BOCA
BOLETIM DE CONJUNTURA

PROTEÇÃO CONTRA RANSOMWARE EM PEQUENAS E MÉDIAS EMPRESAS: UM GUIA DE PRÁTICAS PRIORIZADAS A PARTIR DE REFERENCIAIS PÚBLICOS E DE INCIDENTES BRASILEIROS

RANSOMWARE PROTECTION IN SMALL AND MEDIUM-SIZED ENTERPRISES: A GUIDE OF PRIORITIZED PRACTICES BASED ON PUBLIC FRAMEWORKS AND BRAZILIAN INCIDENTS

PROTECCIÓN CONTRA RANSOMWARE EN PEQUEÑAS Y MEDIANAS EMPRESAS: UNA GUÍA DE PRÁCTICAS PRIORIZADAS BASADA EN MARCOS DE REFERENCIA PÚBLICOS E INCIDENTES OCURRIDOS EN BRASIL

https://doi.org/10.56238/bocav25n84-008

Data de submissão: 06/10/2026 **Data de publicação:** 06/11/2026

David Lucas Silva Botao
Graduando em Sistemas de Informação
Instituição: Centro Universitário Santa Terezinha (CEST)
E-mail: david.botao@cest.edu.br

Carlos Wagner Sousa da Costa
Especialista em Computação Forense e Perícia Digital
Instituição: Centro Universitário Santa Terezinha (CEST)
E-mail: carlos.wagner@cest.edu.br

RESUMO

O *ransomware* é uma das ameaças cibernéticas de maior impacto para organizações de todos os portes, pois combina o sequestro de dados por criptografia com a extorsão baseada na ameaça de divulgação de informações. Pequenas e médias empresas (PMEs) são especialmente expostas por operarem sem equipes dedicadas à segurança e com orçamento restrito. Este artigo tem como objetivo propor um guia de práticas priorizadas de prevenção e resposta a *ransomware* aplicável a PMEs brasileiras. A pesquisa é aplicada, qualitativa, exploratória e descritiva, com procedimentos bibliográficos e documentais. O corpus reuniu cinco referenciais públicos (NIST *Cybersecurity Framework* 2.0, CIS Controls v8.1, *#StopRansomware Guide*, série *Ransomware* do CERT.br e guia da ANPD para agentes de pequeno porte), registros de incidentes ocorridos no Brasil entre 2020 e 2025 e estudos sobre detecção com inteligência artificial (IA). Os resultados indicam forte convergência entre os referenciais em torno de *backups* isolados e testados, autenticação multifator, atualizações, redução de serviços expostos e conscientização contra *phishing*. Os incidentes mostram que o *backup* íntegro foi determinante para a recuperação e que falhas de controle de acesso favoreceram os ataques. O estudo propõe um guia em três níveis de implantação e um roteiro de resposta e recuperação em oito passos, e discute o monitoramento ativo com IA, cujo potencial de detecção precoce é limitado por falsos positivos, técnicas de evasão e custo. Conclui-se que parcela relevante da proteção está ao alcance das PMEs por meio de medidas de baixo custo, embora o guia ainda careça de validação empírica.

Palavras-chave: Ransomware. Segurança da Informação. Pequenas e Médias Empresas. Gestão de Riscos Cibernéticos. Inteligência Artificial.

ABSTRACT
Ransomware is one of the most damaging cyber threats to organizations of all sizes, as it combines data hijacking through encryption with extortion based on the threat of leaking information. Small and medium-sized enterprises (SMEs) are particularly exposed because they often operate without dedicated security teams and with limited budgets. This article aims to propose a guide of prioritized ransomware prevention and response practices applicable to Brazilian SMEs. The research is applied, qualitative, exploratory and descriptive, with bibliographic and documentary procedures. The corpus comprised five free public frameworks (NIST Cybersecurity Framework 2.0, CIS Controls v8.1, #StopRansomware Guide, the CERT.br Ransomware series and the Brazilian Data Protection Authority guide for small processing agents), records of incidents that occurred in Brazil between 2020 and 2025 and studies on artificial intelligence (AI) based detection. The results indicate strong convergence among the frameworks around isolated and tested backups, multifactor authentication, updates, reduction of exposed services and phishing awareness. The incidents show that an intact backup was decisive for recovery and that access control failures favored the attacks. The study proposes a guide with three implementation levels and an eightstep response and recovery roadmap, and discusses active monitoring with AI, whose potential for early detection is limited by false positives, evasion techniques and cost. It is concluded that a relevant share of protection is within reach of SMEs through lowcost measures, although the guide still lacks empirical validation.

Keywords: Ransomware. Information Security. Small and Medium-Sized Enterprises. Cyber Risk Management. Artificial Intelligence.

RESUMEN
El ransomware es una de las amenazas cibernéticas de mayor impacto para organizaciones de todos los tamaños, ya que combina el secuestro de datos mediante cifrado con la extorsión basada en la amenaza de divulgar información. Las pequeñas y medianas empresas (pymes) están especialmente expuestas, debido a que operan sin equipos dedicados a la seguridad y cuentan con un presupuesto limitado. Este artículo tiene como objetivo proponer una guía de prácticas priorizadas para la prevención y respuesta ante el ransomware, aplicable a las pymes brasileñas. La investigación es de carácter aplicado, cualitativo, exploratorio y descriptivo, empleando procedimientos bibliográficos y documentales. El corpus analizado incluyó cinco marcos de referencia públicos (NIST Cybersecurity Framework 2.0, CIS Controls v8.1, la guía #StopRansomware, la serie sobre ransomware de CERT.br y la guía de la ANPD para entidades de menor tamaño), registros de incidentes ocurridos en Brasil entre 2020 y 2025, así como estudios sobre la detección mediante inteligencia artificial (IA). Los resultados indican una fuerte convergencia entre estos marcos de referencia en torno a aspectos clave: copias de seguridad (backups) aisladas y verificadas, autenticación multifactor, actualizaciones de sistemas, reducción de servicios expuestos y concienciación contra el *phishing*. Los incidentes demuestran que contar con una copia de seguridad íntegra fue determinante para la recuperación, mientras que las fallas en el control de acceso facilitaron los ataques. El estudio propone una guía estructurada en tres niveles de implementación, junto con una hoja de ruta de respuesta y recuperación de ocho pasos. Asimismo, se analiza el monitoreo activo mediante IA, cuyo potencial de detección temprana se ve limitado por la aparición de falsos positivos, el uso de técnicas de evasión y los costos

asociados. Se concluye que una parte significativa de la protección está al alcance de las pymes a través de medidas de bajo costo, si bien la guía aún requiere validación empírica.

Palabras clave: Ransomware. Seguridad de la Información. Pequeñas y Medianas Empresas. Gestión de Riesgos Cibernéticos. Inteligencia Artificial.

1 INTRODUÇÃO

O *ransomware* é um tipo de *software* malicioso que impede o acesso a dados ou sistemas, geralmente por meio de criptografia, e condiciona a restauração ao pagamento de um resgate. Em levantamento abrangente sobre o tema, Oz *et al.* (2022) o apontam como uma das ameaças mais notórias contra usuários, governos e empresas, com receitas milionárias para os criminosos e prejuízos que alcançam bilhões de dólares para as organizações atingidas.

