LUMEN ET VIRTUS
ISSN: 2177-2789

SEGURANÇA OFENSIVA COMO INSTRUMENTO DE PREVENÇÃO DE INCIDENTES EM PEQUENAS E MÉDIAS EMPRESAS

OFFENSIVE SECURITY AS AN INSTRUMENT FOR INCIDENT PREVENTION IN SMALL AND MEDIUM-SIZED ENTERPRISES

SEGURIDAD OFENSIVA COMO INSTRUMENTO DE PREVENCIÓN DE INCIDENTES EN PEQUEÑAS Y MEDIANAS EMPRESAS

https://doi.org/10.56238/levv17n61-080

Data de submissão: 19/05/2026 **Data de publicação:** 19/06/2026

Fábio Henrique de Almeida

RESUMO

A crescente dependência de tecnologias digitais ampliou a exposição das pequenas e médias empresas a ameaças cibernéticas, tornando necessária a adoção de mecanismos capazes de identificar vulnerabilidades antes de sua exploração, diante dessa realidade, o estudo teve como objetivo analisar a contribuição da segurança ofensiva para a prevenção de incidentes cibernéticos em pequenas e médias empresas, considerando sua aplicabilidade, os procedimentos de identificação de vulnerabilidades e sua integração ao gerenciamento de riscos, a investigação foi desenvolvida mediante pesquisa bibliográfica de abordagem qualitativa, com caráter exploratório e descritivo, fundamentada na análise crítica de publicações científicas e documentos técnicos relacionados à segurança cibernética, os resultados evidenciaram que testes de intrusão, avaliações automatizadas e verificações técnicas independentes contribuem para identificar fragilidades, validar condições de exploração e orientar a priorização de medidas corretivas, identificou-se também que a efetividade dessas práticas depende da disponibilidade de recursos, da interpretação adequada das evidências e do acompanhamento das intervenções realizadas, concluindo-se que a segurança ofensiva constitui um instrumento relevante para o fortalecimento da proteção empresarial, desde que integrada a processos contínuos de gerenciamento de riscos, sem que a identificação de vulnerabilidades represente, isoladamente, a comprovação da redução de incidentes.

Palavras-chave: Segurança Ofensiva. Segurança Cibernética. Testes de Intrusão. Prevenção de Incidentes. Pequenas e Médias Empresas.

ABSTRACT

The increasing reliance on digital technologies has expanded the exposure of small and medium-sized enterprises to cyber threats, creating a need for mechanisms capable of identifying vulnerabilities before they are exploited, against this background, the study aimed to analyze the contribution of offensive security to cybersecurity incident prevention in small and medium-sized enterprises, considering its applicability, vulnerability identification procedures, and integration into risk management, the investigation was conducted through qualitative bibliographic research with an exploratory and descriptive approach, based on a critical analysis of scientific publications and technical documents addressing cybersecurity, the findings indicated that penetration testing, automated assessments, and independent technical evaluations contribute to identifying weaknesses,

validating exploitation conditions, and guiding the prioritization of corrective measures, the analysis also revealed that the effectiveness of these practices depends on resource availability, appropriate interpretation of technical evidence, and continuous monitoring of implemented interventions, leading to the conclusion that offensive security represents a relevant instrument for strengthening organizational protection when integrated into ongoing risk management processes, although vulnerability identification alone does not provide sufficient evidence of a measurable reduction in cybersecurity incidents.

Keywords: Offensive Security. Cybersecurity. Penetration Testing. Incident Prevention. Small and Medium-sized Enterprises.

RESUMEN

La creciente dependencia de tecnologías digitales ha ampliado la exposición de las pequeñas y medianas empresas a amenazas cibernéticas, haciendo necesaria la adopción de mecanismos capaces de identificar vulnerabilidades antes de su explotación; ante esta realidad, el estudio tuvo como objetivo analizar la contribución de la seguridad ofensiva para la prevención de incidentes cibernéticos en pequeñas y medianas empresas, considerando su aplicabilidad, los procedimientos de identificación de vulnerabilidades y su integración a la gestión de riesgos. La investigación se desarrolló mediante investigación bibliográfica de enfoque cualitativo, con carácter exploratorio y descriptivo, fundamentada en el análisis crítico de publicaciones científicas y documentos técnicos relacionados con la seguridad cibernética. Los resultados evidenciaron que las pruebas de intrusión, evaluaciones automatizadas y verificaciones técnicas independientes contribuyen a identificar fragilidades, validar condiciones de explotación y orientar la priorización de medidas correctivas. Se identificó también que la efectividad de estas prácticas depende de la disponibilidad de recursos, de la interpretación adecuada de la evidencia y del seguimiento de las intervenciones realizadas. Se concluye que la seguridad ofensiva constituye un instrumento relevante para el fortalecimiento de la protección empresarial, siempre que esté integrada a procesos continuos de gestión de riesgos, sin que la identificación de vulnerabilidades represente, aisladamente, la comprobación de la reducción de incidentes.

Palabras clave: Seguridad Ofensiva. Seguridad Cibernética. Pruebas de Intrusión. Prevención de Incidentes. Pequeñas y Medianas Empresas.

1 INTRODUÇÃO

Com a incorporação de plataformas digitais, serviços em nuvem e sistemas integrados às atividades empresariais, pequenas e médias empresas passaram a depender de infraestruturas tecnológicas para administrar informações, realizar transações e manter a comunicação com clientes e fornecedores. Essa transformação também ampliou a superfície de exposição a ameaças cibernéticas, permitindo que vulnerabilidades em aplicações, redes e mecanismos de autenticação sejam exploradas para comprometer dados e interromper processos diretamente relacionados à continuidade das operações (Awan; Alam, 2025).

Embora a digitalização tenha proporcionado novas oportunidades de crescimento e eficiência operacional, a capacidade de acompanhar as exigências de proteção dos ambientes tecnológicos permanece desigual entre organizações de diferentes portes, especialmente porque limitações financeiras, conhecimento técnico insuficiente e dificuldades na contratação de profissionais especializados influenciam a adoção de medidas preventivas, criando circunstâncias para que fragilidades de segurança permaneçam desconhecidas ou sejam tratadas somente após a ocorrência de comprometimentos (Ali, *et al.*, 2025).

Quando essas fragilidades são exploradas, as consequências podem atingir diferentes dimensões da atividade empresarial, incluindo indisponibilidade de sistemas, comprometimento de informações confidenciais, despesas com recuperação e deterioração das relações comerciais, circunstâncias particularmente prejudiciais para organizações que operam com recursos limitados e dependem da estabilidade de suas operações para preservar receitas, cumprir obrigações contratuais e manter a confiança dos clientes (El-Hajj; Mirza, 2024).

