AVALIAÇÃO DE QUALIDADE DA SEGURANÇA DA INFORMAÇÃO UTILIZANDO INTELIGÊNCIA ARTIFICIAL GENERATIVA EM SOFTWARE PÚBLICO BASEADO NA ISO/IEC 25010.

EVALUATION OF INFORMATION SECURITY QUALITY USING GENERATIVE ARTIFICIAL INTELLIGENCE IN PUBLIC SOFTWARE BASED ON ISO/IEC 25010

MARCOS FRANCISCO
UNIDADE DE POS GRADUAÇÃO, EXTENSÃO E PESQUISA - CENTRO PAULA SOUZA

CARLOS HIDEO ARIMA

ELIACY CAVALCANTI LÉLIS
FACULDADE DE TECNOLOGIA DE SÃO PAULO

MARILIA MACORIN DE AZEVEDO
CENTRO PAULA SOUZA

Comunicação:
O XIII SINGEP foi realizado em conjunto com a 13th Conferência Internacional do CIK (CYRUS Institute of Knowledge), em formato híbrido, com sede presencial na UNINOVE - Universidade Nove de Julho, no Brasil.

Agradecimento à orgão de fomento:
Agradeço a todos os colegas que contribuíram para a construção deste artigo na disciplina de Gestão da Qualidade. Estendo meus agradecimentos às professoras Eliacy e Marília, bem como ao meu orientador, Professor Doutor Carlos Arima, pelo apoio e orientação ao longo deste trabalho.

AVALIAÇÃO DE QUALIDADE DA SEGURANÇA DA INFORMAÇÃO UTILIZANDO INTELIGÊNCIA ARTIFICIAL GENERATIVA EM SOFTWARE PÚBLICO BASEADO NA ISO/IEC 25010.

Objetivo do estudo
Este trabalho tem como objetivo identificar e comparar a efetividade das ameaças de segurança da informação geradas pelas ferramentas de inteligência artificial generativa durante o processo de desenvolvimento de produtos digitais.

Relevância/originalidade
A identificação de vulnerabilidades cibernéticas costuma exigir muito conhecimento técnico para análise. Este trabalho propõe um direcionamento estruturado para a avaliação da qualidade de software, utilizando ferramentas de inteligência artificial generativa.

Metodologia/abordagem
O presente estudo foi dividido em três partes: fundamentação teórica, revisão sistemática da literatura e desenvolvimento de um framework para avaliação da qualidade de software.

Principais resultados
O principal resultado foi a criação de um framework baseado em engenharia de prompt, com critérios bem definidos, para auxiliar na identificação da qualidade de softwares, com foco em segurança da informação.

Contribuições teóricas/metodológicas
O presente artigo tem como contribuição acadêmica, o desenvolvimento de uma metodologia acerca do uso de inteligência artificial generativas, visando o aumento dos níveis de qualidade de software.

Contribuições sociais/para a gestão
O desenvolvimento de um framework estruturado aplicado para inteligência artificial generativa para práticas de segurança da informação pode diminuir o grau de exposição ao risco para ciberataques.

Palavras-chave: qualidade de software, inteligência generativa, segurança da informação, software público

EVALUATION OF INFORMATION SECURITY QUALITY USING GENERATIVE ARTIFICIAL INTELLIGENCE IN PUBLIC SOFTWARE BASED ON ISO/IEC 25010

Study purpose
This work aims to identify and compare the effectiveness of information security threats generated by generative artificial intelligence tools during the digital product development process.

Relevance / originality
The identification of cyber vulnerabilities often requires a lot of technical expertise for analysis. This work proposes a structured approach for evaluating software quality using generative artificial intelligence tools.

Methodology / approach
This study was divided into three parts: theoretical foundation, systematic literature review, and the development of a framework for software quality evaluation.

Main results
The main outcome was the creation of a framework based on prompt engineering, with well-defined criteria, to assist in assessing software quality with a focus on information security.

Theoretical / methodological contributions
This paper contributes academically by developing a methodology for the use of generative AI aimed at improving software quality levels.

Social / management contributions
The development of a structured framework applied to generative artificial intelligence for information security practices can reduce the level of exposure to cyberattack risks.

Keywords: software quality, generative intelligence, information security, public software

AVALIAÇÃO DE QUALIDADE DA SEGURANÇA DA INFORMAÇÃO UTILIZANDO INTELIGÊNCIA ARTIFICIAL GENERATIVA EM SOFTWARE PÚBLICO BASEADO NA ISO/IEC 25010:2011.