No Brasil, o fenômeno ganhou visibilidade com incidentes em instituições públicas e grandes empresas. O ataque ao Superior Tribunal de Justiça (STJ), em novembro de 2020, foi descrito pela própria corte como o pior já empreendido contra uma instituição pública brasileira em dimensão e complexidade (Superior Tribunal de Justiça, 2020). Dados mais recentes indicam que a ameaça segue em expansão: o número de vítimas brasileiras reivindicadas publicamente por grupos de *ransomware* passou de 51 em 2023 para 135 em 2024 (Barbosa; Arruda, 2025).

As pequenas e médias empresas (PMEs) estão em situação mais frágil. Embora raramente apareçam no noticiário, elas tendem a operar com equipes reduzidas, sem profissionais dedicados à segurança e com políticas pouco maduras, condições que as tornam alvos recorrentes (Sá; Coelho, 2025). O ecossistema criminoso também inclui operadores menores, capazes de atingir qualquer negócio que apresente uma brecha de acesso (Barbosa; Arruda, 2025).

Existe, contudo, uma oferta ampla de orientações públicas e gratuitas sobre o tema, produzidas por instituições como o National Institute of Standards and Technology (NIST), o Center for Internet Security (CIS), a Cybersecurity and Infrastructure Security Agency (CISA), o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) e a Autoridade Nacional de Proteção de Dados (ANPD). Esses materiais, porém, têm escopos, linguagens e níveis de detalhamento distintos, e a maioria não foi escrita para o gestor de uma PME brasileira que precisa decidir por onde começar.

Diante disso, este trabalho parte da seguinte questão: quais práticas de segurança, ao alcance de pequenas e médias empresas, reduzem a probabilidade e o impacto de ataques de *ransomware*, considerando os referenciais públicos disponíveis e os incidentes registrados no Brasil entre 2020 e 2025?

O objetivo geral é propor um guia de práticas priorizadas de prevenção e resposta a *ransomware* aplicável a PMEs brasileiras. Para alcançá-lo, definem-se os seguintes objetivos específicos:

a) caracterizar o ransomware quanto ao funcionamento, aos vetores de acesso inicial e à evolução recente;
b) analisar incidentes ocorridos no Brasil e identificar falhas e fatores de recuperação recorrentes;
c) mapear as convergências entre as recomendações de cinco referenciais públicos de segurança;
d) organizar as práticas em níveis de prioridade compatíveis com as restrições de custo e de pessoal das PMEs;
e) propor um roteiro de resposta e recuperação e discutir o potencial e os limites do monitoramento ativo com inteligência artificial (IA) para PMEs.

A justificativa reside na distância entre a disponibilidade de orientações técnicas e sua aplicação por organizações de menor porte. Estudo brasileiro recente indica que as ameaças mais recorrentes às PMEs exploram principalmente o fator humano e que a mitigação depende de cultura de segurança, políticas claras e adequação à Lei Geral de Proteção de Dados Pessoais (Santos; Silva; Pinto, 2025). Consolidar essas orientações em um roteiro único, gratuito e priorizado pode reduzir a barreira de entrada para empresas que hoje não sabem por onde começar.

Quanto às características, a pesquisa é de natureza aplicada e abordagem qualitativa; exploratória e descritiva quanto aos objetivos; e bibliográfica e documental quanto aos procedimentos técnicos, segundo a classificação de Prodanov e Freitas (2013). O corpus foi composto exclusivamente por documentos de acesso gratuito, o que permite a qualquer leitor verificar as fontes e reproduzir a análise.

O artigo está organizado em cinco seções. Após esta introdução, a seção 2 apresenta o desenvolvimento teórico sobre *ransomware*, PMEs e referenciais de segurança; a seção 3 descreve os procedimentos metodológicos; a seção 4 discute os resultados e apresenta o guia proposto, o roteiro de resposta e recuperação e a análise do monitoramento com IA; e a seção 5 reúne as considerações finais.

2 DESENVOLVIMENTO TEÓRICO

2.1 RANSOMWARE: CONCEITO E EVOLUÇÃO

Oz *et al.* (2022) observam que o *ransomware*, antes concentrado em computadores pessoais e estações de trabalho, passou a atingir também dispositivos móveis e sistemas de Internet das Coisas e ciberfísicos, o que aumentou a superfície de exposição das organizações. O modelo de negócio, contudo, permaneceu o mesmo: tornar dados ou sistemas indisponíveis e cobrar pela restauração.

A trajetória recente da ameaça pode ser dividida em duas fases. A primeira foi marcada por campanhas massivas e indiscriminadas, cujo exemplo mais conhecido é o WannaCry, que em 2017 comprometeu dispositivos em mais de 150 países, incluindo o Brasil, e se propagava automaticamente entre sistemas vulneráveis (Barbosa; Arruda, 2025). A segunda fase corresponde à migração para ataques direcionados, precedidos de reconhecimento do ambiente da vítima e voltados a organizações com capacidade de pagamento.

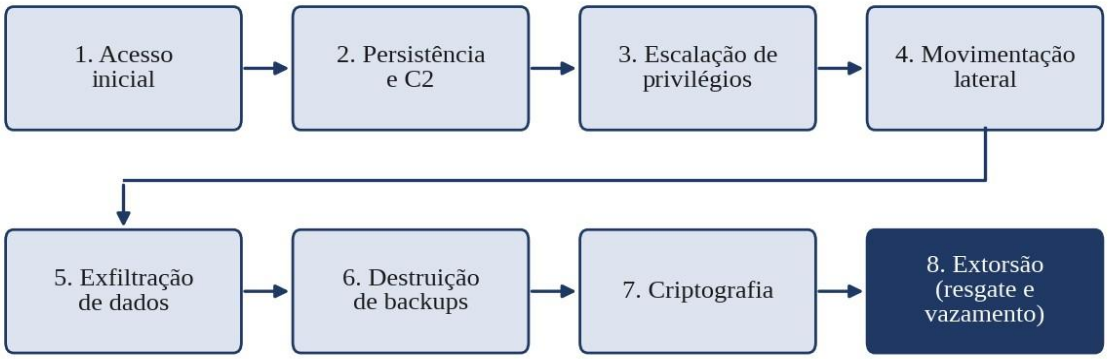
Dois elementos caracterizam essa segunda fase. O primeiro é o modelo *Ransomware-as-a-Service* (RaaS), no qual desenvolvedores fornecem o *malware* e a infraestrutura a afiliados que executam os ataques, o que permite a agentes com pouco conhecimento técnico conduzir operações complexas (Barbosa; Arruda, 2025). O segundo é a dupla extorsão: além de criptografar os dados, os criminosos os copiam e ameaçam publicá-los caso o resgate não seja pago.

A dupla extorsão altera a lógica da defesa. Sá e Coelho (2025) argumentam que ela surgiu como resposta à adoção de *backups* robustos pelas organizações: quando a vítima consegue restaurar seus dados sem pagar, a ameaça de vazamento passa a ser o principal instrumento de pressão. O *backup* continua indispensável para a recuperação, mas deixa de ser suficiente como estratégia única de proteção.

2.2 CICLO DO ATAQUE E VETORES DE ACESSO INICIAL

Ataques direcionados não se resumem ao momento da criptografia. O CERT.br descreve o ataque como uma sequência de fases que vai do acesso inicial ao impacto final, passando por persistência e comunicação com servidores de comando e controle (C2), escalação de privilégios, movimentação lateral, exfiltração de dados e destruição de *backups* (NIC.br, 2025; CERT.br, 2025a). A Figura 1 sintetiza essa sequência.

Figura 1. Fases de um ataque de *ransomware* direcionado



Fonte: elaborado pelo autor (2026), com base em CERT.br (2025a; 2025b) e NIC.br (2025).

