Gestão & Gerenciamento

IMPLEMENTAÇÃO DE CIBERSEGURANÇA EM PMES: UMA ABORDAGEM DE GERENCIAMENTO DE PROJETOS

CYBERSECURITY IMPLEMENTATION IN SMES: A PROJECT MANAGEMENT APPROACH

Ricardo Tadeu Facincani

Analista de Sistemas; Pós-Graduado em Sistemas Distribuídos em Orientação a Objetos e em Computação Forense e Perícia Digital. Pós graduando em Gestão e Gerenciamento de Projetos, Universidade Federal do Rio de Janeiro, Rio de Janeiro, Brasil.

ricardo@facincani.eti.br

Luiz Felippe de Oliveira e Silva Junior

Médico do Trabalho e Gastroenterologista; graduado pela Faculdade Souza Marques, Pós-Graduado em Gastroenterologia pela instituição Carlos Chagas. Rio de Janeiro, Brasil.

luizfelippe@seconci-rio.com.br

Resumo

Este artigo explora a implementação de cibersegurança em Pequenas e Médias Empresas (PMEs) utilizando uma abordagem ágil de gerenciamento de projetos. Com o aumento significativo dos ataques cibernéticos, as PMEs enfrentam desafios únicos devido a recursos limitados e falta de expertise. O estudo analisa o panorama atual das ameaças cibernéticas no Brasil, apresenta fundamentos de cibersegurança e propõe uma metodologia ágil para implementação de medidas de segurança. A pesquisa utiliza dados de relatórios recentes e propõe um framework adaptado para PMEs. Os resultados indicam que a abordagem ágil oferece flexibilidade e eficácia na implementação de cibersegurança, permitindo às PMEs melhorarem sua postura de segurança de forma gradual e contínua.

Palavras-chave: Cibersegurança; PMEs; Gerenciamento Ágil de Projetos; Segurança da Informação; Riscos Cibernéticos.

Abstract

This article explores the implementation of cybersecurity in Small and Medium Enterprises (SMEs) using an agile project management approach. With the significant increase in cyberattacks, SMEs face unique challenges due to limited resources and lack of expertise. The study analyzes the current landscape of cyber threats in Brazil, presents cybersecurity fundamentals, and proposes an agile methodology for implementing security measures. The research uses data from recent reports and proposes an adapted framework for SMEs. The results indicate that the agile approach offers flexibility and effectiveness in implementing cybersecurity, allowing SMEs to improve their security posture gradually and continuously.

Keywords: *Cybersecurity; SMEs; Agile Project Management; Information Security; Cyber Risks.*

1 Introdução

A cibersegurança tornou-se uma prioridade crucial para organizações de todos os tamanhos, especialmente para as Pequenas e Médias Empresas (PMEs). Com o aumento das ameaças cibernéticas e a crescente dependência de tecnologias digitais, as PMEs precisam implementar medidas de segurança robustas para proteger seus ativos, dados e reputação.

Para PMEs, a perda de dados ou a interrupção das operações devido a um ataque cibernético pode ter consequências devastadoras, incluindo perdas financeiras significativas, danos à reputação e até mesmo a falência. Além disso, a conformidade com regulamentações e normas de proteção de dados tornou-se uma exigência legal em muitos setores.

Este artigo apresenta uma abordagem ágil para a implementação de cibersegurança em PMEs, utilizando princípios e práticas de gerenciamento de projetos. Fornece um guia prático e acessível que visa fortalecer a postura de segurança cibernética de forma eficiente e econômica. O artigo aborda o contexto atual de ameaças cibernéticas, fundamentos de cibersegurança específicos para PMEs, aplicação da metodologia Ágil em projetos de cibersegurança, etapas práticas para implementação, desafios comuns e suas soluções, concluindo com recomendações finais. A abordagem é qualitativa, baseada em revisão de literatura e análise de dados secundários. Foram consultados relatórios recentes de segurança cibernética, estudos acadêmicos e publicações de órgãos especializados. A proposta de

implementação ágil foi desenvolvida com base nos princípios do Scrum e adaptada para o contexto das PMEs brasileiras.

