinhadas às demandas do mercado (ISC2, 2023; Petersen *et al*., 2020).

Nesse cenário, abordagens educacionais baseadas em competências têm sido adotadas como forma de aproximar a formação acadêmica das necessidades do mundo do trabalho. No Brasil, a Metodologia SENAI de Educação Profissional (MSEP) propõe um modelo pedagógico estruturado na formação por competências, no protagonismo do estudante e na articulação entre aprendizagem teórica e aplicação prática. Segundo o Serviço Nacional de Aprendizagem Industrial (2019), essa metodologia busca traduzir as demandas do mundo do trabalho em objetivos educacionais, permitindo que os processos formativos desenvolvam capacidades técnicas e comportamentais relevantes para o desempenho profissional.

A avaliação da aprendizagem desempenha papel central nesse processo, uma vez que permite monitorar o desenvolvimento das competências ao longo da formação. Em cursos da área de tecnologia e segurança da informação, avaliações baseadas em problemas reais ou em referenciais profissionais podem contribuir para reduzir a distância entre o ambiente educacional e o mercado de trabalho (Bishop; Frincke, 2005; Mulder, 2014). Nesse sentido, a utilização de questões inspiradas em certificações profissionais de segurança da informação, como CompTIA Security+, CISSP, CISM e CEH, pode representar uma estratégia relevante para avaliar o domínio conceitual dos estudantes e sua aderência às competências exigidas na área.

No campo específico do ensino de criptografia, diversos estudos apontam que o aprendizado desse conteúdo apresenta desafios pedagógicos relevantes. A criptografia envolve conceitos matemáticos abstratos, modelos de segurança e mecanismos técnicos complexos, o que exige estratégias didáticas que combinem fundamentos teóricos e aplicações práticas para promover uma aprendizagem significativa (Marin; Souza; Marin, 2021; Song; Deng, 2009). Dessa forma, avaliar o domínio desses conceitos torna-se

fundamental para compreender o nível de preparação dos estudantes em cursos de segurança cibernética.

Diante desse contexto, este estudo buscou analisar o desempenho de estudantes de um curso superior de Segurança Cibernética em uma avaliação de criptografia composta por questões de múltipla escolha baseadas em conteúdos fundamentais da área. A prova foi estruturada para abranger tópicos como criptografia simétrica, criptografia assimétrica, funções hash, infraestrutura de chaves públicas, certificados digitais e protocolos de comunicação segura.

O problema de pesquisa que orienta este trabalho pode ser formulado da seguinte forma: em que medida uma avaliação baseada em conteúdos de criptografia alinhados a certificações profissionais pode contribuir para medir o desenvolvimento de competências em segurança cibernética no contexto da educação profissional?

Assim, o objetivo geral deste estudo foi analisar o desempenho dos estudantes nessa avaliação e discutir como os resultados podem contribuir para a compreensão da aprendizagem em criptografia em cursos superiores de segurança cibernética. Como objetivos específicos, busca-se: (i) avaliar o desempenho médio dos estudantes na prova aplicada; (ii) identificar o nível de dificuldade das questões; (iii) analisar o desempenho por temas relacionados à criptografia; e (iv) discutir os resultados à luz da formação por competências proposta pela Metodologia SENAI de Educação Profissional.

2 REVISÃO DE LITERATURA

A revisão de literatura adotada neste estudo possui caráter narrativo e descritivo, tendo como finalidade contextualizar os principais referenciais relacionados à educação profissional baseada em competências, à formação em segurança cibernética, ao ensino de criptografia e aos processos de avaliação da aprendizagem. Foram considerados trabalhos acadêmicos, referenciais institucionais e frameworks profissionais diretamente relacionados ao problema de pesquisa e aos objetivos do estudo. A revisão não pretende realizar um mapeamento sistemático da literatura, mas fornecer a fundamentação conceitual necessária para a interpretação dos resultados obtidos.

2.1 Educação profissional baseada em competências

A educação profissional contemporânea tem sido progressivamente orientada por abordagens baseadas em competências, buscando alinhar a formação acadêmica às necessidades do mundo do trabalho. Diferentemente de modelos educacionais centrados exclusivamente na transmissão de conteúdo, a formação por competências enfatiza o desenvolvimento de conhecimentos, habilidades e atitudes aplicáveis a contextos profissionais reais (Mulder, 2014).

Nesse contexto, metodologias educacionais voltadas ao desenvolvimento de competências têm sido amplamente adotadas em cursos técnicos e tecnológicos, especialmente em áreas relacionadas à engenharia, tecnologia da informação e segurança cibernética. Segundo Mulder (2014), o ensino baseado em competências permite que o processo educacional esteja diretamente relacionado ao desempenho profissional esperado, tornando a avaliação da aprendizagem um elemento fundamental para verificar o

desenvolvimento dessas capacidades.

No Brasil, a Metodologia SENAI de Educação Profissional (MSEP) constitui um dos principais referenciais pedagógicos voltados à formação profissional por competências. A MSEP propõe um modelo educacional estruturado na análise das demandas do mundo do trabalho, traduzidas pedagogicamente em perfis profissionais e competências que orientam o planejamento curricular, a prática pedagógica e os processos de avaliação (Serviço Nacional de Aprendizagem Industrial, 2019).

De acordo com o Serviço Nacional de Aprendizagem Industrial (2019), a formação profissional deve ser orientada pela articulação entre teoria e prática, pelo protagonismo do estudante no processo de aprendizagem e pela utilização de situações-problema que simulam desafios reais do ambiente profissional. Nesse modelo, a avaliação da aprendizagem não se limita à verificação de conteúdos, mas busca identificar o nível de desenvolvimento das competências esperadas ao longo do processo formativo.