A visão em fases tem consequência prática: cada etapa oferece uma oportunidade distinta de detecção e interrupção, e quanto mais cedo a detecção ocorre, menores são os impactos e o esforço de resposta (CERT.br, 2025a). Uma empresa que só percebe o ataque quando os arquivos já estão criptografados, na fase 7 da Figura 1, desperdiçou todas as oportunidades anteriores.

Quanto ao acesso inicial, a literatura converge em um conjunto pequeno de vetores. Sá e Coelho (2025) destacam o *phishing*, a exploração de serviços de acesso remoto (Remote Desktop Protocol, RDP) mal protegidos, as vulnerabilidades não corrigidas e o uso de credenciais comprometidas. O levantamento da ESET sobre o Brasil registra padrões semelhantes: o Phobos costuma entrar por *phishing* e por força bruta contra RDP exposto, enquanto o grupo Akira obtém acesso por meio de rede privada virtual (VPN) sem autenticação multifator (MFA) (Barbosa; Arruda, 2025).

Os *backups* ocupam lugar particular nesse ciclo. O CERT.br (2025b) observa que eles são duplamente visados, como fonte de dados a exfiltrar e como alvo de destruição, justamente para impedir que a empresa se recupere sem pagar. Isso explica por que as recomendações dos referenciais enfatizam cópias *offline* e protegidas contra modificação.

2.3 PEQUENAS E MÉDIAS EMPRESAS COMO ALVO

O porte da empresa não a torna irrelevante para os criminosos. Embora os grandes grupos tendam a mirar organizações médias e grandes, o ecossistema inclui agentes menores e campanhas massivas distribuídas por *e-mails* de *phishing*, downloads de *software* pirata e anúncios fraudulentos, que atingem empresas de qualquer tamanho (Barbosa; Arruda, 2025). Segundo o mesmo levantamento, cerca de 29% das empresas brasileiras relataram ter sofrido um ataque de *ransomware* em 2024.

As limitações estruturais das PMEs agravam essa exposição. Santos, Silva e Pinto (2025) apontam a restrição de recursos, a ausência de políticas de segurança estruturadas e a baixa conscientização dos colaboradores, agravada pelo trabalho remoto, como fatores centrais de vulnerabilidade. Sá e Coelho (2025) acrescentam a carência de equipes dedicadas e de processos maduros de gestão da segurança.

Há também evidência experimental de que configurações padrão oferecem proteção insuficiente. Em testes com um simulador não destrutivo, Sá e Coelho (2025) observaram que entre 81,5% e 85,2% dos cenários de *ransomware* simulados tiveram êxito em estações Windows com as configurações de fábrica do antivírus nativo, índice ainda maior no Windows 7, sistema sem suporte do fabricante. Os próprios autores ressaltam o caráter exploratório dos testes, mas o resultado indica que confiar apenas nas proteções padrão é arriscado.

A dimensão regulatória completa o quadro. Quando o incidente envolve dados pessoais, a Lei nº 13.709/2018 obriga o controlador a comunicar à ANPD e aos titulares a ocorrência que possa acarretar risco ou dano relevante (Brasil, 2018). Para uma PME, um ataque com exfiltração de dados pode gerar, além da paralisação, obrigações legais e danos à reputação.

2.4 REFERENCIAIS PÚBLICOS DE SEGURANÇA

Entre os referenciais gratuitos, o NIST *Cybersecurity Framework* (CSF) 2.0 é o mais abrangente. Publicado em fevereiro de 2024, ele organiza os resultados de segurança em seis funções, Governar, Identificar, Proteger, Detectar, Responder e Recuperar, e declara-se aplicável a organizações de qualquer porte, setor ou maturidade (NIST, 2024). O framework não prescreve como cada resultado deve ser alcançado; em vez disso, remete a recursos complementares, como guias de início rápido.

Os CIS *Critical Security Controls* v8.1 seguem lógica mais operacional. O conjunto reúne 153 salvaguardas distribuídas em três grupos de implementação (IG1, IG2 e IG3). O IG1, definido como higiene cibernética essencial, reúne 56 salvaguardas e foi pensado para organizações tipicamente pequenas ou médias, com pouca especialização em tecnologia da informação e baixa tolerância à interrupção das operações (Center for Internet Security, 2024).

O *#StopRansomware Guide*, publicado conjuntamente pela CISA, pelo Federal Bureau of Investigation (FBI), pela National Security Agency (NSA) e pelo Multi-State Information Sharing and Analysis Center (MS-ISAC), é dedicado exclusivamente ao *ransomware*. Sua primeira parte reúne boas práticas de prevenção agrupadas pelos vetores de acesso inicial mais comuns; a segunda traz uma

lista de verificação para resposta a incidentes. A atualização de 2023 incluiu recomendações sobre credenciais comprometidas, engenharia social, *backups* em nuvem e arquitetura de confiança zero (CISA, 2023).

No Brasil, o CERT.br lançou em julho de 2025 a série *Ransomware*, dividida em quatro partes: Como Acontece, Como se Proteger, Como Detectar e Como Responder (NIC.br, 2025). A parte de proteção enfatiza autenticação multifator, *backups*, gestão de vulnerabilidades, conscientização e segregação de redes, enquanto a parte de resposta propõe um plano de oito passos para conter o ataque, eliminar a ameaça e restaurar a operação.

Por fim, a ANPD publicou em 2021 um guia orientativo de segurança da informação para agentes de tratamento de pequeno porte, categoria que inclui microempresas, empresas de pequeno porte e *startups*. O documento propõe medidas administrativas, como política de segurança, conscientização e gestão de contratos, e medidas técnicas, como controle de acesso e segurança dos dados armazenados e das comunicações, acompanhadas de uma lista de verificação (Brasil, 2021). Embora não tenha efeito vinculante, é o único dos cinco referenciais escrito especificamente para organizações de pequeno porte no Brasil.

3 PROCEDIMENTOS METODOLÓGICOS

3.1 CARACTERIZAÇÃO DA PESQUISA

Esta pesquisa é de natureza aplicada, pois busca gerar conhecimento voltado à solução de um problema prático, e adota abordagem qualitativa, uma vez que interpreta documentos e casos sem recorrer a tratamento estatístico (Prodanov; Freitas, 2013). Quanto aos objetivos, é exploratória, por organizar um tema ainda pouco sistematizado para o público de PMEs, e descritiva, por caracterizar incidentes e recomendações.

Quanto aos procedimentos técnicos, trata-se de pesquisa bibliográfica e documental. A parte bibliográfica apoia-se em material já publicado, como artigos científicos; a documental recorre a materiais que ainda não receberam tratamento analítico, como comunicados oficiais, fatos relevantes e notícias sobre incidentes (Prodanov; Freitas, 2013).

3.2 CORPUS E CRITÉRIOS DE SELEÇÃO

O corpus foi formado em três frentes. A primeira reuniu referenciais de segurança que atendessem simultaneamente a três critérios: acesso gratuito, publicação ou atualização a partir de 2021

e emissão por instituição pública ou organização reconhecida na área. A segunda reuniu registros de incidentes de *ransomware* ou de extorsão de dados ocorridos no Brasil entre 2020 e 2025, documentados por fonte oficial ou por veículo de imprensa identificável. A terceira, utilizada na discussão sobre monitoramento ativo, reuniu trabalhos científicos de acesso aberto sobre detecção de *ransomware* com IA. O Quadro 1 apresenta os documentos selecionados.