Prevenir ocorrências dessa natureza requer procedimentos capazes de reconhecer antecipadamente as situações que favorecem a exploração de vulnerabilidades, entretanto, a literatura demonstra que pequenas e médias empresas frequentemente apresentam dificuldades para estabelecer prioridades de proteção, distribuir responsabilidades e integrar recursos humanos e tecnológicos às atividades de segurança, o que compromete a construção de mecanismos preventivos compatíveis com as características e necessidades de suas estruturas operacionais (Michalek; O'Shaughnessy; Wahlstrom, 2026).

Mesmo nas organizações que afirmam possuir controles de proteção implementados, a existência de políticas internas e serviços de suporte tecnológico não assegura que as vulnerabilidades estejam devidamente identificadas ou corrigidas, conforme demonstrado por avaliações especializadas que encontraram discrepâncias entre a maturidade de segurança declarada pelas empresas e os contextos efetivamente verificadas em suas infraestruturas, sobretudo em aspectos relacionados ao gerenciamento de ativos, atualização de sistemas, controle de acessos e monitoramento de atividades suspeitas (Chidukwani; Zander; Koutsakis, 2026).

Diante da necessidade de superar avaliações baseadas exclusivamente em percepções internas, a segurança ofensiva apresenta uma abordagem voltada à investigação técnica dos cenários de exposição dos ambientes digitais, mediante a utilização autorizada de procedimentos que reproduzem comportamentos de possíveis invasores para identificar vulnerabilidades, examinar possibilidades de exploração e produzir evidências sobre fragilidades existentes, permitindo que decisões de proteção sejam fundamentadas em verificações práticas da infraestrutura empresarial (Sarker; Yunus; Deraman, 2023).

Na prática, a aplicação dessa abordagem compreende procedimentos como testes de intrusão, verificações automatizadas e simulações controladas de ataques, capazes de identificar situações relacionadas ao comprometimento de credenciais, à elevação indevida de privilégios e à exploração de configurações inadequadas, enquanto a classificação das falhas encontradas e a realização de novas verificações após as correções possibilitam estruturar um processo de avaliação contínua, direcionado à redução das oportunidades de exploração identificadas nos sistemas corporativos (Lee, 2025).

Para transformar os resultados dessas avaliações em medidas preventivas consistentes, torna-se necessário relacionar as vulnerabilidades identificadas aos ativos organizacionais, aos possíveis impactos sobre as atividades e às prioridades estabelecidas pela administração, integração compatível com a estrutura de gerenciamento de riscos proposta pelo NIST Cybersecurity Framework, que organiza a segurança cibernética em funções interdependentes de governança, identificação, proteção, detecção, resposta e recuperação, favorecendo o acompanhamento sistemático dos fatores de segurança (National Institute of Standards and Technology, 2024).

Entre as situações que justificam verificações técnicas periódicas encontram-se configurações inseguras, mecanismos de autenticação frágeis, sistemas desatualizados e permissões de acesso incompatíveis com as necessidades dos usuários, parâmetros que podem favorecer ataques direcionados à infraestrutura empresarial e comprometer a disponibilidade de informações e serviços, sendo a identificação dessas fragilidades um subsídio para orientar medidas como atualização de componentes, autenticação multifator, segmentação de redes e gerenciamento de privilégios (Awan; Alam, 2025).

Sob a perspectiva das pequenas e médias empresas, entretanto, a adoção de procedimentos especializados precisa considerar a disponibilidade de recursos e a complexidade dos ambientes avaliados, pois a utilização de metodologias incompatíveis com a estrutura organizacional pode dificultar a continuidade das atividades de segurança, tornando relevante estabelecer critérios de priorização que relacionem probabilidade de exploração, impacto operacional e viabilidade das intervenções, de maneira a direcionar investimentos para vulnerabilidades cuja correção represente maior benefício à proteção empresarial (El-Hajj; Mirza, 2024).

É justamente a necessidade de verificar a proteção efetivamente existente, em vez de depender exclusivamente de controles declarados ou avaliações superficiais, que justifica o desenvolvimento desta investigação, considerando que evidências obtidas por procedimentos técnicos independentes podem revelar vulnerabilidades desconhecidas, orientar decisões corretivas e contribuir para uma compreensão mais precisa da exposição organizacional, especialmente em empresas cujas limitações estruturais dificultam o acompanhamento permanente dos requisitos de segurança de seus ambientes digitais (Chidukwani; Zander; Koutsakis, 2026).

Com base nessa problemática, este estudo tem como objetivo analisar a contribuição da segurança ofensiva para a prevenção de incidentes cibernéticos em pequenas e médias empresas, examinando a identificação antecipada de vulnerabilidades, a validação técnica de possibilidades de exploração, a priorização de medidas corretivas e a integração dessas práticas ao gerenciamento de riscos, de modo a compreender as condições em que avaliações ofensivas autorizadas podem contribuir para o fortalecimento da proteção empresarial e para a redução da exposição a ameaças cibernéticas (Lee, 2025).

2 REFERENCIAL TEÓRICO

2.1 SEGURANÇA CIBERNÉTICA E EXPOSIÇÃO A INCIDENTES EM PEQUENAS E MÉDIAS EMPRESAS

Nas pequenas e médias empresas, a crescente utilização de tecnologias digitais modificou a organização dos processos administrativos, comerciais e operacionais, permitindo que informações e serviços fossem compartilhados por meio de plataformas conectadas e aplicações integradas, essa transformação ampliou a dependência de recursos computacionais e introduziu novas possibilidades de comprometimento, especialmente quando a expansão das infraestruturas ocorre sem a implementação proporcional de mecanismos de proteção, monitoramento e gerenciamento das vulnerabilidades associadas aos ambientes empresariais (Awan; Alam, 2025).

Embora os riscos cibernéticos estejam presentes em organizações de diferentes dimensões, suas consequências e possibilidades de enfrentamento variam conforme a disponibilidade de recursos financeiros, profissionais especializados e conhecimentos técnicos, nas empresas de menor porte, a insuficiência de investimentos e a compreensão limitada sobre ameaças digitais podem resultar na manutenção de práticas inadequadas de segurança, dificultando a identificação de fragilidades e a adoção de procedimentos preventivos capazes de acompanhar as mudanças constantes nos ambientes tecnológicos (Ali, *et al.*, 2025).