A adoção desse modelo é particularmente relevante em áreas tecnológicas caracterizadas por rápida evolução, como a segurança da informação. Nessas áreas, o domínio conceitual precisa ser acompanhado da capacidade de aplicar conhecimentos em cenários práticos, o que reforça a importância de metodologias educacionais alinhadas ao desenvolvimento de competências profissionais.

2.2 Formação em segurança cibernética

O aumento da dependência de sistemas digitais e a crescente sofisticação das ameaças cibernéticas têm ampliado a demanda global por profissionais qualificados em segurança da informação. De acordo com o relatório Cybersecurity Workforce Study (ISC2, 2023), o mercado global apresenta um déficit significativo de especialistas em segurança cibernética, o que evidencia a necessidade de programas educacionais capazes de formar profissionais com competências técnicas adequadas para enfrentar os desafios contemporâneos da área.

Nesse contexto, diversos referenciais internacionais têm sido desenvolvidos para orientar a formação e o desenvolvimento da força de trabalho em segurança cibernética. Um dos mais relevantes é o NICE Cybersecurity Workforce Framework, desenvolvido pelo National Institute of Standards and Technology (NIST). Esse framework organiza as atividades da área em funções, categorias de trabalho e competências, servindo como referência para programas educacionais, certificações profissionais e desenvolvimento de carreiras em segurança da informação (Petersen et al., 2020).

Segundo Petersen *et al*. (2020), a utilização de frameworks de competências permite que instituições educacionais alinhem seus currículos às necessidades do mercado, promovendo maior integração entre formação acadêmica e prática profissional. Além disso, tais frameworks podem ser utilizados para orientar a definição de objetivos de aprendizagem, a construção de avaliações e a análise do desenvolvimento de competências ao longo do processo educacional.

No campo educacional, diversos estudos apontam que programas de formação em segurança cibernética devem combinar fundamentos teóricos, desenvolvimento prático de habilidades e compreensão de cenários reais de segurança (Bishop; Frincke, 2005). Essa abordagem busca preparar os estudantes para lidar com ambientes complexos e dinâmicos, característicos da área de cibersegurança.

2.3 Ensino de criptografia na formação em segurança cibernética

A criptografia constitui um dos pilares fundamentais da segurança da informação, sendo responsável por mecanismos essenciais de proteção de dados e comunicação segura. Técnicas criptográficas são amplamente utilizadas para garantir propriedades como confidencialidade, integridade, autenticação e não repúdio em sistemas computacionais e redes de comunicação (Menezes; Van Oorschot; Vanstone, 1997; Stallings, 2017).

Entre os principais mecanismos criptográficos utilizados atualmente destacam-se os algoritmos de criptografia simétrica, como AES, algoritmos de criptografia assimétrica, como RSA e ECC, funções hash criptográficas, sistemas de autenticação baseados em HMAC e infraestruturas de chave pública utilizadas em certificados digitais e protocolos de segurança como TLS.

Apesar de sua importância, o ensino de criptografia apresenta desafios pedagógicos relevantes. Muitos conceitos criptográficos envolvem fundamentos matemáticos complexos, estruturas algorítmicas sofisticadas e modelos de segurança abstratos, o que pode dificultar a compreensão por estudantes em níveis iniciais de formação (Marin; Souza; Marin, 2021).

Diversos estudos sugerem que o ensino eficaz de criptografia deve combinar explicações conceituais, exemplos práticos e atividades que permitam aos estudantes compreender como os mecanismos criptográficos são utilizados em sistemas reais (Marin; Souza; Marin, 2021; Song; Deng, 2009). Além disso, abordagens pedagógicas baseadas em problemas e cenários práticos podem facilitar a assimilação desses conceitos e tornar o aprendizado mais significativo.

Nesse sentido, avaliações que explorem cenários práticos e aplicações reais da criptografia podem contribuir para verificar se os estudantes compreendem não apenas os conceitos teóricos, mas também suas aplicações em contextos de segurança da informação.

2.4 Avaliação de aprendizagem em segurança cibernética

A avaliação da aprendizagem constitui um componente essencial do processo educacional, especialmente em cursos orientados ao desenvolvimento de competências profissionais. Em áreas tecnológicas, a avaliação deve ser capaz de medir tanto o domínio conceitual quanto a capacidade de aplicar conhecimentos em situações práticas (Mulder, 2014).

No contexto da segurança cibernética, avaliações inspiradas em certificações profissionais têm sido utilizadas como forma de aproximar o processo educacional das exigências do mercado de trabalho. Certificações como CompTIA Security+, CISSP, CISM e CEH são amplamente reconhecidas na indústria e costumam avaliar conhecimentos fundamentais relacionados à segurança da informação, incluindo criptografia, gestão de riscos, segurança de redes e governança de segurança.

Conforme Mulder (2014), a utilização de referenciais profissionais na construção de avaliações educacionais pode contribuir para tornar o processo de aprendizagem mais alinhado às competências exigidas no mercado, além de oferecer aos estudantes uma perspectiva mais concreta sobre as expectativas profissionais da área.

Além disso, métodos quantitativos de análise de avaliações educacionais podem fornecer informações relevantes sobre o desempenho dos estudantes e a qualidade dos instrumentos de avaliação. A análise de métricas como taxa de acertos, distribuição de

desempenho e dificuldade das questões pode contribuir para identificar lacunas de aprendizagem e orientar melhorias no processo educacional.

