INTELIGÊNCIA ARTIFICIAL E QUALIDADE DE SOFTWARE: UMA ANÁLISE DA NORMA ISO/IEC 25010

Daniel Matos de Araujo[1]
Maria Eduarda Samulewski Bonilauri Charão[2]
Matheus de Carlo Gomes[3]

RESUMO

A qualidade no desenvolvimento de software, conforme a ISO/IEC 25010 (ISO, 2023), é essencial para garantir eficiência, segurança e confiabilidade, prevenindo vulnerabilidades que possam comprometer dados do usuário e sistemas. Esses padrões definem nove atributos fundamentais: funcionalidade, performance, compatibilidade, interatividade, confiabilidade, segurança, portabilidade e robustez.
Com a popularização da Inteligência Artificial (IA) Generativa, como o ChatGPT e o GitHub Copilot, programadores passaram a automatizar partes do código, muitas vezes sem revisá-lo de forma adequada.
Um estudo aponta que mais de 1/3 do código gerado por IAs apresenta vulnerabilidades, evidenciando um alto índice de riscos (PEARCE et al., 2021). Isso acontece porque grande parte do treinamento dessas IAs foi feita com código público que nem sempre segue as normas e boas práticas da ISO/IEC 25010.
Assim, buscamos orientar que é mais correto uso da IA com base na ISO/IEC 25010 alinhando automatização a critérios robustos de qualidade, segurança e manutenibilidade. Respeitando a norma e prevenindo o acúmulo de erros técnicos e por consequência causando menos falhas de segurança.

Palavras-chave: ISO/IEC 25010 Modelo de Qualidade de Software. Inteligência Artificial. Código Limpo. Controle de Qualidade.

INTRODUÇÃO

Desenvolver software com qualidade é fundamental para garantir não apenas a eficiência e a confiabilidade das aplicações, mas também para mitigar vulnerabilidades, protegendo dados sensíveis e assegurando a integridade e a segurança dos sistemas frente a ameaças cada vez mais sofisticadas. A norma ISO/IEC 25010 define modelos de qualidade tanto para o uso quanto para os produtos de software.

Entre os atributos relacionados à qualidade em uso, destaca-se a proteção contra riscos, que representa a capacidade do software de minimizar ou evitar danos aos usuários, ao ambiente, às informações e, consequentemente, ao próprio projeto. Esse atributo contribui diretamente para a segurança e confiabilidade das soluções desenvolvidas (CALAZANS et al., 2018).

1 Acadêmico do 2º período de Análise e Desenvolvimento de Sistemas na universidade Tuiuti do Paraná. E-mail: daniel.matosdkx@gmail.com
2 Acadêmico do 2º período de Análise e Desenvolvimento de Sistemas na universidade Tuiuti do Paraná. E-mail: mariaeduardacharao@gmail.com
3 Acadêmico do 2º período de Análise e Desenvolvimento de Sistemas na universidade Tuiuti do Paraná. E-mail: matheus.carlo2015@gmail.com

Com o objetivo de manter um padrão de qualidade entre softwares em geral, o Modelo de Qualidade de Software, criado em 2011 e atualizado em 2023 (ISO, 2023), baseia-se em nove fundamentos: Adequação Funcional, Eficiência de Performance, Compatibilidade, Capacidade

de Interação, Confiabilidade, Segurança, Manutenibilidade, Portabilidade e Robustez. Dessa forma, este trabalho tem como objetivo apontar o crescente número de violações à norma decorrentes do uso indevido de inteligências artificiais generativas, além de orientar quanto ao uso adequado dessas ferramentas em conformidade com a norma. Segundo a OX Security, desenvolver com o auxílio de IA pode tornar o código vulnerável a invasões e infringir regras de segurança (ZIV, 2023).