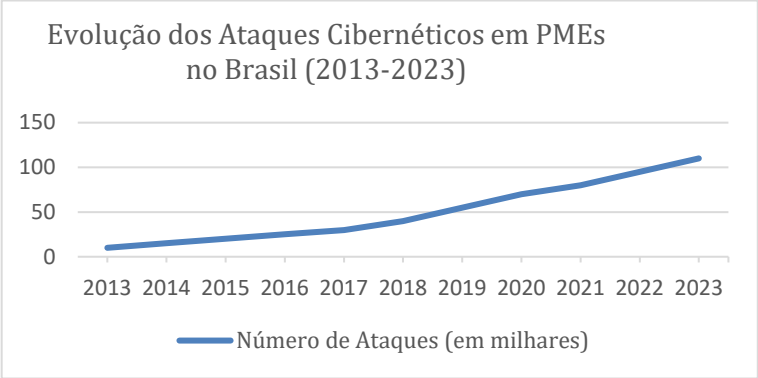
2 Contexto e Justificativa

2.1. Panorama Atual das Ameaças Cibernéticas

2.1.1. Evolução dos Ataques Cibernéticos a PMEs

Segundo o relatório da Fortinet (2002), houve um aumento de 95% nos ataques cibernéticos contra empresas brasileiras em geral, incluindo PMEs, em comparação com o ano anterior. A pesquisa da Confederação Nacional da Indústria (CNI, 2021) indica que 23% das empresas industriais brasileiras, incluindo PMEs, sofreram algum tipo de ataque cibernético nos últimos 12 meses.

Gráfico 1 – Evolução de Ataques no período de 2013 a 2023.



Fonte: Elaborado pelo autor baseado em Fortinet (2022) e Kaspersky (2022)

2.1.2. Tipos de Ataques Mais Comuns

Ransomware e phishing continuam sendo as principais ameaças. De acordo com a Kaspersky (2022), o Brasil foi o país mais afetado por ransomware na América Latina em 2021, com um aumento de 92% nos ataques em relação a 2020. A Axur (2022) reportou um aumento de 27% nos ataques de phishing no Brasil em 2021 em comparação com 2020.

2.1.3. Estudo de Caso Recente: Ataque ao Sicoob

Um incidente recente envolvendo o Sicoob, uma das maiores cooperativas de crédito do Brasil, ilustra a crescente ameaça de ataques cibernéticos no setor financeiro. Em junho de 2023, o grupo de ransomware RansomHub alegou ter obtido acesso a mais de 1 terabyte de dados sensíveis da instituição. Os dados supostamente vazados incluem informações pessoais de clientes e funcionários, dados financeiros de empresas e documentos contratuais (CISO ADVISOR, 2023).

Este caso destaca vários pontos cruciais:

1. A vulnerabilidade de instituições financeiras, incluindo cooperativas, a ataques cibernéticos sofisticados.
2. O potencial impacto devastador em termos de violação de privacidade e possíveis perdas financeiras.

3. A necessidade urgente de implementação de medidas robustas de cibersegurança, mesmo em instituições de médio porte.

Para PMEs do setor financeiro e outros setores que lidam com dados sensíveis, este incidente serve como um alerta claro. Demonstra a importância de:

- Implementar sistemas de segurança avançados
- Manter backups seguros e atualizados
- Treinar funcionários em práticas de segurança cibernética
- Desenvolver e testar planos de resposta a incidentes

Este caso reforça a necessidade das estratégias de implementação ágil de cibersegurança discutidas neste artigo, destacando como mesmo grandes instituições podem ser vulneráveis e como a preparação e resposta rápida são cruciais no cenário atual de ameaças cibernéticas.

2.1.4 Incidente do Sensor Falcon da CrowdStrike

Em 19 de julho de 2024, um problema significativo de segurança cibernética ocorreu devido a um defeito no sensor CrowdStrike Falcon, resultando em uma grande falha tecnológica global. Este incidente afetou múltiplos setores, incluindo aviação, bancos e saúde, causando interrupções em operações críticas e destacando a importância de uma cibersegurança robusta para prevenir tais eventos. A CrowdStrike rapidamente implementou uma correção para o problema, que foi causado por uma atualização de conteúdo para hosts Microsoft Windows, levando a falhas do sistema conhecidas como "Blue Screen of Death" (RAPPLER, 2024; KITCO NEWS, 2024).

