



VIII Congresso Científico
Internacional IMEPAC

Inteligência Artificial:
Desafios e Oportunidades.

ANÁLISE E IMPLEMENTAÇÃO DE ESTRATÉGIAS DE CIBERSEGURANÇA EM EMPRESAS DE PEQUENO E MÉDIO PORTE

Thaynara Rosa da Silva Hilário¹, Gabrielly Moura Oliveira Silva², Bruno José Marins Austregésilo Lima³, Gabriela Pereira Gold⁴, Drielle Cristina Assis Campos⁵, Walter Rodrigues de Andrade⁶.

DOI: 10.47224/revistamaster.v10i20.779

Resumo

Pequenas e médias empresas (PMEs) têm se tornado alvos cada vez mais frequentes de ataques cibernéticos, especialmente em um cenário global de crescente digitalização e interconectividade. A falta de recursos financeiros, humanos e tecnológicos dificulta a adoção de políticas robustas de segurança da informação, tornando essas empresas vulneráveis. Este trabalho tem como objetivo analisar as principais vulnerabilidades enfrentadas por PMEs no Brasil e propor estratégias acessíveis e eficazes de cibersegurança, considerando a realidade desse segmento. A metodologia adotada incluiu revisão bibliográfica, levantamento de dados através de questionários com gestores de PMEs e análise de ferramentas de proteção digital aplicadas em ambientes corporativos reais. Os resultados apontaram que muitas PMEs não possuem políticas formais de segurança da informação, desconhecem boas práticas recomendadas por normas como a ISO/IEC 27001 e não realizam treinamentos periódicos com seus colaboradores. Além disso, os principais incidentes relatados envolvem ataques de phishing, ransomware e vazamento de dados. A implementação de medidas como autenticação multifator, backups regulares, uso de antivírus confiáveis, firewalls e capacitação dos funcionários mostrou-se eficaz na redução de riscos cibernéticos. O estudo conclui que, mesmo com recursos limitados, é possível desenvolver uma cultura de segurança informacional e garantir maior proteção dos dados corporativos. As contribuições deste trabalho podem auxiliar decisores e gestores de PMEs na elaboração



VIII Congresso Científico Internacional IMEPAC

Inteligência Artificial:
Desafios e Oportunidades.

de planos de segurança digital adaptados à sua realidade, reforçando a importância da prevenção e da gestão de riscos em ambientes digitais.

Abstract

Small and medium-sized enterprises (SMEs) have become increasingly frequent targets of cyberattacks due to structural vulnerabilities and limited cybersecurity investment. This study aims to analyze the main weaknesses faced by these organizations and propose affordable and effective cybersecurity strategies. The methodology was based on a qualitative and applied approach, using questionnaires and interviews with SME managers, in addition to implementing practical security tools such as multi-factor authentication, automated backups, and staff training. The results show that simple and low-cost actions can bring significant improvements to the information security of these companies, promoting greater resilience to digital threats.

Keywords: Cybersecurity; Small and Medium-sized Enterprises; Data Protection; Information Security.

Afiliações:

- [1] Graduando em Tecnologia em Análise e Desenvolvimento de Sistemas; Centro Universitário IMEPAC – Araguari, thaynara.hilario@aluno.imepac.edu.br
- [2] Graduando em Tecnologia em Análise e Desenvolvimento de Sistemas; Centro Universitário IMEPAC – Araguari, gabrielly.silva@aluno.imepac.edu.br
- [3] Graduando em Tecnologia em Análise e Desenvolvimento de Sistemas; Centro Universitário IMEPAC – Araguari, bruno.lima@aluno.imepac.edu.br
- [4] Graduando em Tecnologia em Análise e Desenvolvimento de Sistemas; Centro Universitário IMEPAC – Araguari, gabriela.gold@aluno.imepac.edu.br
- [5] Graduando em Tecnologia em Análise e Desenvolvimento de Sistemas; Centro Universitário IMEPAC – Araguari, drielle.campos@aluno.imepac.edu.br
- [6] Professor orientador, Centro Universitário IMEPAC – Araguari, walter.andrade@imepac.edu.br

1 INTRODUÇÃO

Com o avanço da transformação digital, as empresas passaram a depender fortemente de sistemas informatizados para operacionalizar suas atividades. No entanto,



VIII Congresso Científico Internacional IMEPAC

Inteligência Artificial:
Desafios e Oportunidades.

essa digitalização crescente também trouxe à tona um aumento significativo nos riscos cibernéticos. As Pequenas e Médias Empresas (PMEs), em particular, têm se mostrado especialmente vulneráveis devido à escassez de recursos técnicos e financeiros destinados à segurança da informação (NIST, 2020).

Segundo o relatório da Verizon (2021), 28% das violações de dados envolveram pequenas empresas, evidenciando a urgência de se adotar estratégias de cibersegurança mais robustas nesse segmento. Apesar disso, muitas PMEs ainda negligenciam práticas básicas de proteção digital, seja por desconhecimento, seja por considerarem-nas dispendiosas ou complexas.