A ERA DA INTELIGÊNCIA ARTIFICIAL

De acordo com a revista Forbes (2023), o ChatGPT, lançado em 2022, foi a primeira inteligência artificial generativa considerada comercialmente viável. Esse chatbot interativo revolucionou a forma como interagimos com a tecnologia, sendo capaz de gerar textos, sistemas, planos, aulas e, posteriormente, até imagens e vídeos. No entanto, como ocorre com todo avanço tecnológico, surgiram novas discussões e desafios, especialmente relacionados à forma como essas IAs são treinadas, e à confiabilidade das soluções que produzem.

Com a capacidade de gerar sistemas computacionais complexos instantaneamente, cresce a preocupação com a qualidade e a segurança do software gerado. Além disso, muitos programadores passaram a depender excessivamente dessas ferramentas, apenas copiando e colando o código sugerido pela IA, o que compromete a segurança e qualidade dos sistemas em relação à ISO/IEC 25010 (CHEN et al., 2021; ISO, 2023).

Um estudo conduzido pela Universidade de Stanford (BONEH et al., 2023) apontou que desenvolvedores que utilizam assistentes de código baseados em IA têm maior probabilidade de introduzir vulnerabilidades de segurança em comparação com aqueles que escrevem o código manualmente.

A CRISE E AS CONSEQUÊNCIAS

Durante a crise de 2008, o mercado financeiro mundial entra em colapso, afetando o setor tecnológico de forma direta e indireta. A falta de investimento e prioridade no setor fez com que empresas tomassem medidas drásticas: lay-offs e grandes cortes de gastos se tornaram comuns. Empresas de tecnologia passaram a priorizar produtos e serviços que gerassem retorno rápido, muitas vezes negligenciando normas e práticas de código limpo (BREM et al., 2020).

Quando o mundo começou a se acalmar e o desespero da crise diminuiu, a internet ganhou força com a popularização dos smartphones, que oferecem acesso remoto a ela. Isso

fez com que as empresas precisassem migrar precipitadamente para o ambiente digital. Mais uma vez, a pressa prevaleceu sobre a técnica, mesmo após a criação da norma ISO/IEC 25010, um modelo de qualidade de software, em 2011 (ISO, 2023). Nessa norma, o foco principal foi dado à eficiência e à performance, enquanto outros aspectos importantes, como confiabilidade, segurança e manutenibilidade, foram quase deixados de lado (BREM et al., 2020).

Com o surgimento da Covid-19, o mundo passou por uma rápida digitalização. Com a população confinada em casa devido ao lockdown, o número de usuários da internet cresceu drasticamente, tornando as mudanças digitais não apenas necessárias, mas inevitáveis. Ao contrário da crise de 2008, quando houve uma baixa nos investimentos, a necessidade de digitalizar todos os serviços durante a pandemia gerou um volume de investimentos muito acima do esperado. Contudo, diferentemente daquele período, em que a escassez de engenharia era um problema, desta vez o desafio foi o excesso. Sistemas que deveriam ser simples passaram a apresentar arquiteturas excessivamente complexas e funções desnecessárias. Isso não só violava a norma de Adequação Funcional, como também dificultava o uso desses sistemas por pessoas com pouca familiaridade com a internet, negligenciando a norma de Usabilidade (ALASHHAB et al., 2021; ISO, 2023).

A JUNÇÃO DA ISO/IEC 25010 E A IA

Ao longo dos últimos anos, bilhões de linhas de código foram escritas com regras e convenções frequentemente ignoradas, e grande parte desse material serviu como base de treinamento para inteligências artificiais.

A questão que se impõe, no entanto, é: esses códigos estavam em conformidade com a norma ISO/IEC 25010? Estudos apontam que, em diversos casos, as IAs não apenas reproduzem, como também amplificam problemas estruturais, gerando vulnerabilidades que violam diretamente as normas de Segurança. Além disso, foi observado o aumento da produção de código duplicado, o que infringe normas relacionadas à Eficiência de Performance e à Manutenibilidade (PEARCE et al., 2021).

O uso das IAs de forma não supervisionada e revisada assume riscos desnecessários, além de desenvolver código possivelmente nocivo. De acordo com um estudo da Universidade de Nova York, cerca de 37% do código gerado por IAs é, de alguma forma, vulnerável (PEARCE et al., 2021).