Assim como no caso do Sicoob, este incidente ressalta a importância de implementar medidas de segurança cibernética robustas e ágeis, capazes de responder rapidamente a falhas e ameaças emergentes. PMEs devem estar preparadas para lidar com incidentes semelhantes, garantindo a continuidade dos negócios e a proteção de dados sensíveis.

2.1.5 Panorama Atual de Ciberataques em PMEs

“De acordo com uma pesquisa realizada pela Kaspersky, pesquisas recentes revelam um cenário alarmante de ciberataques direcionados a PMEs 63% das vítimas de ciberataques são pequenas e médias empresas, entre outubro de 2022 e outubro de 2023 (PMEs)" (SBT NEWS, 2024):

- 63% das vítimas de ciberataques foram PMEs.
- 192 milhões de tentativas de ataques contra PMEs foram bloqueadas.
- Uma média de 526 mil bloqueios diários ou 365 detecções por minuto foi registrada.
- O Brasil figura entre os países mais atacados globalmente.

Marta Helena Schuh, diretora de Seguros Cibernéticos e Tecnológicos da Howden Brasil, atribui essa vulnerabilidade a fatores como a rápida digitalização, ampliando a superfície de ataque, e a baixa maturidade em segurança cibernética entre empresas brasileiras (SBT NEWS, 2024).

Além disso, um levantamento da Check Point Research aponta que os ataques cibernéticos no Brasil cresceram quase 70% em um ano, destacando um aumento significativo na sofisticação dos cibercriminosos que utilizam técnicas avançadas ligadas à inteligência artificial (DI LORENZO, 2024). De acordo com o estudo, foram registrados 1.636 ataques hackers por semana no segundo trimestre de 2024, representando um aumento de 30% em comparação com o mesmo período do ano anterior.

Quadro 1 – Evolução de ataques hackers por trimestre

Período	Número de ataques por semana	Aumento Percentual
2º Trimestre de 2023	1.257	-----
1º Trimestre de 2024	1.309	4,14%
2º Trimestre de 2024	1.636	30,17%

Fonte: Elaborado pelo autor com base em Di Lorenzo (2004).

A importância de proteger as PMEs é sublinhada pelo fato de que elas representam cerca de 54% do PIB brasileiro, com uma estimativa de 19 milhões de micro e pequenas empresas.

Nycholas Szucko, especialista em cibersegurança, ressalta que em 2023, o faturamento global dos cibercriminosos ultrapassou US$ 10 trilhões, destacando a urgência da situação (SBT NEWS, 2024).

Para mitigar esses riscos, especialistas recomendam:

- Treinamento de funcionários em segurança cibernética básica.
- Instalação de soluções de proteção corporativa específicas para PMEs.
- Implementação de políticas de acesso rigorosas para ativos corporativos.
- Busca de auxílio de profissionais especializados em segurança cibernética.

Estas informações reforçam a necessidade de uma abordagem ágil na implementação de medidas de cibersegurança em PMEs, permitindo uma resposta rápida e adaptativa ao cenário de ameaças em constante evolução.

2.2. Vulnerabilidades Específicas de PMEs

As PMEs enfrentam desafios únicos, incluindo orçamentos limitados, falta de pessoal especializado e menor conscientização sobre riscos cibernéticos. A pesquisa da Cisco de 2021 revelou que 44% das PMEs no Brasil tiveram um incidente de cibersegurança no último ano, e 59% disseram que a cibersegurança é muito desafiadora para elas gerenciarem.

2.3. Necessidade de Implementação de Cibersegurança

O estudo da IBM Security (2021) mostrou que o custo médio de uma violação de dados no Brasil chegou a R$ 6,45 milhões, um aumento de 16,7% em relação ao ano anterior [6]. Isso ressalta a necessidade urgente de implementação de medidas de cibersegurança robustas nas PMEs brasileiras.

3 Fundamentos de Cibersegurança para PMEs

3.1 Princípios Básicos de Cibersegurança

Os princípios fundamentais da cibersegurança, conhecidos como a tríade CIA, incluem:

- Confidencialidade: Proteger dados contra acessos não autorizados.
- Integridade: Garantir a precisão e completude da informação.
- Disponibilidade: Assegurar que sistemas e dados estejam acessíveis quando necessário.