Essa diferença nas condições de proteção evidencia que o porte empresarial não constitui um indicador confiável da probabilidade de exposição a ataques, considerando que pequenas organizações também armazenam informações confidenciais, realizam transações financeiras e mantêm conexões

com sistemas pertencentes a outras instituições, a combinação entre dependência tecnológica e capacidade limitada de recuperação pode intensificar os efeitos de incidentes, sobretudo quando inexistem procedimentos definidos para assegurar a continuidade dos serviços e restabelecer as operações comprometidas (Michalek; O'Shaughnessy; Wahlstrom, 2026).

Entre as ameaças identificadas na literatura encontram-se ataques de phishing, engenharia social, infecções por programas maliciosos, ransomware, exploração de credenciais e tentativas de indisponibilização de serviços, cuja ocorrência está associada a diferentes vulnerabilidades técnicas e comportamentais, a diversidade desses mecanismos demonstra que a exposição empresarial não se restringe às falhas presentes em sistemas computacionais, abrangendo também procedimentos internos, práticas de autenticação e decisões humanas capazes de favorecer acessos indevidos ou comprometer informações corporativas (Awan; Alam, 2025).

Em ambientes nos quais o gerenciamento de atualizações e credenciais ocorre de maneira irregular, vulnerabilidades conhecidas podem permanecer disponíveis para exploração mesmo quando existem soluções destinadas à proteção da infraestrutura, verificações técnicas realizadas em pequenas e médias empresas identificaram problemas relacionados à reutilização de senhas e à ausência de correções de segurança, indicando que práticas operacionais inadequadas podem permitir o comprometimento de contas, a ampliação indevida de privilégios e a exposição de recursos internos a diferentes modalidades de ataque (Lee, 2025).

Contudo, a permanência dessas fragilidades está relacionada à maneira como os responsáveis pelas empresas compreendem e administram os riscos associados às tecnologias utilizadas, pois a percepção reduzida sobre a gravidade das ameaças pode comprometer decisões de investimento, capacitação e estabelecimento de controles, enquanto a insuficiência de conhecimentos especializados dificulta a avaliação das soluções disponíveis e favorece a adoção de medidas fragmentadas, incapazes de proporcionar uma compreensão abrangente das requisitos reais de proteção (Ali, *et al.*, 2025).

Mesmo quando existem investimentos em infraestrutura tecnológica e contratação de suporte especializado, a segurança efetivamente alcançada pode apresentar diferenças significativas em relação à percepção dos gestores, conforme observado em avaliações independentes que identificaram inconsistências entre as práticas declaradas pelas empresas e as evidências obtidas mediante inspeções, entrevistas e verificações técnicas, revelando deficiências no gerenciamento de ativos, na atualização de sistemas, na configuração de redes e na implementação de controles de acesso (Chidukwani; Zander; Koutsakis, 2026).

Para compreender a extensão dessas deficiências, torna-se necessário reconhecer que a proteção empresarial depende do conhecimento sobre os recursos tecnológicos utilizados e das relações estabelecidas entre sistemas, usuários e informações, o gerenciamento dos riscos cibernéticos pressupõe a identificação dos ativos organizacionais, a avaliação das condições de exposição e o

estabelecimento de procedimentos destinados à proteção, detecção, resposta e recuperação, permitindo que as decisões de segurança sejam articuladas às necessidades operacionais e aos objetivos institucionais (National Institute of Standards and Technology, 2024).

Quando essas condições não são adequadamente administradas, os efeitos de um incidente podem ultrapassar os limites dos sistemas diretamente comprometidos e alcançar atividades financeiras, administrativas e comerciais, uma vez que a indisponibilidade de serviços, a perda de informações e os custos associados à recuperação da infraestrutura podem prejudicar a capacidade de funcionamento das empresas, especialmente quando sua estrutura econômica apresenta menor margem para absorver interrupções prolongadas e despesas imprevistas relacionadas à restauração dos ambientes digitais (El-Hajj; Mirza, 2024).

As consequências também se intensificam quando a organização não dispõe de procedimentos definidos para reconhecer incidentes e conduzir ações de contenção e recuperação, visto que a ausência de responsabilidades claramente distribuídas e de preparação operacional pode retardar a identificação dos comprometimentos e dificultar a retomada das atividades, estudos sobre segurança cibernética em pequenas e médias empresas demonstram que a literatura concentra maior atenção nas medidas preventivas, enquanto a preparação para resposta ainda apresenta lacunas relevantes de investigação e implementação (Michalek; O'Shaughnessy; Wahlstrom, 2026).

Considerando essas particularidades, a definição de estratégias de proteção precisa contemplar a capacidade financeira, a complexidade da infraestrutura e a relevância dos processos que dependem dos recursos digitais, pois a adoção indiscriminada de modelos desenvolvidos para organizações maiores pode resultar em exigências técnicas e operacionais incompatíveis com a realidade das pequenas e médias empresas, tornando necessária a aplicação de critérios de avaliação que relacionem ameaças, vulnerabilidades e consequências potenciais para orientar intervenções proporcionais aos riscos identificados (El-Hajj; Mirza, 2024).

Dessa maneira, o fortalecimento da segurança cibernética nas pequenas e médias empresas depende da evolução de práticas predominantemente reativas para procedimentos capazes de examinar antecipadamente as condições que favorecem o comprometimento dos ambientes tecnológicos, a realização de avaliações técnicas estruturadas permite reconhecer fragilidades em redes, aplicações e sistemas, produzindo informações que podem fundamentar ações corretivas e aperfeiçoar os controles existentes, estabelecendo uma aproximação entre a gestão preventiva dos riscos e a utilização de metodologias destinadas à verificação prática das vulnerabilidades organizacionais (Sarker; Yunus; Deraman, 2023).

2.2 FUNDAMENTOS DA SEGURANÇA OFENSIVA E METODOLOGIAS DE IDENTIFICAÇÃO DE VULNERABILIDADES

Diferentemente das abordagens concentradas na proteção contra ameaças previamente reconhecidas, a segurança ofensiva utiliza procedimentos técnicos autorizados para examinar como sistemas, aplicações e redes podem ser comprometidos mediante a exploração de vulnerabilidades existentes, essa perspectiva permite investigar os ambientes digitais sob requisitos próximos às enfrentadas em tentativas reais de invasão, proporcionando informações sobre fragilidades que poderiam permanecer desconhecidas em avaliações restritas à verificação de configurações e à existência de mecanismos defensivos (Sarker; Yunus; Deraman, 2023).

Entre as práticas associadas a essa abordagem, os testes de intrusão constituem procedimentos destinados a avaliar a resistência de recursos tecnológicos diante de tentativas controladas de exploração, diferenciando-se das varreduras convencionais pela possibilidade de verificar tecnicamente determinadas condições de comprometimento, enquanto o levantamento automatizado identifica indícios de falhas conhecidas, a execução de testes específicos permite investigar sua explorabilidade e compreender possíveis consequências sobre os recursos avaliados, respeitando os limites previamente estabelecidos para a atividade (Lee, 2025).

