# Estudo preliminar da integração de Inteligências Artificiais Generativas para geração de relatórios de conformidade em segurança cibernética

**Letícia S. M. Pereira**[1], **Ramicés dos S. Silva**[1], **Anita Maria da R. Fernandes** [1], **Rudimar L. S. Dazzi**[1]

[1]Universidade do Vale do Itajaí (UNIVALI)
Caixa Postal 360 – 88302-901 – Itajaí – SC – Brasil

leticiamangrich@edu.univali.br, ramices@binsoft.br

{anita.fernandes, rudimar}@univali.br

***Abstract.*** *This paper presents a preliminary study on the application of Generative Artificial Intelligence (AI) to automate cybersecurity compliance reports. It proposes integrating AI with the Wazuh platform and the National Vulnerability Database (NVD) through a three-layer architectural model capable of transforming technical data into customized reports. The approach aims to reduce costs, accelerate processes, and strengthen organizational capacity to meet standards and mitigate risks.*

***Resumo.*** *Este trabalho apresenta um estudo preliminar sobre a aplicação de Inteligência Artificial (IA) Generativa para automatizar relatórios de conformidade em segurança cibernética. Propõe-se a integração de IA ao Wazuh e à base National Vulnerability Database (NVD) por meio de um modelo arquitetônico em três camadas capaz de transformar dados técnicos em relatórios personalizados. A abordagem visa reduzir custos, acelerar processos e fortalecer a capacidade organizacional de atender a normas e mitigar riscos.*

## 1. Introdução

Com o avanço da digitalização, a segurança cibernética tem se tornado um tema central em diferentes áreas de estudo, à medida que cresce a necessidade de proteger informações e sistemas frente ao aumento do volume de dados. Nesse cenário de digitalização rápida, organizações de todos os tamanhos estão cada vez mais expostas a ameaças cibernéticas que podem colocar em risco informações confidenciais e interromper suas atividades [Mohammed 2023], necessitando de estratégias que amparem corretamente suas necessidades.

Dessa forma, relatórios de conformidade em segurança cibernética desempenham um papel crucial na identificação de falhas, análise dos mecanismos de proteção e na garantia de conformidade com normas do setor. Entretanto, os métodos convencionais da geração desses relatórios são, geralmente, lentos e trabalhosos [Mohammed 2023], o que torna a gestão de riscos menos eficaz e evidencia a necessidade de soluções mais rápidas e automatizadas.

O presente artigo traz um estudo preliminar da geração de relatórios de conformidade em segurança cibernética como uma prática alternativa para o atual processo manual.

## 2. IA Generativa em relatórios de conformidade

A IA Generativa é uma tecnologia que utiliza algoritmos de IA para criar automaticamente conteúdo a partir de comandos do usuário. Ela é treinada com grandes volumes de dados de fontes, analisando estatisticamente distribuições de elementos para identificar e replicar padrões recorrentes [UNESCO 2024].

No cenário digital interconectado atual, as organizações enfrentam um ambiente regulatório em constante evolução, ao mesmo tempo que lidam com ameaças cibernéticas cada vez mais sofisticadas. A dinâmica das regulamentações em diversos setores tornou-se mais frequente e complexa, respondendo a riscos emergentes, disrupções tecnológicas e à crescente ênfase na privacidade de dados e governança ética [Oluoha et al. 2022].

Diante das complexidades atuais, a IA Generativa revela grande potencial de aplicação em diferentes setores, especialmente na automatização de relatórios de conformidade. Ao transformar dados complexos em documentos claros e personalizados, ela agiliza processos, reduz esforços manuais e reforça a capacidade das organizações de responder a regulamentações em constante evolução e a riscos emergentes.

## 3. Modelo proposto de integração de IA

Para lidar de maneira eficiente com os desafios simultâneos da conformidade e riscos cibernéticos, torna-se necessário um framework de integração de IA estruturado e inteligente em camadas [Oluoha et al. 2022]. Portanto, a integração das tecnologias de IA Generativa com as soluções de monitoramento de segurança, como o Wazuh, para a criação de relatórios de conformidade específicos para cada setor da empresa, oferece uma abordagem eficaz e escalável para esse fim.

Esta integração segue um modelo arquitetônico baseado em três camadas, que conectam as capacidades analíticas do Wazuh, os dados de referência do NVD e a síntese textual fornecida pelas IAs Generativas.

### 3.1. Fundamentação Técnica

A arquitetura proposta fundamenta-se em tecnologias consolidadas para monitoramento e análise de segurança cibernética. O Wazuh, como plataforma SIEM (Security Information and Event Management) oferece capacidades integradas para detecção de vulnerabilidades, avaliação de configuração de segurança, monitoramento de integridade de arquivos e resposta a incidentes [WAZUH 2025a]. Esta plataforma agrega, indexa e analisa dados de segurança em tempo real, facilitando a detecção de intrusões, ameaças e anomalias comportamentais [WAZUH 2025b].

A integração com o NVD do NIST proporciona acesso a dados padronizados de vulnerabilidades, representados pelo Security Content Automation Protocol (SCAP) [NIST 2024b]. O NVD serve como repositório governamental de dados de gerenciamento de vulnerabilidades baseados em padrões, permitindo a automação do gerenciamento de vulnerabilidades, medição de segurança e conformidade [NIST 2024a].