A ISO/IEC 25010 busca melhorar o desenvolvimento de sistemas e prevenir códigos escritos de forma errada ou "suja" (ISO, 2023). Como já apresentado anteriormente, em alguns casos, a IA não leva pilares da norma em consideração. Por isso, o auxílio da ISO/IEC 25010 no desenvolvimento e revisão de código gerado com ajuda de inteligência artificial é de extrema importância para manter a qualidade do software segundo a norma (BONEH et al., 2023).

CONSIDERAÇÕES FINAIS

Princípios éticos fundamentais, como a honestidade e a integridade, desempenham um papel central no desenvolvimento de software, exigindo que o profissional da área adote critérios técnicos rigorosos ao utilizar códigos reutilizáveis ou gerados por inteligência artificial, com o objetivo de garantir a qualidade e a segurança do produto. Sob essa perspectiva, torna-se insustentável a argumentação de que o conhecimento em programação não é necessário para avaliar a qualidade do software entregue.

O Modelo de Qualidade de Software deve ser considerado um pilar fundamental no desenvolvimento de sistemas. Atualmente, o uso de inteligência artificial já é amplamente adotado pelo mercado; no entanto, conforme discutido anteriormente, sua aplicação nem sempre resulta na qualidade exigida pela norma ISO/IEC 25010 (ISO, 2023; PEARCE et al., 2021). Diante disso, torna-se essencial a integração entre as diretrizes da norma e o uso de IA, a fim de assegurar a qualidade do produto de software e garantir conformidade com os critérios estabelecidos pelo Modelo de Qualidade de Software da ISO/IEC 25010.

REFERÊNCIAS

CALAZANS, A. et al. Requisitos de Qualidade de Usabilidade: análise da utilização em sistemas de uma instituição financeira. Anais do WER18 - Workshop em Engenharia de Requisitos. Anais...PUC-Rio, 2018. Disponível em: https:// wer.inf.puc- rio.br/WERpapers/artigos/artigos_WER18/WER_2018_paper_43.pdf. Acesso em: 23 jun. 2025.

No title. Disponível em: https://www.iso.org/obp/ui/en/. Acesso em: 5 jun. 2025.

ZIV, Neatsun. As AI-generated code becomes the new normal, the risks it introduces are often hidden beneath seemingly innocuous code, flaws that traditional security tools are not built to detect. PR Newswire, 7 maio 2025. Disponível em: https://www.prnewswire.com/news-releases/as-ai-accelerates-code-generation-ox- security-raises-60m-to-focus-developers-on-the-5-of-risks-that-truly-matter- 302448458.html. Acesso em: 3 jun. 2025.

Boneh, D. et al. Do User Write More Insecure Code with AI Assistants?, 18 de dezembro de 2023. Stanford. Disponivel em: https://arxiv.org/pdf/2211.03622. Acesso em: 3 jun. 2025

FORBES BRASIL. ChatGPT: como a inteligência artificial se tornou uma febre no mundo dos negócios. Publicado em 24 jan. 2023. Disponível em: https://forbes.com.br/forbes-tech/2023/01/chatgpt-como-a-inteligencia-artificial-se- tornou-uma-febre-no-mundo-dos-negocios. Acesso em: 9 jun. 2025.

PEARCE, H. et al. Asleep at the keyboard? Assessing the security of GitHub

Copilot's code contributions. 2021. Disponível em: http://arxiv.org/abs/2108.09293.

Acesso em: 3 jun. 2025.

CHEN, M. et al. Evaluating large language models trained on code. 2021. Disponível em: https://arxiv.org/ pdf/2107.03374. Acesso em 3 jun. 2025.

BREM, A. et al. The impact of the 2008 financial crisis on innovation: A dominant design perspective. Journal of business research. 2020. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S014829632030059X. Acesso em 25 maio. 2025.

ALASHHAB, Z. R. et al. Impact of coronavirus pandemic crisis on technologies and cloud computing applications. 2021. Disponível em: https://www.sciencedirect.com/science/article/pii/S1674862X20300665. Acesso em 25 maio. 2025.