1. INTRODUÇÃO

A sociedade moderna vivencia um processo avançado de digitalização e disseminação da informação. Com o amplo uso de sistemas e dispositivos móveis, a tecnologia tornou-se parte integrante do cotidiano, estando presente por meio de aplicativos, sistemas e em toda a cadeia produtiva e empresarial. No entanto, esse novo contexto tecnológico ampliou os desafios relacionados à segurança da informação (Fadilah, Maulidiya, Rochimah, 2023).

De acordo com Olatunji et al. (2023), a transformação digital intensificou exponencialmente as preocupações com a segurança, tornando esse tema crítico no cenário global. Incidentes envolvendo vulnerabilidades financeiras têm causado impactos significativos no setor empresarial. Segundo Guembe et al. (2022), as estimativas indicam que, somente no ano de 2022, os prejuízos financeiros decorrentes de incidentes de segurança alcançaram cerca de US$ 400 bilhões na economia global.

Cadeias produtivas globalizadas exigem sistemas conectados e interligados. Essa heterogeneidade, aliada à utilização de sistemas desenvolvidos internamente por empresas ou adquiridos de terceiros, gera uma complexidade adicional no contexto da segurança da informação. Para Guembe, Samonte, Adolfo e Ampiloquio (2022), sistemas integrados combinam diversos componentes, físicos e lógicos, criando arquiteturas e ecossistemas sofisticados e interconectados que operam de forma eficiente.

Segundo Oun, Wince e Cheng (2025), esses sistemas e tecnologias podem possibilitar a coleta e a análise de dados pessoais e corporativos, o que os torna vetores de risco no ambiente empresarial. Diante disso, é necessário considerar os aspectos de qualidade do *software*, especialmente no que diz respeito à segurança e à confiabilidade, desde as etapas iniciais de seu desenvolvimento.

Frameworks específicos permitem a observação de critérios previamente definidos, que servem como referência para o atendimento aos requisitos de qualidade. A norma ISO/IEC 25010 estabelece esses parâmetros. Conforme Nurdayenti e Amiruddin (2022), a adoção dos critérios de avaliação definidos pela ISO/IEC 25010 viabiliza uma análise mais precisa da segurança, dos mecanismos de privacidade e do uso adequado dos dados.

No entanto, a principal limitação dessas metodologias reside na dependência de um conjunto finito de artefatos manualmente elaborados, o que restringe sua capacidade de se adaptar a cenários de ameaças diversos ou inéditos. O processo de criação desses artefatos é trabalhoso e oferece cobertura limitada, deixando lacunas no enfrentamento de todo o espectro de comportamentos sofisticados de *malware*.

A Inteligência Artificial Generativa (GenAI) apresenta uma alternativa transformadora ao automatizar a criação de artefatos de engano adaptativos e conscientes do contexto. Capaz de gerar estratégias escaláveis e diversificadas, adaptadas a táticas específicas de *malware*, a GenAI reduz o esforço manual ao mesmo tempo em que melhora significativamente a adaptabilidade em tempo de execução e a aplicabilidade no mundo real.

Expandir além da geração estática de recursos para abranger mecanismos mais sofisticados e adaptativos pode melhorar enormemente a escalabilidade e a eficácia da dissuasão cibernética. Esta pesquisa procura preencher essa lacuna ao analisar empiricamente o desempenho de modelos de GenAI, ChatGPT Mini, Gemini e Claude— na geração autônoma de estratégias de engano diversas, adaptativas e realistas.

Um fator-chave que viabiliza o potencial da GenAI na dissuasão cibernética é o PE estruturado (Engenharia de Prompt estruturado), que projeta entradas específicas para orientar os modelos de GenAI na produção de saídas precisas, acionáveis e aplicáveis. Pesquisas recentes apresentam que *prompts* bem elaboradas, aumentam significativamente a relevância e a eficácia das respostas da GenAI. Este trabalho propõe a criação de um *framework* com critérios e desafios para criação de *prompts* de segurança.

2. FUNDAMENTAÇÃO TEÓRICA

Nesta seção é apresentado o referencial teórico que embasa o presente estudo.

2.1. Gestão da Qualidade de Software ISO 25010

A conectividade viabilizada por *softwares* e soluções digitais estabelece um novo perímetro na relação entre segurança e confiabilidade entre os diversos atores envolvidos nos processos tecnológicos. De um lado, encontram-se os proprietários e desenvolvedores de *software*, responsáveis pela criação de produtos escaláveis, flexíveis e estáveis. Do outro lado, estão os usuários, que dependem da tecnologia para a maior parte de suas atividades básicas, como pagamentos, transporte público e acesso a sistemas de saúde. Por isso, garantir a segurança dessas soluções torna-se um desafio crescente.