Quadro 1. Composição do corpus da pesquisa

Frente	Documento	Emissor ou fonte	Ano
Referenciais	NIST *Cybersecurity Framework* 2.0	NIST (EUA)	2024
Referenciais	CIS *Critical Security Controls* v8.1 (grupo IG1)	Center for Internet Security	2024
Referenciais	*#StopRansomware Guide*	CISA, FBI, NSA e MS-ISAC	2023
Referenciais	Série *Ransomware* (Como se Proteger, Como Detectar, Como Responder)	CERT.br/NIC.br	2025
Frente	**Documento**	**Emissor ou fonte**	**Ano**
Referenciais	Guia orientativo de segurança da informação para agentes de tratamento de pequeno porte	ANPD	2021
Incidentes	Superior Tribunal de Justiça	Comunicados do STJ e do CJF	2020
Incidentes	Grupo Fleury	Fato relevante e imprensa	2021
Incidentes	Ministério da Saúde (ConecteSUS)	Agência Brasil e imprensa	2021
Incidentes	Panorama brasileiro de vítimas	ESET e Assespro	2024 2025
Detecção com IA	Avaliação de algoritmos de aprendizado de máquina	Bold, Al-Khateeb e Ersotelos	2022
Detecção com IA	Revisão sobre detecção de *ransomware* com IA	Ferdous *et al.*	2024
Detecção com IA	Revisão sistemática de revisões sobre *ransomware* e IA	Daengsi *et al.* (*preprint*)	2026

Fonte: elaborado pelo autor (2026).

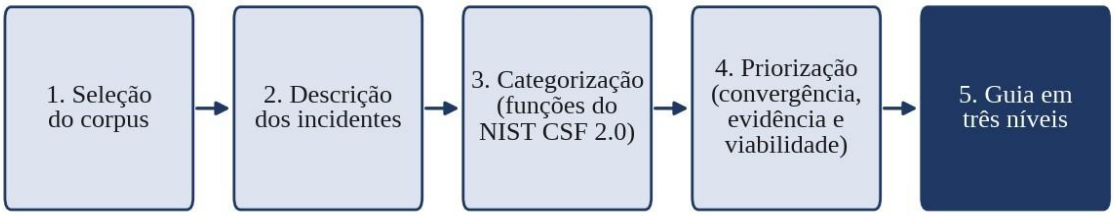
Materiais de fornecedores de produtos de segurança foram admitidos apenas como fonte de dados de panorama, e não como fonte de recomendações. O critério de acesso gratuito foi adotado deliberadamente: um guia destinado a PMEs deve apoiar-se em fontes que o próprio gestor possa consultar sem custo.

3.3 PROCEDIMENTO DE ANÁLISE

A análise ocorreu em etapas sucessivas, representadas na Figura 2. Após a seleção do corpus, cada incidente foi descrito quanto ao vetor de entrada, quando divulgado, ao impacto, ao tempo de recuperação e ao fator determinante para a restauração. Em seguida, as recomendações dos cinco

referenciais foram categorizadas segundo as funções do NIST CSF 2.0, adotadas como categorias prévias por serem neutras em relação a setor e porte.

Figura 2. Etapas do procedimento de análise



Fonte: elaborado pelo autor (2026).

Na etapa de priorização, cada prática recebeu um nível com base em três critérios: (a) convergência, entendida como presença explícita em pelo menos três dos cinco referenciais; (b) evidência, isto é, relação direta com falhas ou fatores de recuperação observados nos incidentes; e (c) viabilidade para PMEs, estimada pela inclusão no grupo IG1 dos CIS Controls ou pela presença no guia da ANPD para agentes de pequeno porte.

Por não envolver coleta de dados com pessoas, a pesquisa dispensou apreciação por comitê de ética. Todos os incidentes analisados foram tornados públicos pelas próprias organizações ou pela imprensa.

4 ANÁLISE E DISCUSSÃO

4.1 O QUE OS INCIDENTES BRASILEIROS REVELAM

O Quadro 2 sintetiza os incidentes analisados. Apesar da diferença de porte entre as organizações atingidas e as PMEs, os casos permitem extrair lições transferíveis, sobretudo quanto ao papel do *backup*, do controle de acesso e da contenção inicial.

Quadro 2. Síntese dos incidentes analisados

Organização (ano)	O que ocorreu	Fator determinante observado	Fontes
STJ (2020)	Ataque detectado durante sessões de julgamento; desconexão dos *links* de internet; sistemas e telefonia indisponíveis; dados criptografados.	Dados preservados no *backup* permitiram concluir o restabelecimento em cerca de duas semanas.	Conselho da Justiça Federal (2020); Superior Tribunal de Justiça (2020)
Grupo Fleury (2021)	Indisponibilidade de parte dos sistemas; atendimento mantido por soluções de contingência.	Relato de movimentação lateral a partir de contas comuns até contas de administrador.	Fleury é alvo... (2021); Ataque no Grupo Fleury... (2021)
Ministério da Saúde (2021)	ConecteSUS, e-SUS Notifica e SI-PNI fora do ar; invasores alegaram ter copiado e excluído dados.	Extorsão baseada em dados; aplicativo restabelecido após 13 dias.	Ataque hacker... (2021); Aplicativo... (2021)
Grupo Jorge Batista (2025)	Sistemas paralisados, vendas interrompidas e rompimento de contratos.	Perdas estimadas em R$ 400 milhões.	Barbosa e Arruda (2025)

Fonte: elaborado pelo autor (2026).

O caso do STJ é o exemplo mais claro do papel do *backup*. O tribunal informou que o ataque bloqueou o acesso aos dados por meio de criptografia, mas que eles estavam preservados em seus sistemas de *backup* (Conselho da Justiça Federal, 2020). Em 19 de novembro de 2020, a presidência anunciou a conclusão do restabelecimento dos sistemas, com apoio de cerca de cem profissionais (Superior Tribunal de Justiça, 2020).

O episódio também ilustra a importância da contenção imediata. Ao perceber a circulação do vírus, o tribunal desconectou seus *links* com a internet como medida de precaução (Conselho da Justiça Federal, 2020), conduta alinhada à orientação do CERT.br (2025c) de, como primeiro passo da resposta, isolar os sistemas afetados e proteger os ainda íntegros, em especial os *backups*.

O caso do Grupo Fleury mostra o outro lado do problema. A empresa comunicou ao mercado a indisponibilidade de parte de seus sistemas e a adoção de soluções de contingência para manter o atendimento (Fleury é alvo..., 2021). Segundo apuração do jornal Valor Econômico reproduzida pela imprensa especializada, os invasores exploraram falhas em contas de usuários comuns até alcançar contas com privilégio de administrador (Ataque no Grupo Fleury..., 2021).

A empresa registrou R$ 29,4 milhões em despesas não recorrentes no segundo trimestre de 2021, rubrica em que se contabilizam custos dessa natureza, e voltou a sofrer um ataque cibernético em 2023 (Fleury sofre..., 2023). Ainda que os detalhes técnicos não tenham sido integralmente

divulgados, o relato aponta para falhas na gestão de privilégios, justamente o tipo de controle que dificulta a movimentação lateral.

O ataque ao Ministério da Saúde, reivindicado pelo grupo Lapsus$, tem natureza distinta: a mensagem deixada pelos invasores alegava que os dados haviam sido copiados e excluídos (Ataque hacker..., 2021). O aplicativo ConecteSUS permaneceu fora do ar de 10 a 23 de dezembro de 2021, e o ataque afetou também sistemas de notificação e de imunização (Aplicativo..., 2021). O caso mostra que a extorsão baseada em dados nem sempre depende de criptografia, o que reforça a necessidade de controlar acessos e monitorar a saída de dados.