Nesse sentido, a análise do desempenho dos estudantes em avaliações estruturadas pode representar uma ferramenta importante para compreender o desenvolvimento de competências em cursos de segurança cibernética e para aprimorar estratégias pedagógicas voltadas ao ensino de conteúdos críticos, como a criptografia.

3 METODOLOGIA

3.1 Desenho de pesquisa

Este estudo caracterizou-se como uma pesquisa quantitativa de natureza exploratória e descritiva, cujo objetivo foi analisar o desempenho de estudantes em uma avaliação de criptografia aplicada no contexto de um curso superior de Segurança Cibernética. A pesquisa buscou investigar o nível de domínio conceitual dos estudantes em temas fundamentais da criptografia, bem como identificar padrões de desempenho e possíveis lacunas de aprendizagem.

A abordagem quantitativa foi adotada devido à possibilidade de mensurar o desempenho dos estudantes por meio da análise estatística das respostas obtidas na avaliação aplicada. Esse tipo de abordagem permite identificar tendências de desempenho, níveis de dificuldade das questões e distribuição de acertos entre os participantes (Creswell, 2014).

3.2 Contexto educacional

A pesquisa foi conduzida no contexto de uma disciplina relacionada à criptografia aplicada à segurança cibernética, ministrada em um curso superior de tecnologia na área de Segurança Cibernética.

A unidade de ensino analisada corresponde à fase de Fundamentos de Criptografia, na qual são abordados conceitos essenciais para a compreensão da proteção da informação em sistemas computacionais. Entre os conteúdos trabalhados na disciplina destacam-se:

- criptografia simétrica
- criptografia assimétrica
- funções hash e HMAC
- infraestrutura de chaves públicas (PKI)
- certificados digitais
- protocolos de comunicação segura (TLS)

Esses conteúdos constituem a base conceitual necessária para o desenvolvimento de competências relacionadas à proteção de dados, autenticação de sistemas e segurança de comunicações digitais.

A disciplina foi estruturada de acordo com os princípios da Metodologia SENAI de Educação Profissional (MSEP), que orienta o processo formativo a partir do desenvolvimento de competências alinhadas às demandas do mundo do trabalho (Serviço Nacional de Aprendizagem Industrial, 2019).

3.3 Participantes

Os participantes da pesquisa foram estudantes matriculados na disciplina de criptografia aplicada à segurança cibernética durante o período letivo analisado.

A amostra é composta pelos estudantes que realizaram a avaliação aplicada ao final da unidade de fundamentos de criptografia. A participação corresponde ao conjunto de alunos presentes no momento da aplicação da prova, sendo considerada uma amostra por conveniência, comum em pesquisas educacionais conduzidas em ambientes de sala de aula (Creswell, 2014).

3.4 Instrumento de avaliação

O instrumento de coleta de dados utilizado neste estudo foi uma prova objetiva composta por questões de múltipla escolha, elaborada para avaliar o domínio conceitual dos estudantes em temas fundamentais da criptografia.

As questões foram construídas com base em conteúdos presentes em certificações profissionais amplamente reconhecidas na área de segurança da informação, incluindo:

1 CompTIA Security+
2 CISSP
3 CISM
4 CEH
5 GIAC

O objetivo da prova foi avaliar a compreensão dos estudantes sobre conceitos fundamentais da criptografia e sua aplicação em cenários de segurança da informação.

As questões abordaram temas como:

a) confidencialidade e integridade da informação
b) funcionamento de algoritmos criptográficos
c) mecanismos de autenticação
d) aplicações de funções hash
e) infraestrutura de chaves públicas
f) certificados digitais
g) protocolos de segurança

A avaliação foi composta por 50 questões de múltipla escolha, cada uma com cinco alternativas e apenas uma resposta correta.

3.5 Coleta de dados

Os dados utilizados na pesquisa foram obtidos a partir das respostas dos estudantes registradas em uma planilha eletrônica. Para cada aluno participante, foram coletadas as respostas fornecidas para cada questão da prova.

A base de dados resultante permite identificar:

a) respostas corretas e incorretas por questão
b) desempenho individual dos estudantes
c) número total de acertos por participante

Essas informações constituem a base para a análise quantitativa do desempenho da turma.

3.6 Procedimentos de análise

A análise dos dados foi realizada por meio de técnicas estatísticas descritivas, com o objetivo de identificar padrões de desempenho dos estudantes na avaliação aplicada.
As métricas analisadas incluem:

3.6.1 Taxa média de acertos

A taxa média de acertos representa o desempenho geral da turma na avaliação, sendo calculada pela razão entre o número total de respostas corretas e o número total de questões respondidas.

3.6.2 Distribuição de notas

A distribuição das notas será analisada por meio de medidas estatísticas como média, mediana e desvio padrão, permitindo compreender a variação de desempenho entre os estudantes.

3.6.3 Índice de dificuldade das questões

O índice de dificuldade de cada questão será calculado com base na proporção de estudantes que responderam corretamente a cada item da prova.

Essa métrica permite classificar as questões de acordo com seu nível de dificuldade: fáceis, médias e difíceis.

3.6.4 Desempenho por tema

As questões da prova serão agrupadas de acordo com os temas de criptografia abordados, permitindo analisar o desempenho dos estudantes em diferentes tópicos da disciplina.

Essa análise permite identificar possíveis áreas de maior ou menor domínio conceitual por parte dos estudantes.

3.7 Ferramentas utilizadas

A análise dos dados foi realizada utilizando ferramentas de análise estatística e visualização de dados em ambiente Python, por meio da plataforma Google Colab. Utilizou-se bibliotecas como:

- Pandas (manipulação de dados)
- NumPy (operações estatísticas)
- Matplotlib (visualização de dados)
- Seaborn (análise gráfica)

Essas ferramentas permitem processar os dados da planilha de respostas e gerar gráficos e métricas estatísticas que auxiliam na interpretação dos resultados.