Segundo Fadilah, Maulidiya e Rochimah (2023), pesquisas recentes vêm destacando a importância de estabelecer critérios de qualidade de *software* como elementos fundamentais para assegurar a segurança das aplicações, promovendo seu uso confiável e sustentável. A norma ISO/IEC 25010:2011 tem sido utilizada como uma extensão de controle que define mecanismos e critérios de segurança para produtos digitais em escala global (Sekarini, Alfinani, Rochimah, 2020).

A definição de critérios comparativos padronizados para atributos como usabilidade, desempenho e segurança em sistemas de informação estabelece uma referência internacional, independente de avaliadores específicos. Essa padronização fornece um arcabouço consistente, com métricas e artefatos voltados à avaliação de produtos digitais (Nurdayenti, Amiruddin, 2020).

As dimensões de segurança estabelecidas pela ISO/IEC 25010:2011 incluem:

i) Confidencialidade,
ii) Integridade,
iii) Não repúdio (*non-repudiation*),
iv) Responsabilidade (*accountability*) e
v) Autenticidade.

2.2. Cibersegurança

A proteção dos perímetros lógicos e físicos, somada ao aumento do uso de novas tecnologias como alavanca de transformação e geração de negócios, delineou um novo paradigma corporativo. Nessa perspectiva, a disciplina de Cibersegurança tem se tornado cada vez mais estratégica nas organizações. À medida que novas tecnologias avançam, as ameaças à segurança também se intensificam de forma assimétrica, elevando os riscos. Torna-se, portanto, um desafio para as empresas a adoção de mecanismos eficazes de proteção da privacidade e da segurança.

A Cibersegurança consiste na prática de proteger recursos, processos e infraestruturas contra-ataques maliciosos, com o objetivo de evitar acessos não autorizados, danos à integridade das informações ou prejuízos à imagem institucional (Hasanov et al., 2024). O ciberataque, nesse contexto, é definido como a exploração intencional de sistemas computacionais, redes e ativos empresariais com fins maliciosos.

Com o aumento da sofisticação dos ataques, os especialistas em segurança encontram dificuldades para realizar avanços significativos na prevenção ou antecipação de ameaças (Guembe et al., 2022). Diante disso, a integração de novas tecnologias aplicadas à Cibersegurança, visando o aumento da cobertura da superfície de testes, surge como uma oportunidade promissora.

A aliança entre a atuação humana e os recursos tecnológicos se mostra essencial na busca por uma Cibersegurança mais abrangente, tanto em espaços públicos quanto privados, elevando, assim, o nível de proteção aos usuários finais.

2.3. Inteligência artificial generativa

Nos últimos anos, o uso prático, a facilidade de implementação e o custo acessível — em alguns casos, inclusive com opções gratuitas — têm despertado o interesse de adoção de novas tecnologias em diferentes processos de negócio. No campo da Cibersegurança, a Inteligência Artificial (IA) generativa surge como um potencial aliada em diversos casos de uso, como: conscientização, detecção de vulnerabilidades e identificação de ameaças de forma eficiente.

O rápido crescimento no uso de IA para fins de detecção e análise tem se tornado uma tendência frequente no campo da segurança cibernética. A IA vem ganhando protagonismo pela sua capacidade de executar atividades repetitivas com maior eficiência (Oun, Wince, Cheng, 2025). Por meio de técnicas avançadas, é possível identificar e acompanhar padrões maliciosos, minimizando falhas causadas por erro humano (Hasanov et al., 2024).

O uso da IA generativa se mostra mais efetivo quando há um correto direcionamento para a extração de valor das plataformas. Segundo Qinyuan et al. (2024), a engenharia de *prompts (prompt engineering*) estruturada é vista como uma disciplina para otimizar o potencial dos modelos de linguagem (LLMs) em tarefas de Cibersegurança, assegurando que as estratégias de defesa geradas sejam precisas, acionáveis e viáveis de serem implementadas.

Os autores propõem a estrutura SPADE *(Situation, Problem, Analysis, Decision and Execution.*) como um exemplo que visa padronizar e otimizar o processo de geração de *prompts*, permitindo a criação de estratégias de decepção cibernética adaptativas e realistas. A capacidade de gerar cenários de segurança de forma dinâmica — em contraposição aos tradicionais cenários estáticos — aumenta significativamente a adaptabilidade e a eficácia diante de ameaças em constante evolução (Qinyuan et al., 2024).