O panorama de 2024 e 2025 confirma que o problema não se restringe a grandes organizações. A relação de vítimas reivindicadas por grupos criminosos em meados de 2024 inclui, ao lado de empresas conhecidas como Braspress e Vivara, uma prefeitura e diversas organizações de pouca projeção pública, de setores variados (Assespro, 2024). Em 2025, o ataque ao Grupo Jorge Batista, do setor farmacêutico, paralisou sistemas e interrompeu vendas, com perdas estimadas em R$ 400 milhões (Barbosa; Arruda, 2025).

Três lições emergem dos casos. Primeiro, o *backup* íntegro e protegido foi o que permitiu ao STJ restabelecer suas operações sem depender dos criminosos. Segundo, a progressão dos ataques esteve associada a falhas de controle de acesso, seja pela escalada a partir de contas comuns, seja pelo acesso remoto sem autenticação multifator, padrão atribuído ao grupo Akira (Barbosa; Arruda, 2025). Terceiro, a contenção rápida e os planos de contingência reduziram o impacto sobre o atendimento, mesmo com sistemas indisponíveis.

4.2 CONVERGÊNCIA ENTRE OS REFERENCIAIS

A categorização das recomendações pelas funções do NIST CSF 2.0 revelou um núcleo comum de práticas. O Quadro 3 apresenta as dez práticas mais recorrentes e indica em quais referenciais cada uma aparece de forma explícita (Sim) ou apenas indireta (Parcial). O NIST CSF 2.0 não consta como coluna porque, por não prescrever controles, foi utilizado como eixo de categorização.

Quadro 3. Presença das práticas nos referenciais analisados

Prática	Função NIST CSF 2.0	CISA (2023)	CIS IG1 (2024)	CERT.br (2025)	ANPD (2021)
1. *Backups* regulares, isolados e testados	Recuperar	Sim	Sim	Sim	
2. Autenticação multifator (MFA)	Proteger	Sim	Sim	Sim	Parcial
3. Atualização de sistemas e gestão de vulnerabilidades	Identificar / Proteger	Sim	Sim	Sim	
4. Redução de serviços expostos à internet (RDP, VPN, portas)	Proteger	Sim	Sim	Sim	
5. Conscientização contra *phishing* e engenharia social	Proteger	Sim	Sim	Sim	Sim
6. Privilégio mínimo e contas administrativas separadas	Proteger	Sim	Sim	Parcial	Sim
7. Proteção contra *malware* em estações e servidores	Proteger / Detectar	Sim	Sim	Sim	Parcial
8. Registro e monitoramento de *logs*	Detectar	Sim	Sim	Sim	
9. Plano de resposta e canal de notificação de incidentes	Responder	Sim	Sim	Sim	
10. Segmentação de rede	Proteger	Sim	(IG2)	Sim	

Legenda: Sim = recomendação explícita; Parcial = abordagem indireta ou genérica; = não identificada no documento.
Fonte: elaborado pelo autor (2026), com base em CISA (2023), Center for Internet Security (2024), CERT.br (2025a; 2025b; 2025c) e Brasil (2021).

O resultado mais evidente é que nove das dez práticas aparecem explicitamente em pelo menos três referenciais, o que indica consenso técnico sobre o núcleo da proteção. A segmentação de rede é a exceção: embora recomendada pela CISA e pelo CERT.br, ela não integra o grupo IG1 dos CIS Controls, o que sugere que sua implantação exige maturidade e recursos acima do mínimo esperado de uma PME.

O guia da ANPD apresenta menor cobertura técnica, o que é coerente com seu propósito, voltado à proteção de dados pessoais de modo geral, e não ao *ransomware*. Em contrapartida, trata diretamente de política de segurança e de gestão de contratos com terceiros e oferece uma lista de verificação em português pensada para pequenos negócios (Brasil, 2021), o que o torna um bom ponto de partida para a dimensão administrativa.

Observa-se ainda uma diferença de ênfase entre as funções. A CISA e o CERT.br dão mais espaço à resposta, com listas de verificação e planos de ação, enquanto os CIS Controls concentram-se na prevenção. Essa complementaridade justifica a combinação dos referenciais, pois nenhum deles, isoladamente, cobre com o mesmo detalhe a preparação, a detecção e a recuperação.

Os achados dialogam com a literatura nacional. As recomendações de Sá e Coelho (2025), que priorizam autenticação multifator, *backup* com cópia *offline* e atualização de sistemas como controles de custo reduzido, coincidem com as práticas de maior convergência. Da mesma forma, a ênfase de Santos, Silva e Pinto (2025) no fator humano encontra correspondência no fato de a conscientização contra *phishing* ser a única prática recomendada explicitamente pelos quatro referenciais comparados.

4.3 GUIA DE PRÁTICAS PRIORIZADAS PARA PMEs

A aplicação dos três critérios de priorização resultou no guia apresentado

no Quadro 4. O Nível 1 reúne práticas de alta convergência, relacionadas às falhas observadas nos incidentes e viáveis com recursos que a maioria das PMEs já possui. Os Níveis 2 e 3 acrescentam capacidades de detecção, resposta e contenção que exigem maior investimento ou conhecimento técnico.

Quadro 4. Guia de práticas priorizadas contra *ransomware* para PMEs

Prática	**Como aplicar em uma PME**
Nível 1 – Essencial (implantação imediata, até 3 meses)	
Backups isolados e testados	Manter cópias periódicas dos dados críticos, com pelo menos uma cópia *offline* ou inacessível a partir da rede principal; testar a restauração regularmente.
Autenticação multifator	Ativar em *e-mail*, VPN, acesso remoto, serviços em nuvem e contas administrativas, preferindo métodos resistentes a *phishing*.
Atualizações	Ativar atualizações automáticas e substituir sistemas operacionais sem suporte do fabricante.
Redução de serviços expostos	Retirar RDP e demais serviços desnecessários da internet; restringir o acesso remoto a VPN com autenticação multifator.
Conscientização e notificação	Treinar periodicamente os colaboradores sobre *phishing* e definir um canal para relatar mensagens e comportamentos suspeitos.
Controle de privilégios	Separar contas administrativas das contas de uso diário e conceder apenas os privilégios necessários a cada função.
Nível 2 – Estruturação (3 a 12 meses)	
Prática	**Como aplicar em uma PME**
Inventário de ativos	Registrar equipamentos, sistemas e dados críticos, definindo o que deve ser protegido e restaurado primeiro.
Proteção de estações e servidores	Manter solução antimalware ativa e atualizada em todos os equipamentos; avaliar serviço gerenciado de detecção e resposta.
Registro de *logs*	Habilitar *logs* em servidores, *firewall* e serviços em nuvem, centralizálos e manter os relógios sincronizados.
Plano de resposta	Documentar responsáveis, contatos, passos de contenção e critérios de comunicação à ANPD e aos titulares quando houver dados pessoais.
Nível 3 – Maturidade (acima de 12 meses)	
Segmentação de rede	Separar servidores, *backups* e estações; isolar equipamentos de visitantes e pessoais.

Exercícios e revisão	Simular incidentes e restaurações completas; revisar o plano de resposta após cada exercício.
Gestão de terceiros	Incluir cláusulas de segurança nos contratos com fornecedores de tecnologia.
Evolução do programa	Elaborar um perfil organizacional com base no NIST CSF 2.0 e avançar para as salvaguardas do grupo IG2 dos CIS Controls.