4 RESULTADOS E DISCUSSÕES

4.1 Estatísticas descritivas do desempenho

A análise inicial consistiu na obtenção de estatísticas descritivas que permitissem compreender o desempenho geral da turma na avaliação.

Tabela 1 - Estatísticas descritivas do desempenho da turma

Métrica	Valor
Número de alunos	44
Número de questões	50
Média de acertos	33,20
Mediana	34
Menor nota	17
Maior nota	48
Média (%)	66,4%

Fonte: Elaborada pelos autores (2026).

A média de acertos foi de aproximadamente 33 questões, correspondendo a 66,4% da prova, indicando que a maioria dos estudantes demonstrou compreensão satisfatória dos conteúdos abordados.

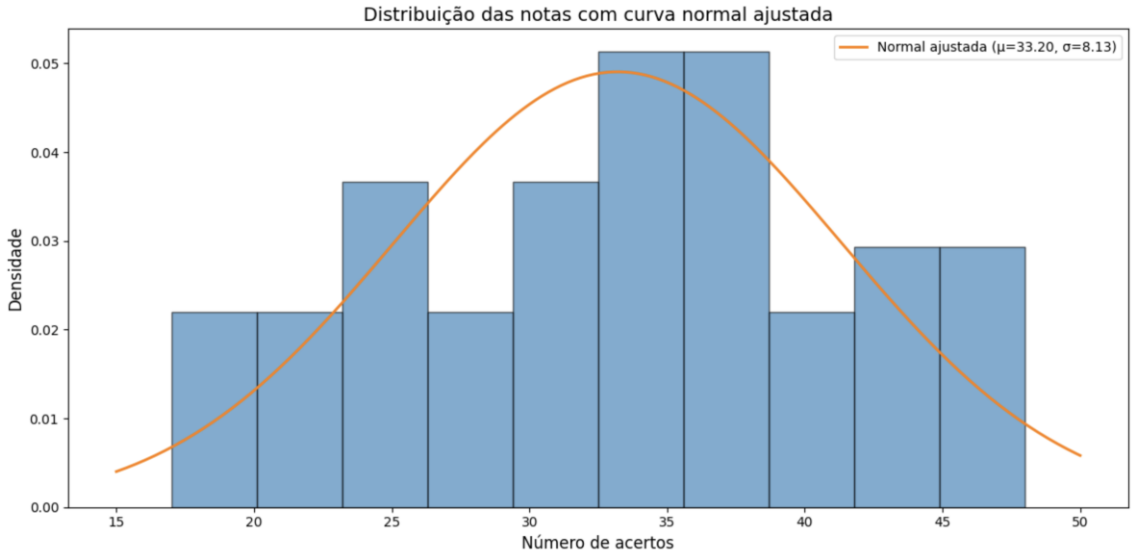
A mediana de 34 acertos sugere que metade da turma obteve desempenho igual ou superior a esse valor.

O desvio padrão de 8,13 indica uma variabilidade moderada entre os resultados, sugerindo diferenças no nível de domínio conceitual entre os estudantes.

4.2 Distribuição das notas

Para compreender a distribuição do desempenho da turma, foi elaborado o histograma apresentado na Figura 1, que representa a frequência das pontuações obtidas pelos estudantes ao longo da avaliação, juntamente com uma curva normal ajustada aos dados.

Figura 1 - Distribuição das notas dos estudantes com curva normal ajustada



Fonte: Elaborada pelos autores (2026).

Observa-se na Figura 1 que a maior parte das pontuações se concentra na região intermediária da distribuição, principalmente entre 28 e 38 acertos. A média de 33,2 questões e a mediana de 34 acertos apresentam valores próximos, indicando uma distribuição relativamente equilibrada dos resultados. A presença de poucos valores nas extremidades também evidencia diferentes níveis de desempenho entre os estudantes, sem concentração excessiva nas menores ou maiores pontuações.

O histograma permite visualizar a concentração das notas ao longo da escala de pontuação. Observa-se que a maior parte dos estudantes obteve pontuação na faixa intermediária da distribuição, principalmente entre 28 e 38 acertos.

Para complementar essa análise, foi ajustada uma curva de distribuição normal sobre os dados observados. A aproximação da distribuição das notas a uma curva normal sugere que a avaliação apresentou nível de dificuldade adequado, sendo capaz de diferenciar diferentes níveis de desempenho entre os estudantes.

Além disso, a presença de poucos valores extremos, com nota mínima de 17 acertos e máxima de 48 acertos, indica que a prova conseguiu discriminar adequadamente os níveis de conhecimento sem gerar concentração excessiva nas extremidades da escala.