Quadro 2 - Estratégias de Cibersegurança Recomendadas para PMEs

Estratégia	Descrição	Implementação
Backup Regular	Realizar ccópia de segurança dos dados	Diário / Semanal
Atualização de Sistemas	Manter softwares e Sistemas Operacionais atualizados	Mensal
Senhas Fortes	Implementar política de Senhas Robustas	Imediata
Treinamento de Funcionários	Educar sobre práticas de segurança	Trimestral
Firewall e Antivírus	Implementar proteções básicas	Imediata

Fonte: Adaptado de SEBRAE (2022)

3.2 Estratégias Simples e Eficazes de Cibersegurança para PMEs

O SEBRAE (2022) recomenda as seguintes ações imediatas para PMEs:

- Realizar backup regular dos dados
- Manter softwares e sistemas operacionais atualizados
- Usar senhas fortes e autenticação de dois fatores
- Treinar funcionários em práticas de segurança
- Implementar um firewall e antivírus

3.3 Ferramentas e Tecnologias Acessíveis

- PMEs podem utilizar soluções como:
- Soluções de criptografia para proteger dados sensíveis
- Software de detecção de intrusões para monitorar atividades suspeitas
- Plataformas de gerenciamento de vulnerabilidades para identificar e corrigir falhas de segurança

4 Gerenciamento de Projetos em Cibersegurança: Abordagem Ágil

4.1. Introdução à Metodologia Ágil e sua relação com o PMI

A metodologia Ágil, reconhecida pelo Project Management Institute (PMI) como uma abordagem eficaz para gerenciamento de projetos, é caracterizada por iterações curtas, adaptabilidade e entrega incremental de valor. O PMI, em seu Guia PMBOK® 7ª edição, incorpora princípios ágeis, reconhecendo sua relevância em ambientes de negócios dinâmicos como o da cibersegurança (PMI, 2021).

4.2. Princípios Ágeis Aplicados à Cibersegurança

- Entregas incrementais: Implementar medidas de segurança gradualmente, alinhadas com recursos limitados.
- Adaptação contínua: Ajustar prioridades de segurança com base em novas ameaças identificadas.
- Colaboração: Promover uma cultura de segurança em toda a organização.
- Feedback contínuo: Facilitar a identificação e correção rápida de problemas de segurança.

4.3. Scrum em Projetos de Cibersegurança

- O Scrum, um framework Ágil popular, pode ser aplicado em projetos de cibersegurança da seguinte forma:
- Sprints curtos: Implementar medidas de segurança em ciclos de 1-2 semanas.
- Backlog do produto: Manter uma lista priorizada de medidas de segurança a serem implementadas.
- Reuniões diárias: Facilitar a comunicação e identificação rápida de problemas.
- Revisões de sprint: Avaliar o progresso e ajustar prioridades conforme necessário.

4.4. Alinhamento com as Práticas do PMI

O PMI enfatiza a importância da adaptabilidade e da entrega contínua de valor, aspectos fundamentais da abordagem Ágil. Em projetos de cibersegurança para PMEs, isso se traduz em:

- Planejamento adaptativo: Ajustar estratégias de segurança com base em ameaças emergentes.
- Entrega iterativa: Implementar medidas de segurança em ciclos curtos, permitindo feedback rápido.
- Colaboração contínua: Envolver stakeholders regularmente para alinhar as medidas de segurança às necessidades do negócio.

5 Etapas para Implementação de Cibersegurança em PMEs

5.1 Identificar ativos críticos e riscos

- Realizar um inventário de ativos digitais

- Conduzir uma avaliação de riscos

5.2 Proteger sistemas e dados

- Implementar controles de acesso
- Aplicar patches e atualizações de segurança

5.3 Detectar ameaças e vulnerabilidades

- Implementar sistemas de detecção de intrusão
- Realizar varreduras regulares de vulnerabilidades

5.4 Responder a incidentes

- Desenvolver um plano de resposta a incidentes
- Treinar a equipe em procedimentos de resposta

5.5 Recuperar e aprender

- Implementar processos de backup e recuperação
- Conduzir análises pós-incidente para melhoria contínua

6 Desafios e Soluções na Implementação de Cibersegurança

Segundo a pesquisa da Cisco, os principais desafios de cibersegurança para PMEs no Brasil são:

- Falta de pessoal treinado (41%)
- Orçamento limitado (40%)
- Falta de tempo para avaliar e entender todas as informações (37%)

Soluções propostas:

- Investir em treinamento e conscientização dos funcionários
- Utilizar soluções de segurança em nuvem para reduzir custos de infraestrutura
- Priorizar medidas de segurança com base em análises de risco

7. Consequências e Custos da Não Implementação de Cibersegurança

7.1. Panorama de Ameaças Cibernéticas no Brasil

Segundo o relatório anual do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT, 2023), em 2022 houve um aumento significativo nos incidentes de segurança reportados:

- Total de 2.714.540 notificações de incidentes, um aumento de 33% em relação a 2021.
- 33,96% dos incidentes foram tentativas de fraudes, seguidos por ataques de varredura (29,12%) e ataques específicos (13,45%).