3. METODOLOGIA

Esta seção relata as metodologias aplicadas a este estudo.

3.1. Critérios de Busca e Identificação dos Estudos

Os seguintes parâmetros de busca foram utilizados para encontrar literatura relevante para este estudo:

1) Elaborar uma lista de palavras-chave com base nas perguntas de pesquisa;
2) Identificar palavras-chave na literatura relevante;

3) Reconhecer sinônimos e variações ortográficas das palavras-chave;
4) Relacionar palavras-chave e conceitos principais utilizando os operadores booleanos "AND" e "OR".

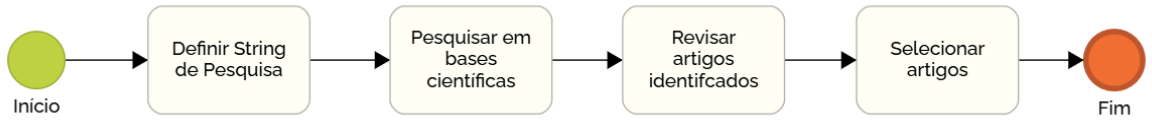
Neste estudo, os dados foram extraídos de sete bases de dados digitais. As bibliotecas digitais utilizadas foram: Web of Science, Scopus, IEEE Xplore. Foram realizadas buscas por títulos, resumos e palavras-chave em anais de conferências publicados, artigos de periódicos, *workshops*, simpósios e trabalhos acadêmicos.

3.2. Revisão da literatura

A contextualização do tema, por meio da revisão da literatura, oferece subsídios para a identificação de lacunas de pesquisa e para o levantamento de fontes de embasamento teórico que sustentam o desenvolvimento do trabalho. Para a condução desta etapa, utilizou-se a *string* de pesquisa apresentada a seguir, seguida do fluxo metodológico descrito na Figura 1.

('threat modeling' OR 'threats modeling') AND 'cybersecurity' AND ('generative AI' OR 'generative artificial intelligence') AND ('quality metrics' OR 'quality') AND ('product development' OR 'software development')

Figura 1 – Fluxo metodológico da revisão da literatura



Fonte: Dados da Pesquisa

3.3. FEECP - *Framework* Estruturado para Engenharia de *Cybersecurity Prompt*

O *framework* permite que modelos de GenAI produzam consistentemente estratégias e passíveis de implantação, alinhadas com cenários reais de cibersegurança. Especificamente, este estudo apresenta as seguintes contribuições:

Avaliação empírica abrangente da GenAI cibernética: avaliar o desempenho de vários modelos de GenAI, incluindo ChatGPT Mini, Gemini e Claude, na geração autônoma de cenários de ameaças de segurança. Essa análise fornece *insights* críticos sobre a eficácia, escalabilidade e aplicabilidade dos modelos para cenários reais de dissuasão cibernética.

Framework Sistemático para Engenharia de *Prompts*: reconhecendo a importância do *design* de *prompts*, o trabalho propõe FEECP, um *framework* estruturado para engenharia de engano adaptativa. O FEECP padroniza o processo de engenharia de *prompts* (PE) entre múltiplos modelos de GenAI, garantindo saídas consistentes e aplicáveis, ao mesmo tempo em que reduz a dependência de ajustes manuais.

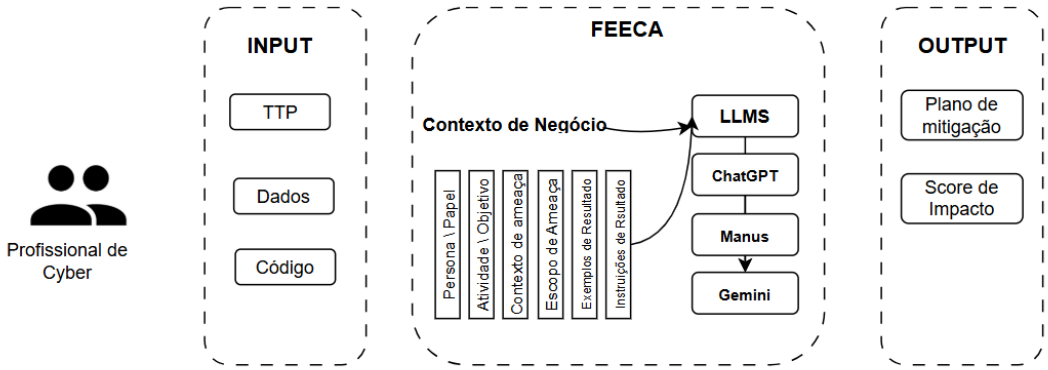
Os parâmetros que estabelecem os critérios para o preenchimento de cada aspecto requerido pelo *framework* estão detalhados na Tabela 1, bem como o fluxo de sequência representado na Figura 2.