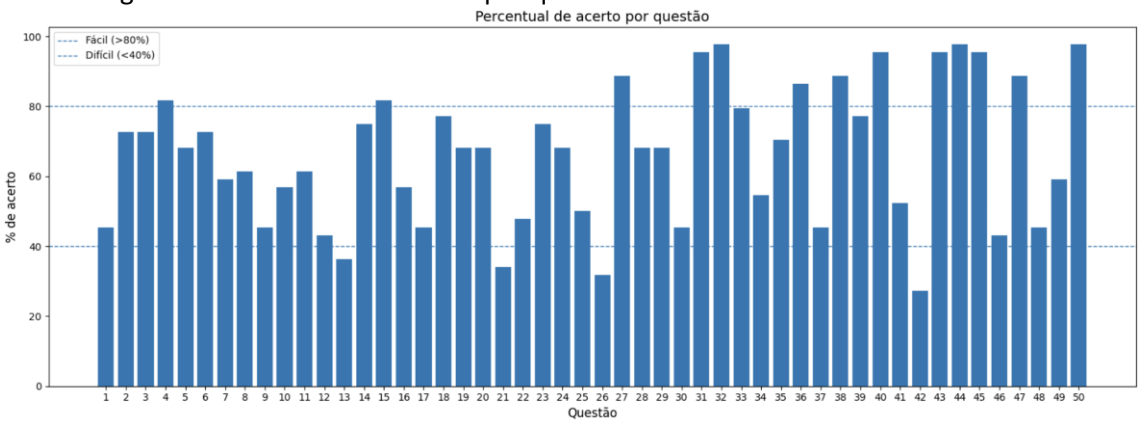
4.3 Análise de dificuldade das questões

Com base na proporção de estudantes que responderam corretamente a cada item da prova, foi possível calcular o índice de dificuldade das questões.

Esse índice corresponde à proporção de acertos em cada questão e permite identificar quais conteúdos apresentaram maior ou menor grau de dificuldade para os estudantes.

Além da análise do desempenho geral da turma, foi calculado o percentual de acertos obtido em cada uma das 50 questões da avaliação. A Figura 2 apresenta essa distribuição, permitindo identificar os itens que apresentaram maior ou menor nível de acerto entre os estudantes.

Figura 2 - Percentual de acertos por questão



Fonte: Elaborada pelos autores (2026).

A Figura 2 evidencia variação considerável no percentual de acertos entre as questões. Alguns itens apresentaram elevado índice de respostas corretas, sugerindo maior domínio dos conceitos avaliados, enquanto outros registraram percentuais inferiores, indicando conteúdos ou situações-problema que apresentaram maior dificuldade para os estudantes. Essa análise permite identificar pontos específicos que podem ser retomados ou aprofundados em futuras aplicações da disciplina.

Cada barra representa a proporção de estudantes que responderam corretamente a uma questão específica.

Essa análise permite identificar padrões relevantes, como:

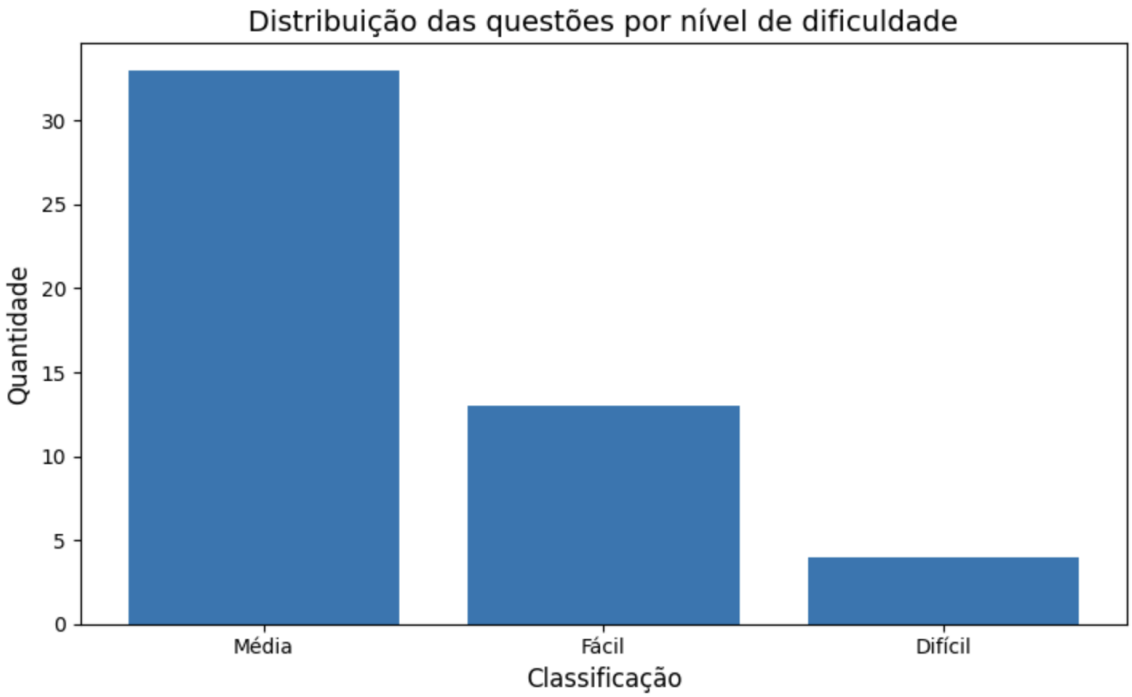
a) questões com alta taxa de acerto, indicando domínio conceitual
b) questões com taxa intermediária, indicando compreensão parcial
c) questões com baixa taxa de acerto, indicando maior dificuldade conceitual

A identificação dessas questões é particularmente relevante para fins pedagógicos, pois permite ao docente revisar conteúdos que podem exigir abordagens didáticas adicionais.

4.4 Classificação das questões por nível de dificuldade

Com base no percentual de acertos de cada item, as questões foram classificadas em três níveis de dificuldade: fáceis, quando apresentaram taxa de acerto superior a 80%; intermediárias, quando a taxa de acerto ficou entre 50% e 80%; e difíceis, quando menos de 50% dos estudantes responderam corretamente. A distribuição dessas categorias é apresentada na Figura 3.

