REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

# OS DESAFIOS NA PROTEÇÃO DE INFORMAÇÕES SENSÍVEIS EM PEQUENAS E MÉDIAS EMPRESAS DIANTE DE ATAQUES CIBERNÉTICOS

## *THE CHALLENGES IN PROTECTING SENSITIVE INFORMATION IN SMALL AND MEDIUM-SIZED ENTERPRISES AGAINST CYBERATTACKS*

## *LOS DESAFÍOS EN LA PROTECCIÓN DE INFORMACIÓN SENSIBLE EN PEQUEÑAS Y MEDIANAS EMPRESAS FRENTE A ATAQUES CIBERNÉTICOS*

Andrei Pereira dos Santos[1], Eliabe Anderson da Silva[1], Diego Santos Almeida Pinto[1]

e6106885
https://doi.org/10.47820/recima21.v6i10.6885

PUBLICADO: 10/2025

**RESUMO**

As pequenas e médias empresas (PMEs) são pilares fundamentais da economia global, porém, sua crescente digitalização, acelerada pela pandemia, as torna alvos preferenciais para ataques cibernéticos. Este artigo tem como objetivo investigar os principais desafios e vulnerabilidades enfrentados pelas PMEs na proteção de suas informações sensíveis. A pesquisa, de natureza qualitativa e baseada em uma extensa revisão bibliográfica, analisa como fatores como limitações de recursos, ausência de políticas de segurança estruturadas e a falta de conscientização dos colaboradores — agravada pelo cenário de trabalho remoto — contribuem para a exposição a riscos digitais. Os resultados demonstram que as ameaças mais recorrentes, como *phishing* e *ransomware*, exploram principalmente o fator humano. Conclui-se que a mitigação eficaz desses riscos não depende apenas de tecnologia, mas da implementação de uma cultura de segurança robusta, que inclua educação digital contínua (além de treinamentos pontuais), políticas claras e a adequação à Lei Geral de Proteção de Dados (LGPD). A adoção dessas estratégias é crucial para garantir a resiliência e a sustentabilidade das PMEs no cenário digital contemporâneo.

**PALAVRAS-CHAVE:** Segurança da Informação. Cibersegurança. Pequenas e Médias Empresas. Educação Digital. LGPD.

***ABSTRACT***

*Small and medium-sized enterprises (SMEs) are fundamental pillars of the global economy; however, their increasing digitalization, accelerated by the pandemic, makes them prime targets for cyberattacks. This article aims to investigate the main challenges and vulnerabilities SMEs face in protecting their sensitive information. The research, qualitative in nature and based on an extensive literature review, analyzes how factors such as financial resource limitations, the absence of structured security policies, and a lack of employee awareness — aggravated by the remote work scenario — contribute to digital risk exposure. The results show that the most recurrent threats, such as phishing and ransomware, primarily exploit the human factor. It is concluded that the effective mitigation of these risks depends not only on technology investments but on a robust security culture, which includes continuous digital education (beyond standard training), clear policies, and compliance with legal regulations, such as the General Data Protection Law (LGPD). The adoption of these integrated strategies is crucial to ensure the resilience and sustainability of SMEs in the contemporary digital landscape.*

***KEYWORDS:*** *Information Security. Cybersecurity. Small and Medium-Sized Enterprises. Digital Education. LGPD.*

[1] Gestão da Tecnologia da Informação no Centro Universitário de Goiatuba – UNICERRADO.



Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



***RESUMEN***
*Las pequeñas y medianas empresas (PYMES) son pilares fundamentales de la economía global; sin embargo, su creciente digitalización, acelerada por la pandemia, las convierte en blancos preferenciales para los ciberataques. Este artículo tiene como objetivo investigar los principales desafíos y vulnerabilidades que enfrentan las PYMES en la protección de su información sensible. La investigación, de carácter cualitativo y basada en una extensa revisión bibliográfica, analiza cómo factores como las limitaciones de recursos financieros, la ausencia de políticas de seguridad estructuradas y la falta de conciencia de los empleados —agravada por el escenario de trabajo remoto— contribuyen a la exposición a riesgos digitales. Los resultados demuestran que las amenazas más recurrentes, como el phishing y el ransomware, explotan principalmente el factor humano. Se concluye que la mitigación efectiva de estos riesgos no solo depende de inversiones en tecnología, sino de la implementación de una cultura de seguridad robusta, que incluya educación digital continua (más allá de capacitaciones puntuales), la definición de políticas claras y el cumplimiento de normativas legales, como la Ley General de Protección de Datos (LGPD). La adopción de estas estrategias integradas es crucial para garantizar la resiliencia y la sostenibilidad de las PYMES en el escenario digital contemporáneo.*