Para que essas verificações produzam resultados tecnicamente consistentes, sua execução deve observar uma metodologia estruturada que contemple planejamento, definição do escopo, reconhecimento dos sistemas, identificação de vulnerabilidades, validação das condições de exploração e documentação das evidências obtidas, a organização dessas etapas contribui para estabelecer critérios de avaliação compatíveis com as características da infraestrutura examinada, evitando procedimentos desnecessários e permitindo que os resultados sejam interpretados conforme os objetivos definidos antes do início dos testes (Sarker; Yunus; Deraman, 2023).

Sob essa perspectiva, a delimitação dos recursos autorizados para avaliação representa uma condição necessária à condução responsável das atividades ofensivas, considerando que sistemas de produção, bases de dados e serviços corporativos podem apresentar diferentes níveis de sensibilidade e dependência operacional, a definição antecipada das permissões, dos procedimentos admitidos e dos requisitos de interrupção das verificações permite reduzir a possibilidade de impactos indesejados, preservando a integridade dos ambientes e a continuidade das atividades durante a realização dos testes (Sarker; Yunus; Deraman, 2023).

Quanto ao conhecimento disponibilizado aos responsáveis pela avaliação, os testes de intrusão podem ser estruturados mediante abordagens de caixa-preta, caixa-cinza e caixa-branca, diferenciadas pela quantidade de informações previamente conhecidas sobre os sistemas examinados, essa classificação possibilita selecionar condições de investigação compatíveis com os objetivos da análise, desde verificações realizadas com conhecimento restrito da infraestrutura até avaliações que utilizam

informações internas para examinar componentes, configurações e possibilidades de comprometimento com maior profundidade (Sarker; Yunus; Deraman, 2023).

Independentemente da abordagem selecionada, o reconhecimento técnico do ambiente permite identificar serviços expostos, dispositivos conectados, componentes de software e interfaces que possam apresentar condições favoráveis à exploração, a compreensão dessas características orienta as etapas posteriores de avaliação e contribui para identificar pontos de entrada potenciais, especialmente em estruturas empresariais nas quais a ausência de inventários atualizados e o gerenciamento inadequado de ativos dificultam o conhecimento sobre os recursos efetivamente disponíveis na infraestrutura tecnológica (Chidukwani; Zander; Koutsakis, 2026).

Com os recursos identificados, a análise de vulnerabilidades pode recorrer a ferramentas especializadas para verificar versões de software, configurações inseguras e falhas conhecidas em serviços e aplicações, entretanto, os resultados produzidos por mecanismos automatizados exigem interpretação técnica para distinguir ocorrências relevantes de identificações imprecisas, pois a existência de uma vulnerabilidade potencial não demonstra necessariamente que sua exploração seja viável nas condições específicas do ambiente examinado, tornando necessária a associação entre os achados e as características dos sistemas avaliados (Sarker; Yunus; Deraman, 2023).

Nesse processo, a automação oferece possibilidades de ampliar a frequência e a abrangência das verificações sem exigir que todas as atividades sejam executadas manualmente, característica particularmente relevante para empresas com restrições de pessoal especializado, experiências com ferramentas automatizadas de testes de intrusão demonstraram a viabilidade de examinar condições relacionadas ao comprometimento de credenciais, à elevação de privilégios e à simulação controlada de ransomware, permitindo reunir evidências técnicas para orientar procedimentos de correção e novas avaliações de segurança (Lee, 2025).

Apesar das possibilidades oferecidas pela automação, a interpretação dos resultados continua dependendo da compreensão sobre as características do ambiente e sobre a relevância operacional dos componentes envolvidos, uma vez que informações técnicas isoladas podem ser insuficientes para representar adequadamente as condições de segurança empresarial, avaliações que combinaram varreduras de vulnerabilidades, inspeções especializadas e análise documental demonstraram a importância de confrontar diferentes evidências para identificar discrepâncias entre os controles declarados e aqueles efetivamente implementados (Chidukwani; Zander; Koutsakis, 2026).

Em termos metodológicos, a classificação das vulnerabilidades identificadas deve considerar critérios que permitam distinguir falhas de maior gravidade de ocorrências com consequências potencialmente limitadas, relacionando características técnicas, possibilidades de exploração e condições específicas dos recursos afetados, a utilização de métodos de pontuação e avaliação contribui para organizar os resultados dos testes, embora a interpretação de sua relevância dependa das

particularidades da infraestrutura e das possíveis consequências decorrentes do comprometimento dos sistemas empresariais (Sarker; Yunus; Deraman, 2023).

No ambiente das pequenas e médias empresas, essa classificação precisa ser compatibilizada com a capacidade de investimento e com a importância dos processos sustentados pelos ativos tecnológicos, considerando que vulnerabilidades semelhantes podem produzir consequências distintas conforme a exposição dos sistemas e a sensibilidade das informações armazenadas, metodologias de avaliação de riscos adaptadas às organizações de menor porte permitem relacionar ameaças, fragilidades e impactos potenciais, favorecendo decisões corretivas proporcionais aos recursos disponíveis e às necessidades de proteção identificadas (El-Hajj; Mirza, 2024).

Concluídas as verificações, os resultados devem ser organizados em registros técnicos que descrevem as vulnerabilidades encontradas, as evidências de exploração, os recursos afetados e as recomendações de tratamento, permitindo que os responsáveis pela infraestrutura compreendam as condições identificadas e estabeleçam prioridades de intervenção, a realização de novas avaliações após a implementação das correções possibilita verificar se as fragilidades foram efetivamente tratadas, transformando os testes de intrusão em instrumentos de acompanhamento da segurança e de aperfeiçoamento progressivo dos mecanismos de proteção empresarial (Lee, 2025).

2.3 APLICAÇÃO DA SEGURANÇA OFENSIVA NA PREVENÇÃO DE INCIDENTES E NO GERENCIAMENTO DE RISCOS EMPRESARIAIS

Após a identificação das vulnerabilidades presentes na infraestrutura tecnológica, a contribuição preventiva da segurança ofensiva depende da transformação dos resultados técnicos em decisões capazes de reduzir as possibilidades de comprometimento dos recursos empresariais, esse processo envolve a interpretação das condições de exploração verificadas, a definição de prioridades corretivas e o acompanhamento das intervenções realizadas, permitindo que as informações produzidas pelos testes de intrusão sejam utilizadas para orientar melhorias concretas nos mecanismos de proteção e estabelecer procedimentos de reavaliação das fragilidades identificadas (Lee, 2025).