Figura 3 - Distribuição das questões por nível de dificuldade



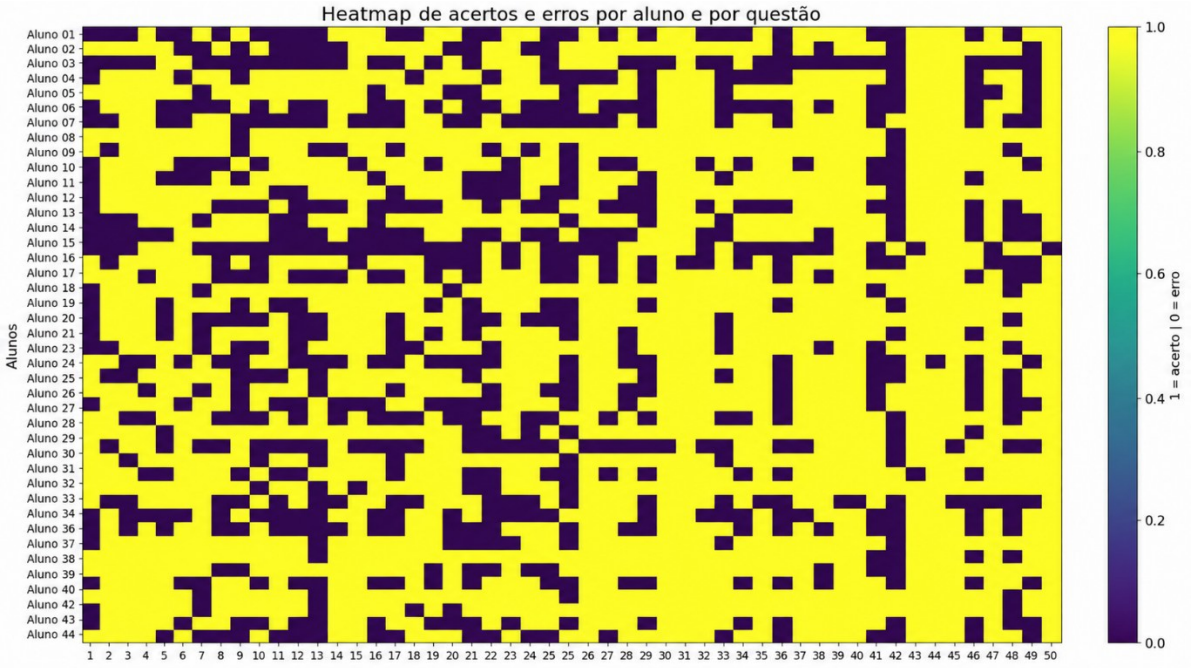
Fonte: Elaborado pelos autores (2026).

Conforme apresentado na Figura 3, predominam questões classificadas com dificuldade intermediária, correspondendo à maior parcela da avaliação, enquanto um número menor de itens foi classificado como fácil ou difícil. Essa distribuição indica que a prova concentrou a maior parte de seus itens em um nível intermediário de exigência, permitindo avaliar diferentes níveis de domínio conceitual sem predominância de questões excessivamente simples ou complexas.

4.5 Heatmap de desempenho dos estudantes

Para complementar as análises agregadas e observar simultaneamente o comportamento dos estudantes e das questões, foi elaborado o mapa de calor apresentado na Figura 4. Cada linha representa um estudante anonimizado e cada coluna corresponde a uma das 50 questões da avaliação, permitindo visualizar os padrões de acerto e erro ao longo da prova.

Figura 4 - Mapa de calor dos acertos e erros dos estudantes por questão.



Fonte: Elaborada pelos autores (2026).

A Figura 4 permite observar tanto diferenças individuais de desempenho quanto padrões coletivos de resposta. Regiões com maior concentração de erros podem indicar questões ou conceitos que apresentaram dificuldade para uma parcela significativa da turma, enquanto sequências predominantes de acertos sugerem maior consolidação dos conteúdos avaliados. O mapa também evidencia a heterogeneidade de desempenho entre os estudantes, complementando as medidas estatísticas apresentadas anteriormente.

4.6 Desempenho por tema da criptografia

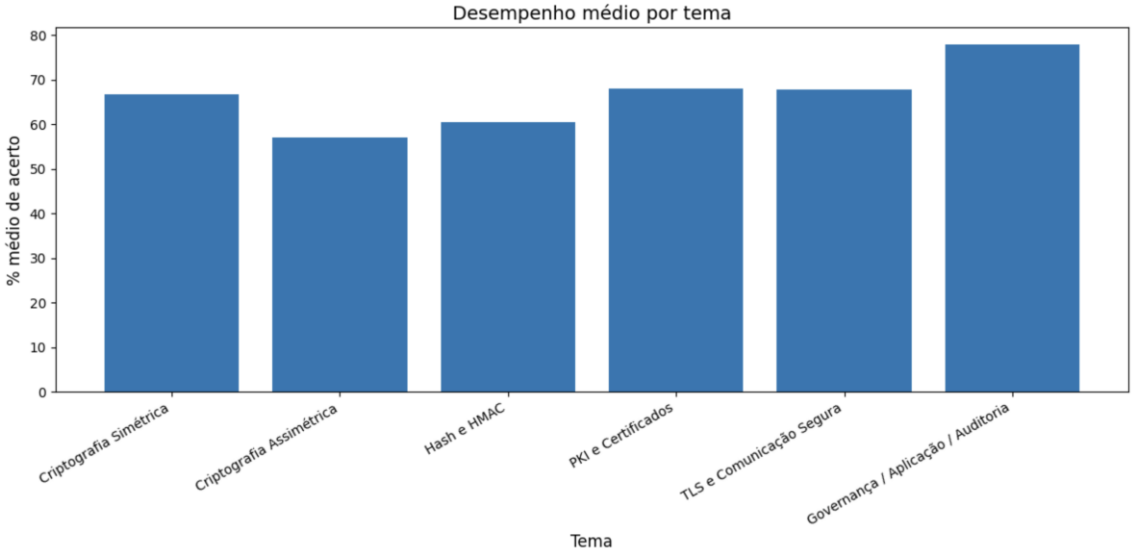
As questões da prova foram agrupadas de acordo com os principais tópicos abordados na disciplina, permitindo analisar o desempenho dos estudantes em diferentes áreas do conteúdo de criptografia.