***PALABRAS CLAVE:*** *Seguridad de la Información. Ciberseguridad. Pequeñas y Medianas Empresas. Educación Digital. LGPD.*

## INTRODUÇÃO

As pequenas e médias empresas (PMEs) desempenham um papel central no tecido econômico global, impulsionando a inovação, a geração de empregos e o desenvolvimento local. No entanto, a transformação digital, que se tornou um imperativo para a competitividade, expôs essas organizações a um cenário de ameaças cibernéticas cada vez mais complexo e persistente. Essa transformação foi drasticamente acelerada pela pandemia da COVID-19, que forçou uma migração abrupta para o trabalho remoto, muitas vezes sem o planejamento de segurança adequado, ampliando exponencialmente a superfície de ataque. Diferentemente de grandes corporações, as PMEs frequentemente operam com recursos limitados, tanto financeiros quanto humanos, o que as torna alvos particularmente vulneráveis a ataques digitais.

A percepção equivocada de que "são pequenas demais para serem um alvo" é um mito perigoso que mascara uma realidade alarmante: agentes maliciosos veem nessas empresas portais de entrada para cadeias de suprimentos maiores ou alvos fáceis para obter ganhos financeiros rápidos (Kaspersky, 2023). A proteção de informações sensíveis — dados de clientes, segredos comerciais, informações financeiras e dados pessoais de colaboradores — transcendeu o âmbito técnico e se consolidou como um pilar estratégico para a sustentabilidade e a reputação de qualquer negócio.

A ocorrência de um incidente de segurança pode resultar em consequências devastadoras, incluindo perdas financeiras diretas, interrupção das operações, danos à imagem da marca e sanções legais severas, especialmente com a vigência de regulamentações como a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) no Brasil.


Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Neste contexto, emerge o problema de pesquisa: Como as pequenas e médias empresas podem fortalecer a proteção de suas informações sensíveis diante de um cenário de recursos limitados e ameaças cibernéticas crescentes, considerando as vulnerabilidades técnicas, humanas e organizacionais?

A relevância deste estudo reside na necessidade urgente de fornecer direcionamentos claros e acessíveis para que gestores de PMEs possam navegar neste ambiente desafiador, compreendendo que a segurança da informação é um investimento essencial e não um custo dispensável.

O objetivo geral deste artigo é investigar os desafios e as vulnerabilidades enfrentados pelas PMEs na proteção de dados e propor um conjunto de estratégias eficazes e de baixo custo para a mitigação de riscos cibernéticos. Para alcançar este propósito, foram definidos os seguintes objetivos específicos: a) Analisar as principais ameaças cibernéticas que afetam as PMEs e as vulnerabilidades humanas e organizacionais que facilitam esses ataques; b) Investigar estratégias de segurança cibernética acessíveis, incluindo medidas técnicas e ações focadas na capacitação de colaboradores; c) Avaliar o impacto da conformidade com a LGPD como um catalisador para a melhoria da governança de dados nas PMEs; d) Examinar como a aceleração digital pós-pandemia intensificou as vulnerabilidades e redefiniu a necessidade de educação digital para os colaboradores.

## 1. REFERENCIAL TEÓRICO

A fundamentação teórica desta pesquisa abrange quatro áreas interligadas: a natureza da segurança da informação em PMEs, as principais estratégias de mitigação de riscos, o arcabouço legal imposto pela LGPD, e o impacto conjuntural da aceleração digital pós-pandemia sobre as vulnerabilidades humanas e organizacionais.

### 1.1. Vulnerabilidades e Ameaças Cibernéticas no Contexto das PMEs

A segurança da informação, definida como a proteção de informações e sistemas de informação contra acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados (Whitman; Mattord, 2019), é um desafio magnificado no ambiente das PMEs. A principal vulnerabilidade reside na escassez de recursos. Amorim (2022, p. 45) aponta que "a escassez de recursos destinados à segurança cibernética nas PMEs as transforma em alvos preferenciais para agentes maliciosos, que se aproveitam de falhas básicas de configuração e da ausência de políticas formais".