Para que essas intervenções estejam relacionadas às necessidades organizacionais, os resultados das avaliações ofensivas precisam integrar os processos de governança e gerenciamento de riscos, considerando a relevância dos ativos digitais, as consequências potenciais de sua indisponibilidade e os objetivos estabelecidos pela administração, essa articulação encontra correspondência no NIST Cybersecurity Framework, cuja estrutura permite relacionar identificação de riscos, implementação de medidas protetivas e preparação para incidentes, favorecendo decisões fundamentadas nas condições de segurança existentes e nas prioridades definidas para a continuidade das atividades empresariais (National Institute of Standards and Technology, 2024).

Dentro dessa perspectiva, a priorização das vulnerabilidades deve considerar fatores que ultrapassam a classificação técnica de gravidade, pois uma falha localizada em um sistema diretamente relacionado às atividades comerciais pode apresentar consequências organizacionais diferentes daquelas observadas em componentes de menor relevância operacional, a associação entre probabilidade de exploração, exposição dos recursos e impacto potencial permite estabelecer critérios de tratamento proporcionais às condições financeiras e tecnológicas das pequenas e médias empresas, contribuindo para uma distribuição mais adequada dos investimentos destinados à proteção digital (El-Hajj; Mirza, 2024).

Na avaliação das possibilidades de comprometimento, a segurança ofensiva oferece informações sobre condições que podem favorecer a atuação de invasores e comprometer mecanismos defensivos existentes, mediante procedimentos controlados que examinam fragilidades em sistemas operacionais, aplicações, redes e serviços corporativos, os resultados dessas verificações contribuem para compreender como determinadas vulnerabilidades podem ser exploradas e quais componentes permanecem expostos, permitindo direcionar as recomendações técnicas para situações efetivamente identificadas durante os testes e reduzir a dependência de avaliações fundamentadas exclusivamente em configurações presumidamente seguras (Sarker; Yunus; Deraman, 2023).

Compreendidas as condições de exposição, a seleção das medidas corretivas precisa estabelecer correspondência entre os mecanismos de ataque identificados e os recursos disponíveis para reduzir sua efetividade, incluindo atualização de sistemas, fortalecimento da autenticação, restrição de privilégios, segmentação de redes e proteção das informações armazenadas, a literatura sobre segurança cibernética em pequenas e médias empresas demonstra que a combinação dessas práticas com capacitação profissional e planejamento de resposta contribui para estruturar estratégias de defesa compatíveis com ameaças recorrentes, especialmente aquelas relacionadas ao comprometimento de credenciais e à disseminação de programas maliciosos (Awan; Alam, 2025).

Quando as vulnerabilidades identificadas envolvem permissões inadequadas, reutilização de credenciais ou ausência de atualizações, a implementação das correções deve ser acompanhada por verificações que permitam determinar se as condições anteriormente exploráveis foram efetivamente modificadas, experiências com testes de intrusão automatizados demonstram a possibilidade de estruturar processos que relacionam identificação de falhas, classificação de riscos, execução de medidas corretivas e revalidação técnica, estabelecendo uma sequência operacional destinada a acompanhar a redução das fragilidades detectadas nos ambientes empresariais (Lee, 2025).

Entretanto, a correção de vulnerabilidades conhecidas não elimina a necessidade de preparação para situações nas quais os mecanismos preventivos sejam insuficientes, considerando que novas ameaças, alterações na infraestrutura e limitações dos controles implementados podem permitir a ocorrência de comprometimentos mesmo em organizações que realizam avaliações periódicas, a

integração entre prevenção e resposta exige procedimentos definidos para reconhecer incidentes, distribuir responsabilidades e restabelecer atividades afetadas, especialmente nas pequenas e médias empresas que apresentam dificuldades para manter estruturas especializadas e processos permanentes de segurança (Michalek; O'Shaughnessy; Wahlstrom, 2026).

Nesse cenário, a verificação independente das condições de proteção contribui para identificar diferenças entre a segurança declarada pelos responsáveis e aquela demonstrada pelas evidências técnicas, pois a existência de contratos de suporte, políticas internas ou ferramentas de monitoramento pode produzir uma percepção de proteção incompatível com as vulnerabilidades efetivamente presentes na infraestrutura, avaliações realizadas com diferentes fontes de evidência identificaram fragilidades que não eram adequadamente reconhecidas pelas organizações, reforçando a necessidade de utilizar procedimentos técnicos verificáveis para fundamentar decisões de gerenciamento de riscos (Chidukwani; Zander; Koutsakis, 2026).

Para organizações com disponibilidade limitada de profissionais especializados, a incorporação dessas avaliações à rotina empresarial pode encontrar obstáculos relacionados ao conhecimento técnico, à compreensão dos resultados e à capacidade de executar as recomendações recebidas, uma vez que investimentos em ferramentas ou serviços especializados não produzem melhorias consistentes quando inexistem condições organizacionais para interpretar as vulnerabilidades e acompanhar seu tratamento, a literatura evidencia que limitações de conhecimento sobre segurança cibernética influenciam tanto a percepção dos riscos quanto a capacidade de selecionar e implementar medidas de proteção adequadas (Ali, *et al.*, 2025).

Considerando essas restrições, a adoção da segurança ofensiva deve observar critérios de viabilidade que relacionem frequência das avaliações, complexidade dos sistemas, importância dos recursos examinados e disponibilidade financeira para executar intervenções posteriores, a utilização de modelos de avaliação de riscos adaptados às pequenas e médias empresas pode contribuir para estabelecer prioridades compatíveis com sua capacidade operacional, evitando que a identificação de numerosas vulnerabilidades resulte em recomendações excessivamente complexas ou desconectadas das possibilidades concretas de implementação (El-Hajj; Mirza, 2024).

Quanto ao acompanhamento dos resultados, a eficácia das iniciativas preventivas pode ser examinada mediante registros que permitam comparar as condições identificadas em avaliações sucessivas, verificar o tratamento das vulnerabilidades prioritárias e reconhecer fragilidades que permanecem sem correção, a utilização dessas informações para atualizar os perfis de segurança e revisar os planos de ação estabelece uma relação entre evidências técnicas e melhoria contínua, favorecendo a identificação de diferenças entre a situação atual da organização e os resultados de proteção pretendidos pela administração (National Institute of Standards and Technology, 2024).

Dessa forma, a contribuição da segurança ofensiva para a prevenção de incidentes em pequenas e médias empresas deve ser compreendida a partir de sua integração com medidas corretivas, processos organizacionais e mecanismos de preparação para situações de comprometimento, sem pressupor que a realização de testes seja suficiente para demonstrar a redução efetiva da ocorrência de ataques, uma vez que a literatura ainda apresenta limitações quanto à validação empírica de soluções adaptadas a essas organizações, tornando relevante analisar continuamente as condições de aplicação, os resultados alcançados e sua relação com o fortalecimento da capacidade empresarial de prevenção e resposta (Michalek; O'Shaughnessy; Wahlstrom, 2026).