Os temas considerados incluem:

a) criptografia simétrica
b) criptografia assimétrica
c) funções hash
d) infraestrutura de chave pública (PKI)
e) certificados digitais
f) protocolos de comunicação segura

Além da análise individual das questões, os itens da avaliação foram agrupados conforme os principais temas de criptografia abordados na disciplina. A Figura 5 apresenta o percentual médio de acertos em cada grupo temático, permitindo comparar o nível de domínio demonstrado pelos estudantes em diferentes conteúdos.

Figura 5 - Desempenho médio dos estudantes por tema de criptografia.



Fonte: Elaborada pelos autores (2026).

A análise apresentada na Figura 5 evidencia diferenças de desempenho entre os temas avaliados. Alguns conteúdos apresentaram percentuais médios de acerto superiores, indicando maior domínio conceitual por parte dos estudantes, enquanto outros obtiveram resultados relativamente menores e podem demandar maior atenção pedagógica. Essa comparação fornece ao docente informações mais específicas sobre os conteúdos que podem ser reforçados em futuras edições da disciplina, contribuindo para o aprimoramento contínuo do processo de ensino-aprendizagem.

A literatura sobre experiências de ensino de criptografia destaca a importância de estratégias didáticas que articulem fundamentos conceituais e atividades aplicadas, especialmente em contextos de formação tecnológica (Marin; Souza; Marin, 2021; Song; Deng, 2009).

4.7 Interpretação pedagógica dos resultados

Sob a perspectiva pedagógica, os resultados obtidos indicam que a estratégia de ensino baseada na Metodologia SENAI de Educação Profissional (MSEP) contribuiu para o desenvolvimento das competências técnicas relacionadas aos fundamentos da criptografia.

A MSEP enfatiza a aprendizagem baseada em situações-problema, aplicação prática e protagonismo do estudante, favorecendo a construção de conhecimento significativo.

A análise quantitativa do desempenho permitiu identificar lacunas específicas de aprendizagem e ajustar estratégias pedagógicas para futuras edições da disciplina.

Além disso, avaliações inspiradas em certificações profissionais de segurança da informação podem contribuir para alinhar o processo educacional às competências exigidas no mercado, conforme sugerido por frameworks como o NICE Cybersecurity Workforce Framework (Petersen *et al*., 2020).

Assim, a utilização de métodos quantitativos para analisar avaliações educacionais pode representar uma ferramenta relevante para aprimorar continuamente o ensino de conteúdos críticos da segurança da informação, como a criptografia.

5 CONCLUSÃO

Este estudo teve como objetivo avaliar o nível de aprendizagem dos estudantes na disciplina de criptografia aplicada à segurança cibernética, utilizando como instrumento de medição uma prova composta por questões de certificações profissionais da área. A avaliação foi conduzida dentro da Metodologia SENAI de Educação Profissional (MSEP), que enfatiza a aprendizagem baseada em problemas, contextualização com cenários reais e desenvolvimento de competências aplicáveis ao mercado de trabalho.

A análise estatística dos resultados permitiu observar indicadores importantes sobre o desempenho da turma. Entre as principais métricas analisadas estão média de acertos, mediana, desvio padrão, distribuição das notas, porcentagem média de acertos e desempenho por questão. Os dados mostraram uma média de aproximadamente 33 acertos em um total de 50 questões, o que corresponde a cerca de 66% de aproveitamento médio. A mediana próxima da média indica uma distribuição relativamente equilibrada das notas, enquanto o desvio padrão evidencia uma variação moderada entre os desempenhos individuais dos estudantes. Além disso, a análise de itens e o mapa de calor das respostas permitiram identificar quais questões apresentaram maior taxa de erro ou acerto, fornecendo indícios sobre os tópicos de criptografia que foram melhor assimilados ou que ainda demandam reforço pedagógico.

Considerando que a prova foi composta por questões reais de certificações profissionais, é possível realizar uma aproximação com os critérios normalmente exigidos nesses exames. De modo geral, certificações da área de segurança da informação costumam exigir entre 70% e 75% de acertos para aprovação. Nesse contexto, a média da turma (aproximadamente 66%) indica que uma parcela significativa dos estudantes estaria próxima da aprovação, embora a média geral ainda fique ligeiramente abaixo do limiar típico exigido por certificações. No entanto, ao observar o desempenho individual, verifica-se que diversos alunos atingiram pontuações superiores a esse limite, sugerindo que parte da turma já apresenta nível de conhecimento compatível com exames profissionais.

Do ponto de vista pedagógico, os resultados indicam que a aplicação da MSEP contribuiu para o desenvolvimento de competências relevantes, especialmente na compreensão conceitual e na aplicação prática de mecanismos criptográficos. A utilização de questões baseadas em certificações também se mostrou uma estratégia eficaz para aproximar o processo de avaliação do nível de exigência do mercado, permitindo que os estudantes tenham contato com o padrão de dificuldade encontrado em exames profissionais.