Fonte: elaborado pelo autor (2026), com base em CISA (2023), Center for Internet Security (2024), CERT.br (2025a; 2025b; 2025c), Brasil (2021) e NIST (2024).

A escolha do *backup* como primeira prática decorre tanto da evidência dos casos quanto da dinâmica do ataque. Como as cópias de segurança são alvos deliberados dos criminosos, o CERT.br (2025b) recomenda mantê-las *offline*, protegidas contra modificações não autorizadas e testadas regularmente, e ressalta que, quando o ataque chega à criptografia, elas podem ser a única alternativa de recuperação do negócio. Uma cópia nunca testada, portanto, não deve ser considerada proteção.

A autenticação multifator aparece em seguida porque atua sobre dois momentos do ataque: impede o acesso inicial com credenciais comprometidas e dificulta a movimentação lateral (CERT.br, 2025b). O padrão atribuído ao grupo Akira, que ingressa por VPN sem MFA (Barbosa; Arruda, 2025), e o relato de escalada de privilégios no caso Fleury ilustram o custo de sua ausência. O CERT.br alerta ainda que VPNs baseadas em navegador podem permitir o sequestro de sessão e o contorno do MFA, o que recomenda cautela na escolha da solução.

As práticas do Nível 2 exigem mais do que configuração. O inventário de ativos é pré-requisito para decidir o que proteger e restaurar primeiro; os *logs* só têm valor se alguém os analisar; e o plano de resposta precisa de responsáveis definidos. Para PMEs sem equipe técnica, a contratação de serviços gerenciados tende a ser o caminho mais realista, alternativa também apontada por Sá e Coelho (2025).

O plano de resposta, por sua vez, só tem utilidade se descrever o que fazer quando a prevenção falhar. Por isso, a seção 4.4 detalha um roteiro de resposta e recuperação que complementa o guia, e a seção 4.5 discute como o monitoramento ativo pode antecipar a detecção do ataque.

4.4 ROTEIRO DE RESPOSTA E RECUPERAÇÃO

O guia do Quadro 4 concentra-se na prevenção, mas os casos analisados na seção 4.1 mostram que a capacidade de recuperação depende igualmente do que a empresa faz nas primeiras horas após a detecção. Para orientar essa etapa, o CERT.br (2025c) organiza a resposta a ataques de *ransomware* em oito passos, que podem ser executados simultaneamente, em outra ordem ou apenas em parte, conforme o ambiente e o tipo de *ransomware*. O Quadro 5 adapta esses passos à realidade de uma PME.

Quadro 5. Roteiro de resposta e recuperação a *ransomware* para PMEs

Passo	O que fazer	Ponto de atenção em uma PME
1. Acionar o plano de resposta	Comunicar os responsáveis definidos no plano e registrar as ações tomadas e as informações coletadas.	Manter atualizada a lista de quem pode decidir desligar sistemas e de quais fornecedores, assessoria jurídica e seguradora acionar.
2. Conter o ataque	Proteger os sistemas ainda íntegros, em especial os *backups*; desconectar da rede os equipamentos comprometidos e bloquear conexões maliciosas.	Desconectar o cabo de rede e o WiFi do equipamento afetado é a medida de contenção mais simples e pode ser executada por qualquer colaborador treinado.
3. Identificar o *ransomware*	Usar a nota de resgate e a extensão dos arquivos para identificar a variante e verificar se há decifradores disponíveis.	Projetos gratuitos, como o No More Ransom, auxiliam nessa verificação.
4. Analisar as informações	Determinar o ponto de entrada, os sistemas atingidos, os dados exfiltrados e a causa raiz do comprometimento.	Havendo exfiltração de dados pessoais com risco relevante aos titulares, comunicar a ANPD e os titulares.
5. Eliminar o *ransomware*	Reinstalar do zero os sistemas afetados, com mídias e fontes confiáveis, atualizálos e corrigir a falha usada na invasão.	Só remover o *malware* é insuficiente: o atacante pode ter deixado alterações e formas de retorno ao ambiente.
6. Trocar senhas e revisar acessos	Trocar as senhas de todas as contas, remover privilégios e contas criadas pelo atacante e reativar a autenticação multifator.	Priorizar contas administrativas e de serviços em nuvem.
7. Restaurar dados e conectividade	Recuperar os dados a partir de *backups* confiáveis, de preferência *offline*, e só então reconectar os equipamentos à rede.	Verificar se os dados restaurados não contêm cópias do *malware*, para evitar reinfecção.
8. Aplicar as lições aprendidas	Registrar o incidente em relatório, atualizar o plano de resposta e reforçar a monitoração e as medidas preventivas.	Revisar o Quadro 4 para identificar qual prática teria evitado ou reduzido o incidente.

Fonte: elaborado pelo autor (2026), com base em CERT.br (2025c) e Brasil (2018).

Dois pontos do roteiro merecem destaque. O primeiro é que a contenção, embora indispensável, pode ser percebida pelo atacante e levá-lo a disparar rotinas preparadas para apagar arquivos ou apressar a criptografia (CERT.br, 2025c). Isso reforça a necessidade de que papéis e decisões estejam definidos antes do incidente, e não improvisados durante ele, como previsto no plano de resposta do Nível 2 do Quadro 4.

O segundo é a ordem entre eliminação e restauração. Restaurar os dados antes de reinstalar os sistemas e trocar as credenciais expõe a empresa à reinfecção, pois o atacante pode manter acesso por contas ou mecanismos de persistência não removidos (CERT.br, 2025c). O caso do STJ ilustra a sequência adequada: a desconexão imediata dos *links* de internet conteve o avanço do ataque, e a

restauração a partir de *backups* preservados permitiu retomar as operações (Conselho da Justiça Federal, 2020; Superior Tribunal de Justiça, 2020).

Quanto ao pagamento do resgate, o CERT.br (2025c) adverte que pagar não afasta o risco de nova extorsão, não assegura que os dados serão devolvidos ou mantidos em sigilo e ainda pode financiar a atividade criminosa. A decisão envolve aspectos jurídicos e de negócio e deve estar prevista no plano de resposta, mas o roteiro proposto busca justamente que a empresa consiga se recuperar sem depender dessa alternativa.

4.5 MONITORAMENTO ATIVO E USO DE INTELIGÊNCIA ARTIFICIAL NA DETECÇÃO

A detecção precoce é o elo entre a prevenção e a resposta. No NIST CSF 2.0, ela corresponde à função Detectar, que reúne o monitoramento contínuo dos ativos e a análise de eventos adversos (NIST, 2024), e o CERT.br (2025a) recomenda acompanhar os alertas das ferramentas de proteção e os sinais de atividade suspeita para responder o mais rápido possível. A dificuldade é que os métodos convencionais de detecção perdem eficácia à medida que os ataques se tornam mais sofisticados, o que tem motivado o uso de técnicas de IA nessa função (Ferdous *et al.*, 2024).

Os modelos de aprendizado de máquina aplicados ao *ransomware* combinam, em geral, dois tipos de análise. A análise estática examina o arquivo sem executá-lo, enquanto a análise dinâmica observa o comportamento do programa em execução, como chamadas de sistema, alterações em arquivos e no registro do sistema e comunicações de rede. Segundo a revisão de Daengsi *et al.* (2026), abordagens híbridas, que reúnem as duas, têm apresentado os melhores resultados, e a detecção comportamental busca identificar o ataque antes que a criptografia se complete, a partir de sinais como a troca acelerada de extensões de arquivos, a modificação de grande volume de arquivos em pouco tempo e o aumento da entropia dos dados gravados.