3 METODOLOGIA

A pesquisa foi desenvolvida por meio de uma abordagem qualitativa, de natureza bibliográfica e caráter exploratório e descritivo, com o propósito de compreender as contribuições da segurança ofensiva para a prevenção de incidentes cibernéticos em pequenas e médias empresas, esse delineamento possibilitou examinar fundamentos teóricos, metodologias de identificação de vulnerabilidades e estratégias de proteção organizacional, estabelecendo relações entre os conhecimentos científicos disponíveis e as condições de aplicação das práticas ofensivas em ambientes empresariais (Gil, 2019).

Como procedimento de investigação, adotou-se a revisão bibliográfica de caráter narrativo, orientada pela análise de publicações científicas e documentos técnicos relacionados à segurança cibernética, aos testes de intrusão e ao gerenciamento de riscos, a utilização desse método permitiu reunir diferentes perspectivas sobre a exposição das organizações a ameaças digitais, considerando tanto os fundamentos das avaliações técnicas quanto as particularidades financeiras e operacionais que influenciam sua implementação.

Para delimitar o conteúdo examinado, foram considerados estudos que apresentassem relação direta com a identificação de vulnerabilidades, os mecanismos de exploração de falhas e as possibilidades de prevenção de incidentes em infraestruturas corporativas, a pertinência temática, a consistência das informações e a contribuição para o objetivo estabelecido orientaram a seleção bibliográfica, preservando a correspondência entre os materiais utilizados e as questões investigadas.

Na organização do conteúdo, as informações foram distribuídas em três eixos analíticos complementares, abrangendo a exposição das pequenas e médias empresas a ameaças cibernéticas, os fundamentos e procedimentos empregados em avaliações ofensivas e a integração dessas práticas aos processos de prevenção e gerenciamento de riscos, essa estrutura permitiu estabelecer uma sequência de análise que relacionasse as vulnerabilidades organizacionais às possibilidades de identificação, tratamento e acompanhamento das condições de segurança.

Posteriormente, procedeu-se à leitura analítica e à interpretação das informações, buscando identificar aproximações conceituais, diferenças entre metodologias e relações entre as evidências apresentadas nas publicações examinadas, o tratamento do conteúdo privilegiou a comparação crítica dos argumentos e resultados disponíveis, permitindo construir uma discussão articulada sobre as possibilidades e limitações das práticas investigadas, em conformidade com os procedimentos de análise bibliográfica descritos por Marconi e Lakatos (2017).

Durante a interpretação dos materiais, foram examinadas as condições de aplicação dos testes de intrusão, os critérios utilizados na classificação de vulnerabilidades e a relação entre as evidências técnicas e a definição de medidas corretivas, considerando as particularidades das pequenas e médias empresas, a análise também contemplou as restrições de recursos, a necessidade de acompanhamento das correções e a integração das avaliações aos mecanismos de proteção existentes, de maneira a compreender a viabilidade dessas práticas em diferentes condições organizacionais.

Quanto à discussão dos resultados, adotou-se uma perspectiva interpretativa fundamentada no confronto entre as contribuições teóricas e as evidências empíricas identificadas, buscando distinguir a capacidade de reconhecer vulnerabilidades da efetiva redução da ocorrência de incidentes, essa diferenciação permitiu examinar os limites das conclusões apresentadas na literatura e evitar a atribuição de resultados preventivos que não tenham sido demonstrados pelas investigações consultadas.

Por se tratar de uma investigação fundamentada em materiais bibliográficos, não foram realizados testes de intrusão, simulações de ataques ou procedimentos experimentais em infraestruturas empresariais, as conclusões foram elaboradas a partir da interpretação crítica das fontes examinadas, respeitando o alcance das evidências disponíveis e direcionando a discussão para as condições em que a segurança ofensiva pode contribuir para o aprimoramento dos mecanismos de prevenção de incidentes cibernéticos.

4 RESULTADOS E DISCUSSÃO

A análise das publicações evidenciou que a exposição de pequenas e médias empresas a incidentes cibernéticos está relacionada tanto às vulnerabilidades presentes nas infraestruturas tecnológicas quanto às condições organizacionais que dificultam sua identificação e correção, enquanto Ali, *et al.* (2025) associam as limitações de proteção à insuficiência de conhecimento especializado, à percepção inadequada dos riscos e às restrições financeiras, Michalek, O'Shaughnessy e Wahlstrom (2026) ampliam essa interpretação ao demonstrar que a distribuição imprecisa de responsabilidades e a dificuldade de estabelecer prioridades comprometem a preparação preventiva, indicando que a segurança empresarial depende da articulação entre recursos técnicos, decisões administrativas e procedimentos operacionais.

Essa relação entre fatores humanos e tecnológicos torna-se mais evidente quando são examinadas as modalidades de ataque que afetam as organizações de menor porte, pois Awan e Alam (2025) identificam phishing, ransomware, engenharia social e fragilidades de autenticação entre as ameaças recorrentes, enquanto Ali, *et al.* (2025) demonstram que a baixa compreensão dos riscos pode interferir na adoção de mecanismos de proteção, permitindo interpretar que a exposição empresarial decorre de uma combinação de condições técnicas exploráveis e práticas organizacionais insuficientes para reconhecer e tratar essas fragilidades.

Entretanto, reconhecer a existência dessas ameaças não significa compreender adequadamente as condições reais de segurança de uma organização, conforme evidenciado por Chidukwani, Zander e Koutsakis (2026), que identificaram divergências entre os controles declarados e aqueles efetivamente observados em oito pequenas e médias empresas, enquanto Sarker, Yunus e Deraman (2023) demonstram que metodologias de testes de intrusão permitem examinar vulnerabilidades mediante procedimentos estruturados de avaliação técnica, estabelecendo uma relação entre a necessidade de validação independente e a utilização de práticas ofensivas para investigar fragilidades que poderiam permanecer desconhecidas.

Os resultados apresentados por Chidukwani, Zander e Koutsakis (2026) também indicam que a percepção de segurança pode ser influenciada pela interpretação equivocada das responsabilidades atribuídas aos prestadores de serviços tecnológicos, situação que compromete a identificação de controles ausentes e de vulnerabilidades não tratadas, Lee (2025) complementa essa discussão ao apresentar a utilização de testes de intrusão automatizados em pequenas e médias empresas, mediante os quais foram verificadas condições relacionadas à reutilização de credenciais, à ausência de atualizações e a possibilidades de comprometimento, demonstrando a utilidade de avaliações técnicas para transformar suspeitas de fragilidade em evidências verificáveis.