Por fim, conclui-se que os estudantes demonstraram nível consistente de aprendizagem em criptografia, com desempenho médio próximo ao exigido por certificações da área. A análise das métricas também evidencia oportunidades de melhoria, especialmente no aprofundamento de determinados tópicos e na ampliação de atividades práticas. Como trabalhos futuros, recomenda-se a aplicação de avaliações ao longo do curso, bem como a comparação longitudinal entre turmas, permitindo acompanhar a evolução do desempenho

dos estudantes e aprimorar continuamente o processo de ensino-aprendizagem em segurança cibernética.

REFERÊNCIAS

BISHOP, Matt; FRINCKE, Deborah A. Teaching secure programming. **IEEE Security & Privacy**, v. 3, n. 5, p. 54-56, 2005. DOI: https://doi.org/10.1109/MSP.2005.133 .

CRESWELL, John W. **Research design**: qualitative, quantitative, and mixed methods approaches. 4. ed. Thousand Oaks: SAGE Publications, 2014.

ISC2. **ISC2 Cybersecurity Workforce Study 2023**. ISC2, 2023.

MARIN, Regina Paiva Melo; SOUZA, Jackson Gomes Soares; MARIN, Luciano Heitor Gallegos. Ensinando conceitos básicos de criptografia no ensino médio profissional. **Revista on line de Política e Gestão Educacional**, Araraquara, v. 25, n. 2, p. 1277-1290, maio/ago. 2021. DOI: https://doi.org/10.22633/rpge.v25i2.14469 . Disponível em: https://periodicos.fclar.unesp.br/rpge/pt_BR/article/view/14469 . Acesso em: 10 nov 2025.

MENEZES, Alfred J.; VAN OORSCHOT, Paul C.; VANSTONE, Scott A. **Handbook of applied cryptography**. Boca Raton: CRC Press, 1997.

MULDER, Martin. Conceptions of professional competence. In: BILLETT, Stephen; HARTEIS, Christian; GRUBER, Hans (ed.). **International handbook of research in professional and practice-based learning**. Dordrecht: Springer, 2014. p. 107-137. DOI: https://doi.org/10.1007/978-94-017-8902-8_5.

PETERSEN, Rodney; SANTOS, Danielle; WETZEL, Karen; SMITH, Matthew; WITTE, Greg. **Workforce framework for cybersecurity (NICE Framework)**. Gaithersburg: National Institute of Standards and Technology, 2020. (NIST Special Publication 800-181 Rev. 1). DOI: https://doi.org/10.6028/NIST.SP.800-181r1 .

SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL. Departamento Nacional. **Metodologia SENAI de educação profissional**. Brasília, DF: SENAI/DN, 2019.

SONG, Xiuli; DENG, Hongyao. Taking flexible and diverse approaches to get undergraduate students interested in cryptography course. *In*: INTERNATIONAL WORKSHOP ON EDUCATION TECHNOLOGY AND COMPUTER SCIENCE, 1., 2009. **Proceedings [...]**. [S. l.]: IEEE, 2009. v. 2, p. 490-494. DOI: https://doi.org/10.1109/ETCS.2009.371.

STALLINGS, William. **Cryptography and network security: principles and practice**. 7. ed. [S. l.]: Pearson, 2017.

Sobre os Autores:

_____

[i] Hebert de Oliveira Silva



Mestre e Doutorando em Tecnologia da Informação pela UNICAMP; Coordenador de Cibersegurança no Grupo Hapvida e professor (IBMEC, Impacta, UNIP e SENAI Informática). Atuação em Blue/Red Team, governança e resposta a incidentes, com foco em aprendizado federado, IA e segurança em CPS/IoT. Autor de livros e artigos IEEE, ACM e Elsevier.
https://orcid.org/0000-0002-0186-5925

[ii] Caique Zaneti Kirilo



Possui bacharelado em Ciência da Computação (2012-2015); Mestrado em Engenharia de Produção com ênfase em Inteligência Artificial na linha de pesquisa de Métodos Quantitativos em Engenharia de Produção (2016-2017); É Doutorando em Engenharia Elétrica e da Informação pela Universidade Federal do ABC. Atua como Professor Universitário e Pesquisador integrante do Grupo de Pesquisa de Engenharia de Software aplicada à criação de Sistemas Críticos.
https://orcid.org/0000-0001-5667-0861

[iii] Tiago Augusto Orcajo Demay Cordeiro



Mestre em Engenharia de Computação (Poli-USP), pós-graduado em Computação em Nuvem e graduado em Engenharia Eletrônica (IMT). Atua no Insper (Laboratório de Redes e Supercomputação) e como professor de Computação em Nuvem. Pesquisa em redes, segurança com IA e HPC.
https://orcid.org/0000-0002-4991-478

[iv] Vivian de Oliveira Preto



Graduada em Tecnologia Gráfica (Faculdade SENAI Theobaldo de Nigris) e Mestre em Educação (UNESP/Marília). Coordenadora dos cursos superiores de Tecnologia em Ciência de Dados e Segurança Cibernética da Faculdade SENAI Mecatrônica (Campus Paulo Antônio Skaf). https://orcid.org/0009-0006-0193-5571

[v] Emerson Costa Santos



Diretor de Unidade de Formação Profissional do SENAI-SP, com atuação em planejamento, gestão e avaliação de Escola e Faculdade. Professor Convidado na Sheridan College (Canadá). Doutorando em Sociologia, Mestre em Engenharia Elétrica e Engenheiro Mecânico. Pesquisador no C4AI-USP, CECS-UFABC (Indústria 4.0) e Expert Independente da WorldSkills International. Experiência como especialista e docente em Educação Profissional nas áreas de Manutenção Industrial, Automação, Ferramentaria e EJA.
https://orcid.org/0000-0002-4730-9983