Arquiteturas em camadas para sistemas de segurança têm demonstrado eficácia na organização de processos complexos, proporcionando modularidade e escalabilidade [Zhang et al. 2022]. A abordagem de três camadas permite a separação clara de responsabilidades: coleta de dados, análise e correlação, e síntese de informações para consumo humano [Becker et al. 2016].

### 3.2. Fluxo Conceitual

**Camada de Coleta:**

Nesta camada, agentes Wazuh monitoram continuamente os ativos corporativos, coletando eventos de segurança [WAZUH 2025a]. Esses eventos são normalizados pelo servidor Wazuh com o uso de regras pré-definidas, garantindo uniformidade no processamento. Para enriquecer as informações, os metadados de vulnerabilidades são obtidos por meio de consultas à API do NVD [NIST 2024a], proporcionando contexto adicional às ameaças identificadas.

**Camada de análise:** Na camada de análise, os dados estruturados são indexados no Wazuh Indexer [WAZUH 2025b], permitindo uma busca eficiente e escalável. As consultas realizadas correlacionam os eventos de segurança com diversas fontes de referência, como bases de conhecimento (CVE, CWE), requisitos de conformidade (frameworks aplicáveis) e o contexto organizacional, incluindo setores específicos e a criticidade dos ativos monitorados [Elgammal et al. 2011].

**Camada de síntese:** A IA generativa recebe os dados técnicos processados (estruturados em JSON) e templates adaptáveis, projetados para diferentes públicos-alvo (técnicos, gerenciais ou regulatórios) [Dimyadi and Amor 2017]. Além disso, são fornecidas diretrizes de formatação para garantir conformidade com normas institucionais. Utilizando modelos de linguagem, a IA aplica técnicas de sumarização para gerar descobertas, mapeamento de controles e vulnerabilidades, e recomendações contextualizadas, de forma automatizada e escalável [Zhang and El-Gohary 2013].

## 4. Validação Proposta

A eficácia desta integração deve ser avaliada por meio de diversas métricas de desempenho, incluindo:

- Comparação dos relatórios gerados automaticamente com os relatórios manuais existentes, analisando consistência e precisão;
- Análise da qualidade das recomendações geradas pela IA, verificando a aderência a boas práticas de segurança;
- Medição do tempo de produção de cada relatório, visando melhorar a eficiência do processo;
- Verificação da aderência dos relatórios aos templates institucionais, garantindo a conformidade com os requisitos organizacionais.

Essa abordagem permite que a arquitetura existente do Wazuh e do NVD seja mantida, enquanto a IA Generativa é integrada como uma ferramenta para orquestrar a produção de relatórios consumíveis por seres humanos, sem alterar os processos subjacentes de detecção ou coleta de vulnerabilidades.

## 5. Conclusão

A segurança cibernética tornou-se um pilar fundamental da infraestrutura digital contemporânea, demandando soluções inovadoras para uma interpretação ágil de ameaças e conformidade regulatória. Neste contexto, a automação inteligente de processos surge como alternativa estratégica para superar os desafios de escalabilidade e precisão na gestão de riscos.

A fim de viabilizar a geração de relatórios de conformidade em segurança cibernética, este trabalho apresentou um estudo preliminar sobre a integração de IA Generativa com Wazuh e NVD. A abordagem proposta demonstra potencial para automatizar a criação de relatórios técnicos e gerenciais, reduzindo custos e aumentando a eficiência nos processos de conformidade.

## Referências


Becker, J., Delfmann, P., Dietrich, H.-A., Steinhorst, M., and Eggert, M. (2016). Business process compliance checking – applying and evaluating a generic pattern matching approach for conceptual models in the financial sector. *Information Systems Frontiers*, 18(2):359–405.

Dimyadi, J. and Amor, R. (2017). Automating conventional compliance audit processes. In *Product Lifecycle Management and the Industry of the Future*, pages 324–334. Springer.

Elgammal, A., Türetken, O., van den Heuvel, W.-J., and Papazoglou, M. (2011). On the formal specification of regulatory compliance: A comparative analysis. In Benatallah, B., Casati, F., Kappel, G., and Rossi, G., editors, *Service-Oriented Computing – ICSOC 2010*, pages 27–38, Berlin, Heidelberg. Springer.

Mohammed, A. (2023). Elevating cybersecurity audits: How ai is shaping compliance and threat detection. *Aitoz Multidisciplinary Review (AMR)*, 2:1–9.

NIST (2024a). Introduction to development with nvd data. Disponível em: https://nvd.nist.gov/developers.

NIST (2024b). National vulnerability database. Disponível em: https://nvd.nist.gov/.

Oluoha, O. M., Odeshina, A., Reis, O., Okpeke, F., Attipoe, V., and Orieno, O. H. (2022). Artificial intelligence integration in regulatory compliance: A strategic model for cybersecurity enhancement. *Journal of Frontiers in Multidisciplinary Research*, 3(1):35–46.

UNESCO (2024). *Guia para a IA generativa na educação e na pesquisa*. UNESCO, Paris. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000390241.

WAZUH (2025a). Wazuh for cmmc compliance. Disponível em: https://wazuh.com/blog/wazuh-for-cmmc-compliance/.

WAZUH (2025b). Wazuh overview. Disponível em: https://wazuh.com/platform/.

Zhang, J. and El-Gohary, N. M. (2013). Semantic nlp-based information extraction from construction regulatory documents for automated compliance checking. *Journal of Computing in Civil Engineering*, 30(2).

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., and Choo, K.-K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 55:1029–1053.