A avaliação desses modelos exige cuidado com as métricas. Bold, AlKhateeb e Ersotelos (2022) observaram que parte da literatura privilegia a precisão e negligencia os falsos negativos. Ao comparar algoritmos em uma base de 730 amostras maliciosas e 735 benignas, os autores verificaram que a rede neural artificial obteve a maior precisão (98,65%), enquanto o *Random Forest*, com precisão menor (92,73%), não deixou passar nenhuma amostra maliciosa. Para eles, o custo de um falso negativo, isto é, de uma infecção não detectada, tende a superar o custo previsível de tratar os falsos positivos.

A literatura também aponta limitações relevantes. A revisão de Daengsi *et al.* (2026) destaca a escassez de bases de dados públicas, padronizadas e representativas, já que muitos estudos usam

amostras sintéticas ou geradas em ambientes controlados e muitas vítimas não relatam os ataques; a dificuldade de conciliar alta taxa de detecção com poucos alarmes falsos, que sobrecarregam os administradores; e o alto consumo de recursos das abordagens baseadas em anomalias. Os mesmos autores relatam que amostras modificadas para enganar um modelo de aprendizado profundo reduziram sua acurácia de 94% para 50%, e que os próprios atacantes passaram a empregar IA para tornar suas ferramentas mais difíceis de detectar. O Quadro 6 sintetiza esse balanço.

Quadro 6. Potencial e limitações do monitoramento com IA para PMEs

Potencial	Limitação
Detectar variantes novas pelo comportamento, e não apenas por amostras já conhecidas.	Bases de dados escassas e pouco representativas reduzem a capacidade de generalização dos modelos.
Identificar o ataque antes que a criptografia se complete.	Falsos positivos geram excesso de alertas e exigem alguém para analisá-los.
Isolar automaticamente o equipamento suspeito, apoiando a contenção.	Atacantes usam técnicas de evasão e de aprendizado adversarial para enganar os modelos.
Analisar um volume de eventos que uma equipe pequena não conseguiria acompanhar.	Custo e consumo de recursos tornam inviável o desenvolvimento de modelos próprios por PMEs.

Fonte: elaborado pelo autor (2026), com base em Bold, Al-Khateeb e Ersotelos (2022), Ferdous *et al.* (2024) e Daengsi *et al.* (2026).

Para as PMEs, essas constatações têm duas implicações práticas. A primeira é que desenvolver ou treinar modelos próprios está fora do alcance da maioria delas; o caminho realista é adotar soluções de proteção de estações e servidores que incorporem análise comportamental ou contratar serviços gerenciados de monitoramento e resposta, alternativa já prevista no Nível 2 do Quadro 4.

A segunda é que a IA complementa, mas não substitui, as práticas do Nível 1. Um alerta só tem valor se houver alguém para analisá-lo e um plano para agir, como o roteiro do Quadro 5, e nenhum modelo de detecção dispensa *backups* íntegros, autenticação multifator e sistemas atualizados. Como mostrou o caso do STJ, a recuperação continua dependendo do que foi preparado antes do ataque.

4.6 LIMITES DA PROTEÇÃO EM PMEs

O guia proposto não elimina o risco. A dupla extorsão faz com que mesmo uma empresa com *backups* adequados possa ser pressionada pela ameaça de vazamento, e controles como autenticação multifator e atualizações reduzem, mas não anulam, a probabilidade de acesso inicial. O objetivo do Nível 1 é tornar a empresa um alvo mais difícil e garantir que ela consiga se recuperar sem depender dos criminosos.

É preciso reconhecer, ainda, que medidas de baixo custo financeiro não são necessariamente de baixo esforço. Testar restaurações, manter atualizações e treinar colaboradores exigem tempo e disciplina contínuos, recursos igualmente escassos em organizações pequenas. Por isso, a designação de um responsável interno pela segurança, ainda que em acúmulo de funções, é condição para que o guia seja efetivamente aplicado.

5 CONSIDERAÇÕES FINAIS

Este estudo partiu da pergunta sobre quais práticas de segurança, ao alcance de PMEs, reduzem a probabilidade e o impacto de ataques de *ransomware*. A análise de cinco referenciais públicos e de incidentes brasileiros ocorridos entre 2020 e 2025 permitiu responder que existe um núcleo consensual de práticas, em grande parte viável com recursos já disponíveis nessas empresas.

Quanto ao primeiro objetivo específico, a caracterização da ameaça mostrou a transição de campanhas massivas para ataques direcionados, sustentados pelo modelo RaaS e pela dupla extorsão, e identificou *phishing*, acesso remoto mal protegido, vulnerabilidades não corrigidas e credenciais comprometidas como principais vetores de entrada.

Em relação ao segundo objetivo, os incidentes analisados indicaram três fatores recorrentes: o *backup* íntegro como condição de recuperação independente dos criminosos, as falhas de controle de acesso como facilitadoras da progressão dos ataques e a contenção rápida como redutora de impacto.

Quanto ao terceiro objetivo, verificou-se que nove das dez práticas mapeadas aparecem explicitamente em pelo menos três dos cinco referenciais. O quarto objetivo foi atendido com a organização dessas práticas em um guia de três níveis, cujo primeiro nível concentra *backups* isolados e testados, autenticação multifator, atualizações, redução de serviços expostos, conscientização e controle de privilégios.

O quinto objetivo foi atendido com o roteiro de resposta e recuperação em oito passos, adaptado do CERT.br, que evidenciou que a recuperação depende de decisões tomadas antes do incidente e da ordem correta entre contenção, eliminação e restauração. A análise do monitoramento com IA mostrou que essas técnicas ampliam a capacidade de detectar ataques antes da criptografia, mas enfrentam falsos positivos, bases de dados limitadas e técnicas de evasão; para PMEs, sua adoção realista ocorre por meio de soluções ou serviços gerenciados, como complemento, e não substituto, das práticas essenciais.

O estudo apresenta limitações. Os incidentes analisados envolvem, em sua maioria, organizações de grande porte, pois as PMEs raramente divulgam os ataques que sofrem, de modo que as lições foram transpostas por analogia. Parte das informações sobre os casos provém da imprensa, e não de relatórios técnicos das vítimas. A discussão sobre IA baseou-se em estudos publicados, sem testes próprios de ferramentas, e uma das revisões utilizadas ainda é um *preprint*. O guia também não foi aplicado em empresas reais, e sua eficácia e seu custo de implantação permanecem hipóteses.

Como trabalhos futuros, sugere-se aplicar o guia em PMEs de diferentes setores, medindo o esforço de implantação e o nível de maturidade antes e depois da intervenção, bem como investigar formas de estimular a notificação de incidentes por empresas de menor porte, o que ampliaria a base de evidências disponível no país. Sugere-se, ainda, avaliar em ambientes reais de PMEs soluções de detecção baseadas em IA quanto à taxa de falsos positivos, ao custo e ao esforço de operação.

Por fim, o trabalho contribui ao traduzir referenciais extensos, em sua maioria estrangeiros, em um roteiro único, gratuito e priorizado, adequado à realidade de quem precisa começar pela proteção essencial. As seis práticas do Nível 1 dependem sobretudo da configuração de recursos que muitas PMEs já utilizam, como serviços de *e-mail* e nuvem com autenticação multifator, atualizações automáticas e cópias de segurança, o que torna possível iniciá-las sem investimento elevado.