7.2. Impacto Financeiro em PMEs

Um estudo realizado pela Confederação Nacional da Indústria (CNI) em 2021 revelou:

- 23% das empresas industriais brasileiras, incluindo PMEs, sofreram ataques cibernéticos nos 12 meses anteriores à pesquisa.
- 49% das empresas que sofreram ataques tiveram prejuízos financeiros.
- 18% das empresas afetadas estimaram perdas entre R$ 10 mil e R$ 50 mil.

7.3. Consequências Jurídicas e Regulatórias

Com a implementação da Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018), as consequências jurídicas para violações de dados se tornaram mais severas:

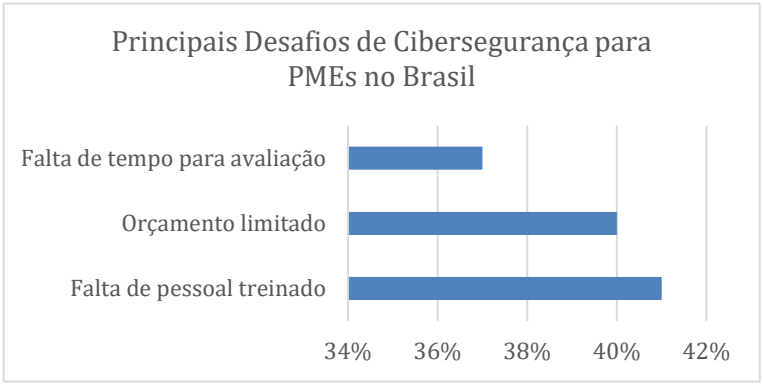
- Multas de até 2% do faturamento da empresa, limitadas a R$ 50 milhões por infração.
- Obrigação de notificar afetados e autoridades em caso de vazamentos de dados.
- Possibilidade de ações coletivas por danos morais em caso de violações.

7.4. Desafios Específicos para PMEs

De acordo com o relatório "Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense" da Cisco (2021), as PMEs brasileiras enfrentam desafios únicos:

- 44% das PMEs no Brasil sofreram um incidente de cibersegurança no ano anterior.
- Os principais desafios citados foram:
    1. Falta de pessoal treinado (41%)
    2. Orçamento limitado (40%)
    3. Falta de tempo para avaliar e entender todas as informações de segurança (37%)

Gráfico 2 - Cisco. Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense. 2021.



Fonte: Elaborado pelo autor (2024) com dados do relatório da Cisco (2021)

7.5. Necessidade de Investimento em Cibersegurança

Considerando os dados apresentados, fica evidente que o investimento em cibersegurança não é apenas uma medida preventiva, mas uma necessidade crítica para a sustentabilidade e competitividade das PMEs no cenário digital atual. A implementação de

medidas de segurança adequadas pode prevenir perdas financeiras significativas, proteger a reputação da empresa e garantir conformidade com regulamentações como a LGPD.

8. Estudo de Caso: Implementação Ágil de Cibersegurança em uma PME

Este estudo de caso hipotético é baseado em práticas recomendadas e adaptado para ilustrar como uma PME pode implementar medidas de cibersegurança usando princípios ágeis alinhados com as diretrizes do PMI.

Contexto: Uma empresa de comércio eletrônico com 50 funcionários decidiu melhorar sua postura de cibersegurança após um incidente menor de violação de dados.

Abordagem Ágil: A empresa adotou um framework Scrum simplificado, com sprints de duas semanas.