Essa limitação se desdobra em sistemas operacionais e *softwares* desatualizados, ausência de soluções de segurança robustas (como *firewalls* e sistemas de detecção de intrusão) e falta de pessoal especializado.


Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



O fator humano é consistentemente identificado como o elo mais fraco na cadeia de segurança. Ataques de engenharia social, especialmente o *phishing*, são extremamente eficazes nesse contexto. Pereira e Silva (2021, p. 102) destacam que "o *phishing* e outras formas de engenharia social exploram justamente o despreparo dos usuários, sendo uma das principais formas de invasão". Colaboradores sem treinamento adequado podem, inadvertidamente, clicar em links maliciosos, divulgar credenciais ou executar arquivos infectados, comprometendo toda a rede corporativa.

Uma ameaça de impacto particularmente severo é o *ransomware*. Este tipo de *malware* criptografa os dados da vítima e exige um resgate, geralmente em criptomoedas, para restaurar o acesso. Para uma PME, um ataque de *ransomware* pode significar a paralisação completa das operações. Santos (2020, p. 78) afirma que "PMEs são especialmente suscetíveis a *ransomwares* devido à ausência de *backups* regulares e de planos de resposta a incidentes". A falta de uma cópia de segurança atualizada e testada deixa a empresa sem alternativas além de pagar o resgate — sem garantia de reaver os dados — ou perder permanentemente suas informações.

Além das ameaças diretas, as PMEs enfrentam um risco crescente como vetores em ataques à cadeia de suprimentos (*supply chain attacks*). Conforme antecipado na introdução, agentes maliciosos comprometem PMEs com controles de segurança mais fracos para, a partir delas, obter acesso a clientes e parceiros maiores (Souza, 2023). Essa tática é particularmente perigosa, pois a PME, sendo um fornecedor confiável, serve como um "cavalo de Troia" para contornar as defesas robustas das grandes corporações. A falta de verificação de segurança por parte de clientes maiores, que presumem a segurança de seus fornecedores menores, agrava essa vulnerabilidade (Silva; Martins, 2024).

### 1.2. Estratégias de Mitigação de Riscos Digitais

Contrariando a ideia de que a segurança cibernética é inacessível, PMEs podem adotar um conjunto de práticas de alto impacto e custo relativamente baixo. A abordagem deve ser multifacetada, combinando tecnologia, processos e pessoas.

A implementação de uma política de senhas fortes e a ativação da autenticação de múltiplos fatores (MFA) são medidas primordiais que aumentam drasticamente a dificuldade de acesso não autorizado a contas e sistemas (Cisco, 2024).

A prática de *backups* regulares é a defesa mais eficaz contra *ransomware* e perda de dados. Costa (2021, p. 134) enfatiza que "a realização regular e o teste de *backups* é uma das práticas mais eficientes no combate a ataques de *ransomware*". É crucial seguir a regra "3-2-1": ter pelo menos três cópias dos dados, em dois tipos de mídia diferentes, com uma cópia mantida offline ou em local externo.

ISSN: 2675-6218 - RECIMA21
Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



A capacitação contínua dos colaboradores é, talvez, o investimento com o maior retorno. Programas de conscientização que ensinam a identificar e-mails de *phishing*, a navegar com segurança na internet e a seguir as políticas de segurança da empresa são fundamentais. Almeida (2022, p. 67) argumenta que "a conscientização constante dos colaboradores é a principal linha de defesa contra-ataques que exploram falhas humanas". Simulações periódicas de ataques de *phishing* podem ajudar a reforçar o aprendizado e a manter a equipe alerta.

Tecnicamente, outras duas medidas de baixo custo e alto impacto são a adoção do Princípio do Menor Privilégio (PoLP) e a segmentação da rede. O PoLP determina que cada colaborador deve ter acesso apenas aos dados e sistemas estritamente necessários para executar sua função (Lopes, 2023). Isso limita o dano potencial de uma conta comprometida. Em conjunto, a segmentação da rede — como separar a rede Wi-Fi de visitantes da rede interna, ou isolar sistemas críticos (como o financeiro) do resto da operação — impede que um malware se espalhe lateralmente por toda a empresa (Whitman; Mattord, 2019). Essas são configurações que, embora técnicas, muitas vezes podem ser implementadas em equipamentos de rede já existentes na PME.