Embora a identificação automatizada de vulnerabilidades contribua para ampliar o conhecimento sobre as condições de exposição dos sistemas, sua utilização isolada apresenta limitações relacionadas à interpretação dos resultados e à determinação das possibilidades efetivas de exploração, Sarker, Yunus e Deraman (2023) distinguem metodologias, ferramentas e critérios empregados nos testes de intrusão, enquanto Lee (2025) apresenta a validação de cenários envolvendo comprometimento de credenciais, elevação de privilégios e simulação de ransomware, permitindo compreender que a contribuição da segurança ofensiva depende da correspondência entre os achados técnicos e as condições concretas de funcionamento dos ambientes avaliados.

Quando essas evidências são incorporadas aos processos de gerenciamento de riscos, torna-se possível estabelecer prioridades corretivas fundamentadas na exposição dos recursos e nas consequências potenciais de seu comprometimento, enquanto El-Hajj e Mirza (2024) propõem uma estrutura de avaliação adaptada às limitações financeiras e operacionais das pequenas e médias

empresas, Sarker, Yunus e Deraman (2023) examinam métodos de classificação utilizados na análise de vulnerabilidades, indicando que a gravidade técnica das falhas precisa ser interpretada em conjunto com as características dos ativos afetados para orientar decisões proporcionais às necessidades organizacionais.

A priorização também depende da capacidade de relacionar os resultados dos testes aos objetivos empresariais e aos mecanismos de proteção já implementados, pois o National Institute of Standards and Technology (2024) estabelece uma estrutura de gerenciamento de riscos que contempla governança, identificação, proteção, detecção, resposta e recuperação, enquanto El-Hajj e Mirza (2024) demonstram a necessidade de adaptar modelos de avaliação às condições específicas das organizações de menor porte, permitindo compreender que a utilização dos resultados ofensivos deve orientar decisões administrativas e investimentos em segurança, em vez de permanecer restrita à produção de relatórios técnicos.

Sob a perspectiva da implementação, a disponibilidade de ferramentas automatizadas pode favorecer a realização de avaliações mais frequentes em ambientes com recursos humanos limitados, conforme observado por Lee (2025), que também propõe a possibilidade de utilização de serviços de testes de intrusão como alternativa operacional para pequenas e médias empresas, entretanto, Ali, *et al.* (2025) demonstram que as limitações de conhecimento especializado e de compreensão dos riscos interferem na capacidade de adoção de soluções de segurança, indicando que a contratação de serviços externos precisa estar acompanhada de responsabilidades definidas e condições efetivas para executar as recomendações recebidas.

Essa necessidade de acompanhamento demonstra que os benefícios das avaliações ofensivas dependem da continuidade das ações desenvolvidas após a identificação das vulnerabilidades, considerando que Lee (2025) propõe um processo composto por classificação de riscos, tratamento das fragilidades e revalidação das correções, enquanto o National Institute of Standards and Technology (2024) orienta a atualização dos perfis organizacionais de segurança e dos planos de ação conforme as condições identificadas, permitindo interpretar que o aperfeiçoamento da proteção exige verificações sucessivas e acompanhamento das alterações realizadas na infraestrutura tecnológica.

Mesmo com a adoção de procedimentos de correção e reavaliação, a prevenção de incidentes não pode ser compreendida como resultado exclusivo da aplicação de testes de intrusão, uma vez que vulnerabilidades desconhecidas, falhas humanas e alterações nos sistemas podem produzir novas condições de comprometimento, enquanto Awan e Alam (2025) apresentam medidas complementares relacionadas à autenticação multifator, segmentação de redes, atualização de componentes e proteção de cópias de segurança, Michalek, O'Shaughnessy e Wahlstrom (2026) ressaltam a necessidade de equilibrar prevenção e capacidade de resposta, evidenciando que avaliações ofensivas devem integrar uma estrutura de proteção mais abrangente.

Essa integração apresenta implicações para a preparação das empresas diante de incidentes que não puderam ser evitados, pois Michalek, O'Shaughnessy e Wahlstrom (2026) identificam menor desenvolvimento científico das práticas de resposta quando comparadas às iniciativas preventivas, enquanto o National Institute of Standards and Technology (2024) estabelece a necessidade de manter procedimentos destinados à detecção, contenção e recuperação de atividades comprometidas, permitindo compreender que informações obtidas durante avaliações ofensivas também podem orientar o reconhecimento de condições de ataque e a definição de medidas destinadas à preservação da continuidade operacional.

Quanto à avaliação da efetividade preventiva, os estudos examinados sustentam a utilização de indicadores relacionados à identificação de vulnerabilidades, à execução de correções e à verificação posterior das condições de exploração, entretanto, a diminuição de fragilidades identificadas não comprova isoladamente uma redução na frequência de incidentes, distinção relevante diante das limitações de validação empírica apontadas por Michalek, O'Shaughnessy e Wahlstrom (2026), enquanto El-Hajj e Mirza (2024) reconhecem a necessidade de análises quantitativas adicionais para examinar a efetividade do modelo proposto, demonstrando a importância de diferenciar resultados técnicos observáveis de benefícios preventivos que ainda dependem de comprovação.

A comparação das evidências permite reconhecer uma convergência entre a necessidade de avaliações técnicas independentes e a adoção de procedimentos corretivos compatíveis com a realidade das pequenas e médias empresas, pois Chidukwani, Zander e Koutsakis (2026) demonstram que verificações especializadas podem revelar fragilidades não reconhecidas internamente, enquanto Lee (2025) apresenta possibilidades de aplicação de testes automatizados para identificar condições de exploração e orientar seu tratamento, resultados que sustentam a utilização da segurança ofensiva como instrumento de diagnóstico e aperfeiçoamento dos controles, sem permitir generalizar sua capacidade de impedir incidentes em diferentes contextos empresariais.

Portanto, a contribuição identificada na literatura concentra-se na possibilidade de antecipar o reconhecimento de condições exploráveis, estabelecer prioridades fundamentadas em evidências e acompanhar a implementação de medidas corretivas, enquanto Sarker, Yunus e Deraman (2023) fundamentam tecnicamente a utilização de metodologias estruturadas de testes de intrusão, El-Hajj e Mirza (2024) demonstram a pertinência de modelos de avaliação adaptados às organizações de menor porte e Ali, *et al.* (2025) evidenciam a influência das condições humanas e financeiras sobre a adoção de práticas de segurança, permitindo concluir que a efetividade preventiva da segurança ofensiva depende de sua integração contínua ao gerenciamento de riscos e à capacidade operacional das empresas.