Tabela 1 – Parâmetros para estabelecimento de critérios

Componente	Motivação	Especificação	Resultado
Persona / Papel	Garantir o alinhamento com objetivo final específico designando a pape / responsabilidade correta	Espeficificar a função ou papel que Gen AI deve assumir durante a execução	"Atuar como um consultor de cibersegurança para modelagem de ameças utilizando ISO 25010"
Atividade / Objetivo	Evitar ambiguidades através de requisitos claros e definidos	Clareza dos estados que a Gen AI deve executar, alinhados com o resultado esperado	"Modelar ameaças de cibersegurança para API ou módulo do sistema
Contexto da Ameaça	Fornecer para Gen IA o comportamento especifico e contexto dos ambientes de saída	Descrever o ambiente, detalhar o framework, os padrões e contexto da ameaça	"Explorar ameaças de média complexidade"
Delimitar o escopo	Guiar o modelo na criação de situações exequíveis	Incluir restrições operacionais e táticas especificas que a Gen IA deve utilizar ou não	"Modelar entre 3 e 5 ameaças"
Exemplos de Resultado	Melhorar a qualidade do resultado final fornecendo templates	Fornecer exemplos de resultados esperado	" O resultado deve especificar o passo a passo da ameça, impactos e severidade"
Instruções de Resultado	Garantir que a entrega final siga os formatos especificados	Definir formatos e padrões esperados no resultado (Doc, PDF, Image) e os metadados	Gerar um relatório em pdf com as ameças e sugestões de correação

Fonte: Dados da Pesquisa

Figura 2 – Fluxograma da sequência do *framework*



Fonte: Dados da Pesquisa

4. RESULTADOS

O objeto de estudo prático para esse *framework* é o SAELE - *Software* público, gratuito e *open source* disponível na página do Governo Federal Brasileiro.

Para avaliação de cibersegurança do aplicativo, foi baixado o código fonte e posteriormente submetido às ferramentas de GenIA com seguinte *prompt* baseado no FEECP:

"Você é um consultor de segurança da informação, que precisa fazer uma avaliação de segurança em um novo aplicativo. O seu objetivo é identificar ou modelar 5 ameaças relacionadas à cibersegurança à luz dos critérios estabelecidos pela ISO 25010. Você deve buscar Confidencialidade, Integridade, Não repúdio (non-repudiation), Responsabilidade (accountability) e Autenticidade.

No final você deve gerar um relatório detalhado explicando os motivos e os passos para chegar nas ameaças.

Por fim, você deve gerar um relatório complementar com recomendações para sanar os problemas identificados."

Os resultados observados para o *prompt* aplicado diretamente na análise SAELE são analisados de forma comparativa baseado no resultado individual gerado por cada provedor IA Generativa, detalhado na Tabela 2.

Tabela 2 – Análise comparativa dos resultados da SAELE

Critério ISO 25010	Gemini	ChatGPT 4.1 Nano	Claude AI
Confidencialidade	Falhas críticas de autenticação permitem acesso irrestrito e exposição de dados sensíveis (vulnerabilidade alta)	Risco de acesso não autorizado a dados sensíveis, com exemplos práticos, mas genérico (vulnerabilidade moderada)	Exposição de credenciais e dados pessoais, ausência de HTTPS e possível *directory traversal* (vulnerabilidade alta)
Integridade	Manipulação de dados de eleições e configurações sem restrições; *upload* malicioso e *path* traversal (vulnerabilidade alta)	Alteração de dados sem detecção como risco, mas sem análise técnica profunda (vulnerabilidade moderada)	SQL *Injection*, manipulação de notas e conteúdos, validação insuficiente e ausência de controles de integridade (vulnerabilidade alta)
Não Repúdio	Dificuldade de rastrear ações devido à autenticação falha e ausência de homologação (vulnerabilidade alta)	Ausência de mecanismos de prova de transações e não repúdio (vulnerabilidade moderada)	Ausência de assinaturas digitais, *logs* insuficientes e falta de *timestamps* seguros (vulnerabilidade alta)
Responsabilidade (*Accountability*)	Falha na rastreabilidade; recomenda auditoria e logs imutáveis (vulnerabilidade alta)	Falta de registros e auditoria, dificultando responsabilização (vulnerabilidade moderada)	Ausência de trilhas de auditoria abrangentes e logs não protegidos contra alteração (vulnerabilidade alta)
Autenticidade	Autenticação aceita qualquer credencial; risco de *bypass* de *login* via SQL *Injection* (vulnerabilidade alta)	Risco de falsificação de identidade, especialmente por uso de credenciais roubadas (vulnerabilidade moderada)	Autenticação fraca, ausência de MFA e possibilidade de personificação de usuários (vulnerabilidade alta)