### 1.3. A Lei Geral de Proteção de Dados (LGPD) como Estrutura de Segurança

A LGPD (Lei nº 13.709/2018) estabeleceu um novo paradigma para o tratamento de dados pessoais no Brasil, impactando empresas de todos os portes. Embora a conformidade possa parecer um fardo para as PMEs, a lei pode ser encarada como um guia para a implementação de boas práticas de governança e segurança da informação.

A LGPD exige que as organizações adotem medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas (Brasil, 2018). Oliveira (2023, p. 112) pontua que "a adequação à LGPD exige a adoção de controles básicos de segurança, como o mapeamento de dados e o estabelecimento de políticas de acesso, o que contribui para a mitigação de riscos". O processo de adequação força a empresa a entender quais dados coleta, porque os coleta, onde os armazena e quem tem acesso a eles, promovendo uma organização interna que, por si só, já reduz vulnerabilidades.

Ademais, a conformidade com a LGPD tornou-se um fator de confiança e um diferencial competitivo. Ribeiro (2022, p. 91) reforça que "empresas que demonstram conformidade com a LGPD conquistam vantagem competitiva, pois transmitem maior segurança e confiabilidade no tratamento de dados sensíveis". Em um mercado onde a privacidade é cada vez mais valorizada, estar em conformidade sinaliza maturidade e respeito ao cliente.


Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



### 1.4. A Aceleração Digital Pós-Pandemia e a Educação como Vetor de Segurança

A pandemia de COVID-19 atuou como um catalisador para uma transformação digital sem precedentes, forçando PMEs a adotarem o trabalho remoto e a digitalizarem seus processos em um ritmo acelerado (Lima; Andrade, 2023). Essa transição abrupta, embora necessária para a sobrevivência dos negócios, expandiu drasticamente a superfície de ataque. O perímetro de segurança tradicional, antes confinado ao escritório, dissolveu-se, com colaboradores utilizando redes domésticas, muitas vezes inseguras, e dispositivos pessoais para acessar dados corporativos sensíveis.

Nesse novo cenário, a educação digital transcende o simples treinamento de conscientização. Não se trata mais apenas de ensinar a identificar um e-mail de *phishing*, mas de capacitar o colaborador com uma compreensão mais ampla sobre os riscos do ambiente digital descentralizado (Fernandes, 2024). Isso inclui boas práticas para a segurança de redes Wi-Fi domésticas, o uso de VPNs (Virtual Private Networks), a gestão de senhas em múltiplos dispositivos e a compreensão dos riscos associados ao uso de *softwares* não autorizados. A educação passa a ser um vetor estratégico para construir uma cultura de segurança resiliente e adaptada à nova realidade do trabalho híbrido (Lima; Andrade, 2023).

## 2. MÉTODOS

A presente pesquisa foi desenvolvida com base em uma abordagem qualitativa, de caráter exploratório e descritivo. O método de procedimento adotado foi a revisão bibliográfica e documental, que permite uma análise aprofundada do conhecimento já consolidado sobre o tema, oferecendo uma base sólida para a discussão e proposição de estratégias.

Para a coleta de dados, realizou-se um levantamento sistemático de produções científicas em bases de dados acadêmicas, como Scielo, Google Scholar e repositórios de universidades. Os descritores utilizados na busca foram: "segurança da informação", "cibersegurança", "pequenas e médias empresas", "ataques cibernéticos", "vulnerabilidades digitais", "LGPD", "pandemia", “trabalho remoto" e "educação digital".

Foram selecionados artigos, dissertações, livros e relatórios técnicos publicados preferencialmente entre 2020 e 2025, a fim de garantir a atualidade das informações e análises, dada a rápida evolução do campo da tecnologia e das ameaças cibernéticas.

A análise dos dados foi realizada de forma interpretativa, buscando identificar os principais desafios, as vulnerabilidades mais recorrentes e as estratégias de mitigação mais eficazes e acessíveis para as PMEs.


Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

## 3. RESULTADOS E DISCUSSÃO

A análise da literatura confirmou que as PMEs se encontram em uma posição de alta vulnerabilidade no ecossistema digital. Os resultados podem ser discutidos em torno de três eixos centrais: a predominância do fator humano nas brechas de segurança, a eficácia de medidas de segurança de baixo custo e o papel duplo da LGPD como desafio e oportunidade.