5 CONSIDERAÇÕES FINAIS

A análise desenvolvida permitiu compreender que a segurança ofensiva constitui uma abordagem relevante para o fortalecimento da proteção cibernética em pequenas e médias empresas, especialmente pela possibilidade de identificar vulnerabilidades antes que sejam exploradas em situações reais de comprometimento, os resultados discutidos demonstraram que a utilização de avaliações técnicas estruturadas contribui para ampliar o conhecimento sobre as condições de exposição dos ambientes empresariais, fornecendo informações que podem orientar intervenções preventivas e aperfeiçoar os mecanismos de segurança existentes.

Entre as contribuições identificadas, destaca-se a capacidade dos testes de intrusão de verificar condições de exploração que poderiam permanecer desconhecidas em avaliações fundamentadas exclusivamente em configurações declaradas ou na presença de ferramentas defensivas, essa característica permite estabelecer uma compreensão mais precisa das fragilidades tecnológicas, favorecendo a identificação de situações relacionadas ao comprometimento de credenciais, às permissões inadequadas e à ausência de atualizações, cujas consequências podem comprometer a integridade das informações e a continuidade das operações empresariais.

Entretanto, a identificação antecipada de vulnerabilidades não representa uma garantia de prevenção de incidentes, uma vez que sua contribuição depende da interpretação adequada dos resultados, da implementação das medidas corretivas e da realização de verificações posteriores, essa relação demonstra que a segurança ofensiva precisa ser incorporada a um processo contínuo de gerenciamento de riscos, no qual as fragilidades identificadas sejam avaliadas conforme sua relevância operacional e acompanhadas até que as condições de exposição sejam efetivamente tratadas.

No caso das pequenas e médias empresas, a viabilidade dessa abordagem está diretamente relacionada à capacidade de adaptar os procedimentos técnicos às limitações financeiras e à disponibilidade de profissionais especializados, sendo necessário estabelecer prioridades que considerem a importância dos ativos digitais e as consequências potenciais de seu comprometimento, a adoção de avaliações proporcionais à estrutura organizacional favorece a utilização racional dos recursos disponíveis, permitindo direcionar investimentos para intervenções que apresentem maior correspondência com as necessidades de proteção identificadas.

Quanto ao objetivo estabelecido, verificou-se que a contribuição da segurança ofensiva para a prevenção de incidentes está associada à produção de evidências técnicas, à priorização das vulnerabilidades e ao acompanhamento das correções implementadas, entretanto, as publicações examinadas apresentam limitações quanto à demonstração de uma relação direta entre a realização dessas avaliações e a diminuição da frequência de ataques bem-sucedidos, circunstância que exige distinguir a melhoria das condições de proteção da comprovação efetiva de redução dos incidentes.

Diante dessas limitações, recomenda-se que investigações futuras contemplem avaliações longitudinais em pequenas e médias empresas, acompanhando indicadores relacionados à recorrência de vulnerabilidades, ao tempo necessário para implementação de correções e à ocorrência de incidentes antes e depois da adoção de práticas ofensivas, pesquisas dessa natureza poderão produzir evidências mais consistentes sobre a efetividade preventiva das metodologias utilizadas, permitindo compreender sua viabilidade econômica e seus resultados em organizações com diferentes níveis de maturidade tecnológica.

Conclui-se que a segurança ofensiva apresenta contribuições relevantes para o aperfeiçoamento das práticas de proteção cibernética em pequenas e médias empresas, desde que sua aplicação esteja vinculada ao planejamento organizacional, ao tratamento das vulnerabilidades e à continuidade das avaliações técnicas, sua utilização sistemática pode favorecer decisões fundamentadas em evidências e fortalecer a capacidade empresarial de reconhecer e reduzir condições de exposição, consolidando uma perspectiva preventiva orientada pela verificação das fragilidades e pelo aprimoramento permanente dos mecanismos de segurança.

REFERÊNCIAS

ALI, Adnan Bin Amanat; AYYASAMY, Ramesh Kumar; AKBAR, Rehan; JEBNA, Abdulkarim Kanaan; ADNAN, Kiran. Cybersecurity infrastructure compliance key factors to detect and mitigate malware attacks in SMEs: a systematic literature review. SAGE Open, v. 15, n. 1, 2025. DOI: https://doi.org/10.1177/21582440251314671

AWAN, Mujtaba; ALAM, Abu. Cybersecurity threats and defensive strategies for small and medium firms: a systematic mapping study. Administrative Sciences, Basel, v. 15, n. 12, art. 481, 2025. DOI: https://doi.org/10.3390/admsci15120481.

CHIDUKWANI, Alladean; ZANDER, Sebastian; KOUTSAKIS, Polychronis. Beyond self-reporting: uncovering the operational realities of SME cybersecurity through expert assessment. Computers & Security, Amsterdam, v. 164, art. 104839, 2026. DOI: https://doi.org/10.1016/j.cose.2026.104839.

EL-HAJJ, Mohammed; MIRZA, Zuhayr Aamir. Protecting small and medium enterprises: a specialized cybersecurity risk assessment framework and tool. Electronics, Basel, v. 13, n. 19, art. 3910, 2024. DOI: https://doi.org/10.3390/electronics13193910.

GIL, Antonio Carlos. Métodos e técnicas de pesquisa social. 7. ed. São Paulo: Atlas, 2019.

LEE, Keun-Ho. Design of a security vulnerability analysis and response model based on automated penetration testing for SMEs: a case study using Pentera Core. Journal of Internet of Things and Convergence, v. 11, n. 2, p. 179-184, 2025. DOI: https://doi.org/10.20465/KIOTS.2025.11.2.179.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. Fundamentos de metodologia científica. 8. ed. São Paulo: Atlas, 2017.

MICHALEK, Josephine; O'SHAUGHNESSY, Peter Kevin; WAHLSTROM, Kirsten. Cyber incident prevention and response for small and medium sized enterprises: a scoping review. Computers & Security, Amsterdam, v. 169, art. 104972, 2026. DOI: https://doi.org/10.1016/j.cose.2026.104972.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg: NIST, 2024. (NIST Cybersecurity White Paper, NIST CSWP 29). DOI: https://doi.org/10.6028/NIST.CSWP.29.

SARKER, Kamal Uddin; YUNUS, Farizah; DERAMAN, Aziz. Penetration taxonomy: a systematic review on the penetration process, framework, standards, tools, and scoring methods. Sustainability, Basel, v. 15, n. 13, art. 10471, 2023. DOI: https://doi.org/10.3390/su151310471.