DECLARAÇÃO DE USO DE INTELIGÊNCIA ARTIFICIAL

Ferramentas de inteligência artificial generativa foram utilizadas como apoio na pesquisa de fontes, na organização e na redação do texto. Todas as fontes foram verificadas pelos autores, que revisaram criticamente o conteúdo e assumem integral responsabilidade pelo trabalho.

REFERÊNCIAS

APLICATIVO ConecteSUS é restabelecido, diz Ministério da Saúde. **IstoÉ Dinheiro**, São Paulo, 23 dez. 2021. Disponível em: https://istoedinheiro.com.br/aplicativoconectesus-e-restabelecido-diz-ministerio-da-saude. Acesso em: 25 set. 2026.

ASSESPRO. **Grupos de ransomware atacam 25 empresas no Brasil**. [S. l.]: Assespro, 2024. Disponível em: https://assespro.org.br/en/grupos-de-ransomwareatacam-25-empresas-no-brasil/. Acesso em: 25 set. 2026.

ATAQUE hacker leva governo a adiar novas regras sanitárias para viajantes. **Sul21**, Porto Alegre, 10 dez. 2021. Disponível em: https://sul21.com.br/?p=153432. Acesso em: 25 set. 2026.

ATAQUE no Grupo Fleury foi de ransomware. **Baguete**, [S. l.], 23 jun. 2021. Disponível em: https://www.baguete.com.br/noticias/ataque-no-grupo-fleury-foi-deransomware. Acesso em: 25 set. 2026.

BARBOSA, Daniel Cunha; ARRUDA, Guilherme. Ransomware no Brasil em 2025: a evolução da ameaça. **WeLiveSecurity**, [S. l.], 15 out. 2025. Disponível em: https://www.welivesecurity.com/pt/ransomware/ransomware-brasil-2025-evolucaoameaca/. Acesso em: 25 set. 2026.

BOLD, Robert; AL-KHATEEB, Haider; ERSOTELOS, Nikolaos. Reducing false negatives in ransomware detection: a critical evaluation of machine learning algorithms. **Applied Sciences**, Basel, v. 12, n. 24, art. 12941, 2022. DOI: https://doi.org/10.3390/app122412941. Acesso em: 7 out. 2026.

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: 25 set. 2026.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte**.
Versão 1.0. Brasília, DF: ANPD, out. 2021. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-epublicacoes. Acesso em: 25 set. 2026.

CENTER FOR INTERNET SECURITY. **CIS Critical Security Controls**: version 8.1. [S. l.]: CIS, 2024. Disponível em: https://www.cisecurity.org/controls/implementationgroups/ig1. Acesso em: 25 set. 2026.

CERT.BR. **Ransomware**: como detectar. Versão 1.1. São Paulo: NIC.br, 5 out.
2025a. Disponível em: https://cert.br/docs/ransomware/detectar/. Acesso em: 25 set. 2026.

CERT.BR. **Ransomware**: como se proteger. São Paulo: NIC.br, 2025b. Disponível em: https://cert.br/docs/ransomware/proteger/. Acesso em: 25 set. 2026.

CERT.BR. **Ransomware**: como responder. Versão 1.1. São Paulo: NIC.br, 5 out. 2025c. Disponível em: https://cert.br/docs/ransomware/responder/. Acesso em: 25 set. 2026.

CISA. **#StopRansomware guide**. Washington, DC: Cybersecurity and Infrastructure Security Agency; FBI; NSA; MS-ISAC, maio 2023. Disponível em: https://www.cisa.gov/sites/default/files/2023-05/StopRansomware_Guide_508c.pdf. Acesso em: 25 set. 2026.

CONSELHO DA JUSTIÇA FEDERAL. **Comunicado**. Brasília, DF: CJF, nov. 2020. Disponível em: https://www.cjf.jus.br/cjf/noticias/2020/11-novembro/comunicado. Acesso em: 25 set. 2026.

DAENGSI, Therdpong et al. Ransomware and artificial intelligence: a comprehensive systematic review of reviews. **arXiv**, [S. l.], 2026. Preprint arXiv:2603.13734. Disponível em: https://arxiv.org/abs/2603.13734. Acesso em: 7 out. 2026.

FERDOUS, Jannatul; ISLAM, Rafiqul; MAHBOUBI, Arash; ISLAM, Md Zahid. AIbased ransomware detection: a comprehensive review. **IEEE Access**, [S. l.], v. 12, p. 136666-136695, 2024. DOI: https://doi.org/10.1109/ACCESS.2024.3461965. Acesso em: 7 out. 2026.

FLEURY é alvo de ciberataque e afirma que soluções de contingência foram adotadas. **IstoÉ Dinheiro**, São Paulo, 22 jun. 2021. Disponível em: https://istoedinheiro.com.br/fleury-e-alvo-de-ciberataque-e-afirma-que-solucoes-decontingencia-foram-adotadas-2. Acesso em: 25 set. 2026.
FLEURY sofre novo ataque. **Baguete**, [S. l.], 8 maio 2023. Disponível em: https://www.baguete.com.br/noticias/fleury-sofre-novo-ataque. Acesso em: 25 set. 2026.

NIC.BR. **Guia do CERT.br mostra como proteger empresas de ataques de ransomware**. São Paulo: NIC.br, 2025. Disponível em: https://www.nic.br/noticia/namidia/guia-do-cert-br-mostra-como-proteger-empresas-de-ataques-de-ransomware/. Acesso em: 25 set. 2026.

NIST. **The NIST Cybersecurity Framework (CSF) 2.0**. Gaithersburg, MD: National Institute of Standards and Technology, 2024. (NIST CSWP 29). DOI: https://doi.org/10.6028/NIST.CSWP.29. Acesso em: 25 set. 2026.

OZ, Harun; ARIS, Ahmet; LEVI, Albert; ULUAGAC, A. Selcuk. A survey on ransomware: evolution, taxonomy, and defense solutions. **ACM Computing Surveys**, New York, v. 54, n. 11s, art. 238, p. 1-37, 2022. DOI: https://doi.org/10.1145/3514229. Versão aberta disponível em: https://arxiv.org/abs/2102.06249. Acesso em: 25 set. 2026.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed.
Novo Hamburgo: Feevale, 2013. Disponível em: http://www.feevale.br/Comum/midias/8807f05a-14d0-4d5b-b1ad-1538f3aef538/Ebook%20Metodologia%20do%20Trabalho%20Cientifico.pdf. Acesso em: 25 set. 2026.

SÁ, José Cândido Reis de; COELHO, Keoma de Sousa. Ransomware: análise de impactos e metodologia de prevenção em pequenas e médias empresas.
RevistaFT, Rio de Janeiro, v. 29, n. 152, nov. 2025. DOI: 10.69849/revistaft/pa10202511291852. Disponível em: https://revistaft.com.br/ransomware-analise-de-impactos-e-metodologia-deprevencao-em-pequenas-e-medias-empresas/. Acesso em: 25 set. 2026.

SANTOS, Andrei Pereira dos; SILVA, Eliabe Anderson da; PINTO, Diego Santos Almeida. Os desafios na proteção de informações sensíveis em pequenas e médias empresas diante de ataques cibernéticos. **RECIMA21 Revista Científica Multidisciplinar**, [S. l.], v. 6, n. 10, e6106885, 2025. DOI: https://doi.org/10.47820/recima21.v6i10.6885. Acesso em: 25 set. 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Comunicado da Presidência do STJ**. Brasília, DF: STJ, 19 nov. 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/19112020Comunicado-da-Presidencia-do-STJ.aspx. Acesso em: 25 set. 2026.