Primeiramente, evidencia-se que, embora as vulnerabilidades técnicas (como *softwares* desatualizados) sejam relevantes, a maior parte dos incidentes de segurança bem-sucedidos em PMEs se origina de falhas humanas. A pesquisa de Gomes e Barbosa (2023) corrobora este achado, indicando que mais de 80% dos ataques de *phishing* e *ransomware* em PMEs brasileiras em 2023 tiveram como vetor inicial a ação de um colaborador. Isso reforça a tese de Almeida (2022) sobre a necessidade de investir maciçamente em conscientização, pois a tecnologia, por si só, é insuficiente para conter ameaças que exploram a psicologia humana, como a curiosidade, o medo ou o senso de urgência. A discussão se aprofunda ao considerar que a falta de políticas formais de segurança (como uma política de uso aceitável de recursos de TI) deixa os colaboradores sem um guia claro sobre o que é um comportamento seguro, tornando a organização reativa em vez de proativa.

O cenário pós-pandemia intensificou a centralidade do fator humano na segurança cibernética. A migração massiva e apressada para o modelo de trabalho remoto expôs os colaboradores a um novo espectro de ameaças, fora do ambiente controlado da rede corporativa (Lima; Andrade, 2023). A discussão, portanto, avança da necessidade de "treinamentos" para a urgência de uma "educação digital" contínua. Enquanto treinamentos pontuais são eficazes contra ameaças conhecidas, como um *phishing* genérico, a educação digital prepara o funcionário para raciocinar sobre segurança em contextos variados e desconhecidos, transformando-o em um agente ativo na defesa da organização (Fernandes, 2024). A ausência dessa capacitação mais ampla tornou-se uma vulnerabilidade crítica, explorada por atacantes que adaptaram suas táticas para visar especificamente o ambiente doméstico.

Em segundo lugar, a pesquisa desmistifica a noção de que a segurança cibernética é proibitivamente cara. Medidas como a implementação de autenticação de múltiplos fatores (MFA), a política de privilégio mínimo (concedendo aos usuários apenas o acesso necessário para suas funções) e a realização de *backups* consistentes representam um custo marginal, mas oferecem uma camada de proteção robusta (Costa, 2021). A discussão aqui se volta para a barreira cultural e de conhecimento: muitos gestores de PMEs não implementam essas medidas não por falta de recursos, mas por desconhecimento de sua existência ou de sua importância. Conforme apontado por Nunes *et al.,* (2024), a disseminação de guias de boas práticas e a oferta de consultorias acessíveis são cruciais para transpor essa barreira.


Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



Essa "barreira cultural" merece destaque. A cultura organizacional de muitas PMEs é focada na operação e em vendas, relegando a segurança da informação a um segundo plano, vista como um "custo" operacional e não como um habilitador de negócios ou um diferencial estratégico (Amorim, 2022). O gestor, muitas vezes sobrecarregado com múltiplas funções, prioriza o faturamento imediato em detrimento da mitigação de um risco que parece abstrato ou improvável (Souza, 2023). Esta mentalidade reativa é o maior obstáculo para a implementação de medidas preventivas, mesmo as de baixo custo, pois a percepção de risco só se concretiza e ganha prioridade após a ocorrência do primeiro incidente severo, quando o dano financeiro ou reputacional já ocorreu.

Finalmente, a LGPD emergiu na análise como uma faca de dois gumes. Por um lado, representa um desafio de conformidade que exige investimento de tempo e, por vezes, de recursos. Por outro, atua como um poderoso catalisador para a maturidade em segurança da informação. A necessidade de mapear dados, definir bases legais, criar relatórios de impacto e nomear um Encarregado de Proteção de Dados (DPO) força as PMEs a adotarem uma postura de governança de dados que, por consequência, eleva seu nível de segurança (Oliveira, 2023). A discussão se enriquece com a perspectiva de Ribeiro (2022), que argumenta que PMEs que comunicam ativamente sua conformidade com a LGPD ganham a confiança de clientes e parceiros, transformando uma obrigação legal em um ativo de marketing e reputação.

## 4. CONSIDERAÇÕES

Este estudo demonstrou que os desafios enfrentados pelas pequenas e médias empresas na proteção de informações sensíveis são complexos, mas não intransponíveis. A pesquisa alcançou seus objetivos ao identificar que a vulnerabilidade das PMEs reside em uma combinação de recursos limitados, ausência de uma cultura de segurança e, principalmente, no despreparo do fator humano diante de ameaças cada vez mais sofisticadas, uma fragilidade exacerbada pela aceleração digital pós-pandemia.