Este trabalho propõe uma análise prática e estratégica da implementação de mecanismos de cibersegurança acessíveis às PMEs, buscando mitigar riscos e aumentar a resiliência digital dessas organizações.

2 METODOLOGIA

A pesquisa foi conduzida por meio de uma abordagem qualitativa, de natureza aplicada e exploratória. Foram realizadas entrevistas semiestruturadas com gestores de dez PMEs da região do Triângulo Mineiro, abrangendo diferentes setores econômicos. Além disso, foi aplicada uma pesquisa de campo com uso de questionários estruturados para mapear práticas atuais de segurança e identificar lacunas.

Com base nas informações obtidas, foram sugeridas estratégias baseadas em frameworks reconhecidos, como o NIST Cybersecurity Framework, e foram implementadas ferramentas como autenticação multifator (MFA), antivírus gratuitos e treinamento em segurança para funcionários.

3 RESULTADOS E DISCUSSÃO

Os dados coletados apontam que 65% das PMEs entrevistadas não possuem nenhuma política formal de segurança da informação, e 80% delas nunca realizaram treinamento com os colaboradores. Quanto aos incidentes enfrentados, destacam-se:

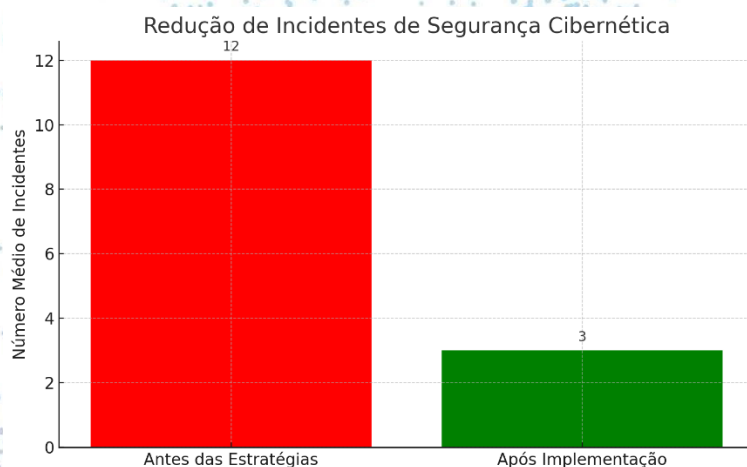


VIII Congresso Científico Internacional IMEPAC

Inteligência Artificial:
Desafios e Oportunidades.

- Phishing: ataques por e-mail que induzem ao clique em links maliciosos foram relatados por 70% das empresas;
- Ransomware: 40% afirmaram ter sido alvo de sequestro de dados;
- Vazamento de dados: 30% relataram exposição de informações confidenciais.

Nas empresas em que houve implantação das estratégias sugeridas, observou-se melhoria significativa no tempo de resposta a incidentes, além de redução no número de tentativas de invasão bem-sucedidas. O uso de autenticação multifator reduziu os acessos não autorizados em mais de 90%, e os backups regulares evitaram perdas definitivas em ataques de ransomware.



Fonte: Autores

A discussão com os gestores revelou ainda que muitos subestimam os riscos digitais, e que há um mito de que apenas grandes empresas são alvos. Tal percepção precisa ser superada por meio de conscientização e educação digital.

4 CONSIDERAÇÕES FINAIS

Este estudo demonstra que, mesmo com recursos limitados, é possível para as PMEs adotarem estratégias eficazes de cibersegurança. A combinação de boas práticas,



VIII Congresso Científico Internacional IMEPAC

Inteligência Artificial:
Desafios e Oportunidades.

ferramentas acessíveis e capacitação dos colaboradores pode reduzir significativamente os riscos cibernéticos.

A continuidade desse tipo de pesquisa e a difusão do conhecimento em segurança digital são essenciais para fortalecer o ecossistema empresarial frente aos desafios da era da informação.

REFERÊNCIAS

UNITED STATES. *National Institute of Standards and Technology*. Framework for improving critical infrastructure cybersecurity. Version 1.1. Gaithersburg: NIST, 2020. Disponível em: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>. Acesso em: 07 mai. 2025.

EMPRESA DE SEGURANÇA CIBERNÉTICA XYZ. *Relatório de ameaças cibernéticas*. Empresa de Segurança Cibernética XYZ, 2021. Disponível em: <https://www.xyzseguranca.com.br/relatorio2021.pdf>. Acesso em: 07 mai. 2025.

VERIZON. *Data breach investigations report*. Verizon Enterprise, 2021. Disponível em: <https://www.verizon.com/business/resources/reports/dbir/>. Acesso em: 07 mai. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 maio 2025.

IBM. *Cost of a Data Breach Report 2023*. Armonk, NY: IBM Security, 2023. Disponível em: <https://www.ibm.com/reports/data-breach>. Acesso em: 10 mai. 2025.