Fonte: Resultado da Pesquisa

5. CONSIDERAÇÕES FINAIS

A presente pesquisa evidenciou a relevância e a aplicabilidade da inteligência artificial generativa (GenAI) como instrumento de apoio à avaliação da segurança da informação em

sistemas digitais, à luz da norma ISO/IEC 25010. Por meio do desenvolvimento e aplicação do *framework* FEECP — um modelo estruturado de engenharia de *prompts* voltado à geração de ameaças de cibersegurança — procurou-se apresentar que os modelos de GenAI são capazes de identificar vulnerabilidades críticas de forma autônoma, adaptativa e contextualizada.

O uso de *prompts* estruturados revelou-se uma alternativa para a obtenção de resultados consistentes, elevando a precisão e a utilidade das respostas fornecidas pelos modelos de linguagem. A aplicação prática do *framework* no sistema SAELE, *software* de código aberto utilizado em processos eleitorais universitários, permitiu a identificação de ameaças aos atributos de segurança definidos pela ISO 25010, bem como a proposição de recomendações técnicas para mitigação de riscos.

Os achados desta investigação contribuem para a literatura ao apresentar que a integração entre qualidade de *software*, cibersegurança e inteligência artificial generativa constitui um caminho promissor para o aprimoramento contínuo da segurança em produtos digitais. Sugere-se, para pesquisas futuras, a ampliação do escopo empírico com diferentes tipos de sistemas, bem como o aprofundamento da análise quanto à eficácia de respostas geradas por diferentes modelos de GenAI em variados contextos de aplicação.

REFERÊNCIAS

Blessing Guembe, Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of AI-driven cyber attacks: A review. *Applied Artificial Intelligence, 36*(1), 2037254. https://doi.org/10.1080/08839514.2022.2037254

Fadilah, M. D., Maulidiya, E., & Rochimah, R. (2023). Security evaluating security of insurance agency portal: An ISO/IEC 25023 quality model approach. In *Proceedings of the 3rd International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA 2023)* (pp. xxx–xxx). IEEE. https://doi.org/10.1109/ICICyTA60173.2023.10428701

Hasanov, H., et al. (2024). Application of large language models in cybersecurity: A systematic literature review. *IEEE*.

Nurdayenti, N., & Amiruddin, A. (2022). Comparative analysis of usability, performance, and security of open-source Windows-based password manager applications based on ISO/IEC 25010. In *Proceedings of the 2022 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS 2022)* (pp. 178–182). IEEE. https://doi.org/10.1109/ICIMCIS56303.2022.10017543

Olatunji, O., et al. (2023). A systematic review of the role of artificial intelligence in cybersecurity. *IEEE*, 2024.

Oun, F., Wince, P., & Cheng, T. (2025). The role of artificial intelligence in boosting cybersecurity and trusted embedded systems performance: A systematic review on current and future trends. *IEEE Access*.

SAELE – Sistema Aberto de Eleições Eletrônicas. (2014, 4 de dezembro). *Sobre o software* [Página web]. Portal do Software Público Brasileiro. Recuperado em 11 de agosto de 2025, de https://softwarepublico.gov.br/social/saele

Sekarini, S., Alfinani, M., & Rochimah, R. (2020). Security characteristic evaluation of new students admission information system based on ISO/IEC 25010 quality standard. In

Proceedings of the 12th International Conference on Information Technology and Electrical Engineering (ICITEE 2020).

Qinyuan Ye, Mohamed Ahmed, Reid Pryzant, and Fereshte Khani. 2024. Prompt Engineering a Prompt Engineer. In Findings of the Association for Computational Linguistics: ACL 2024, pages 355–385, Bangkok, Thailand. Association for Computational Linguistics.