A principal conclusão é que a segurança cibernética eficaz para PMEs não é uma questão de adquirir as tecnologias mais caras, mas de adotar uma abordagem estratégica e em camadas, que equilibre medidas técnicas acessíveis, processos bem definidos e, acima de tudo, a educação contínua dos colaboradores. A implementação de práticas fundamentais, como autenticação de múltiplos fatores, *backups* regulares e segmentação de rede, aliada a um programa robusto de conscientização, constitui a base para uma defesa resiliente.

A Lei Geral de Proteção de Dados, embora represente um desafio inicial, deve ser vista como uma aliada, fornecendo um roteiro para a implementação de uma governança de dados sólida que não apenas mitiga riscos, mas também gera valor e confiança no mercado. Como limitação do estudo, aponta-se o seu caráter teórico, baseado em revisão bibliográfica.

ISSN: 2675-6218 - RECIMA21
Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



Sugere-se, para futuras pesquisas, a realização de estudos de caso e pesquisas de campo em PMEs brasileiras para validar empiricamente as estratégias propostas e quantificar o impacto da adoção de medidas de segurança na redução de incidentes.

Em suma, a proteção de informações sensíveis deixou de ser uma opção e se tornou uma condição para a sobrevivência e prosperidade das PMEs na era digital. Investir em segurança da informação é investir na continuidade do próprio negócio.

## REFERÊNCIAS

ALMEIDA, D. S. A. **Conscientização e cultura organizacional em segurança da informação.** São Paulo: Atlas, 2022.

AMORIM, J. F. Desafios da cibersegurança em pequenas empresas brasileiras. **Revista de Tecnologia e Sociedade**, v. 18, n. 2, p. 40–55, 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 out. 2025.

CISCO. **Cybersecurity for Small & Medium Business for Dummies.** 2. ed. Hoboken, NJ: John Wiley & Sons, 2024.

COSTA, R. L. Estratégias acessíveis de proteção digital para PMEs. **Revista Gestão & Inovação**, v. 9, n. 3, p. 130–145, 2021.

FERNANDES, T. A nova fronteira da segurança: o fator humano no trabalho remoto. **Revista Brasileira de Segurança Digital**, v. 8, n. 1, p. 30–45, 2024.

GOMES, P. H.; BARBOSA, M. F. Cibersegurança e resiliência digital nas pequenas empresas. **Revista Brasileira de Tecnologia da Informação**, v. 5, n. 1, p. 15–30, 2023.

KASPERSKY. **Cybersecurity threats to SMBs:** 2023 Report. Moscou: Kaspersky Lab, 2023.

LIMA, M.; ANDRADE, C. **O Paradoxo Digital:** Cibersegurança em PMEs na Era Pós-Pandêmica. Rio de Janeiro: Editora FGV, 2023.

LOPES, F. G. **Controles Essenciais de Cibersegurança para Gestores.** Curitiba: Editora CRV, 2023.

NUNES, L. C. *et al.* Boas práticas em segurança cibernética para PMEs brasileiras. **Journal of Cyber Studies**, v. 3, n. 2, p. 22–39, 2024.

OLIVEIRA, F. R. Governança da informação e adequação à LGPD nas PMEs. **Revista de Direito Digital**, v. 7, n. 1, p. 110–125, 2023.

PEREIRA, A.; SILVA, E. Engenharia social e vulnerabilidades humanas em ambientes corporativos. **Revista Segurança Digital**, v. 4, n. 2, p. 100–115, 2021.

ISSN: 2675-6218 - RECIMA21

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



RIBEIRO, L. F. LGPD como vantagem competitiva para PMEs. **Revista Brasileira de Gestão da Informação**, v. 6, n. 3, p. 85–98, 2022.

SANTOS, M. A. Impactos do ransomware em pequenas empresas. **Caderno de Estudos em Tecnologia**, v. 12, n. 4, p. 75–90, 2020.

SILVA, B.; MARTINS, F. Vulnerabilidades de PMEs como Vetores de Invasão. **Journal of Information Security**, v. 10, n. 1, p. 45–59, 2024.

SOUZA, R. M. **Ataques à Cadeia de Suprimentos na Nova Economia Digital.** São Paulo: Editora Tech, 2023.

WHITMAN, M. E.; MATTORD, H. J. **Principles of Information Security.** 6. ed. Boston, MA: Cengage Learning, 2019. Disponível em: https://www.cengage.com/c/principles-of-informationsecurity-6e-whitman-mattord/9781337102063/. Acesso em: 04 out. 2025.


Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.