Etapas do Projeto:

1. **Formação da Equipe:**
   - Scrum Master: Gerente de TI
   - Product Owner: Diretor de Operações
   - Equipe: 2 desenvolvedores, 1 analista de segurança, 1 representante do atendimento ao cliente
2. **Criação do Backlog do Produto:**
   - Implementar autenticação de dois fatores
   - Atualizar políticas de senha
   - Configurar firewall de nova geração
   - Treinar funcionários em práticas de segurança
   - Implementar sistema de detecção de intrusão
   - Desenvolver plano de resposta a incidentes
3. **Sprints:**
   - Sprint 1: Implementação de autenticação de dois fatores e atualização de políticas de senha
   - Sprint 2: Configuração de firewall e início do treinamento de funcionários
   - Sprint 3: Continuação do treinamento e implementação do sistema de detecção de intrusão
   - Sprint 4: Desenvolvimento do plano de resposta a incidentes
4. **Revisões e Retrospectivas:** Ao final de cada sprint, a equipe realizava uma revisão com stakeholders e uma retrospectiva para melhorar o processo.

Resultados:

- Implementação rápida de medidas críticas de segurança

- Maior engajamento dos funcionários devido ao treinamento contínuo
- Adaptação ágil às mudanças de prioridade baseadas em novas ameaças identificadas

Alinhamento com Princípios do PMI:

- Entrega de valor incremental
- Engajamento de stakeholders
- Adaptação a mudanças

9 Considerações Finais

A implementação de cibersegurança em PMEs através de uma abordagem ágil representa uma estratégia promissora para enfrentar os desafios crescentes no cenário digital. Este estudo demonstrou que a flexibilidade e adaptabilidade do método ágil são particularmente adequadas para o contexto dinâmico das ameaças cibernéticas.

A análise do panorama brasileiro revelou um aumento alarmante nos ataques cibernéticos, ressaltando a urgência de medidas de proteção. O framework proposto, baseado em princípios ágeis, oferece uma abordagem prática e acessível para PMEs implementarem gradualmente medidas de segurança, alinhadas com suas limitações de recursos.

Os desafios identificados, como a falta de pessoal treinado e orçamento limitado, podem ser mitigados através de estratégias como o investimento em treinamento contínuo e a adoção de soluções em nuvem. A priorização baseada em análise de risco permite uma alocação eficiente dos recursos disponíveis.

Futuros estudos poderiam explorar a eficácia a longo prazo desta abordagem, bem como desenvolver métricas específicas para avaliar o progresso da maturidade em cibersegurança em PMEs. Ademais, a colaboração entre PMEs, formando comunidades de prática em cibersegurança, poderia ser uma via promissora para compartilhar conhecimentos e recursos.

Em conclusão, a adoção de uma abordagem ágil na implementação de cibersegurança oferece às PMEs uma via viável para fortalecer sua postura de segurança, adaptando-se continuamente às ameaças emergentes e contribuindo para um ecossistema digital mais resiliente.

9.1. Resumo dos Pontos-Chave

- A cibersegurança é crucial para a sobrevivência e competitividade das PMEs
- A abordagem Ágil oferece flexibilidade e adaptabilidade necessárias para projetos de cibersegurança
- A implementação deve ser gradual, focada em prioridades e adaptável a novas ameaças

9.2. Recomendações Finais para PMEs

- Adotar uma abordagem Ágil para implementação de cibersegurança
- Priorizar a educação e conscientização dos funcionários

- Implementar medidas básicas de segurança imediatamente (backup, atualizações, senhas fortes)
- Buscar parcerias ou consultorias especializadas quando necessário
- Manter-se informado sobre novas ameaças e regulamentações

Referências

AXUR. **Relatório de Ameaças Digitais - Brasil 2021**. 2022. Disponível em: https://www.axur.com/pt-br/relatorio-ameacas-digitais-2021. Acesso em05/11/2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157, p. 59-64, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 09/01/2024

CERT. **Estatísticas dos Incidentes Reportados ao CERT.br.** 2023. Disponível em: https://www.cert.br/stats/incidentes . Acesso em: 09/01/2024.

CISCO. **Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense**, 2021.

CISO ADVISOR. **Sicoob sofre ataque de ransomware e tem dados vazados, diz grupo hacker.** 2023. Disponível em: https://cisoadvisor.com.br/sicoob-sofre-ataque-de-ransomware-e-tem-dados-vazados-diz-grupo-hacker/. Acesso em: 02/07/2024

CNI. **Cibersegurança: diagnóstico e recomendações para as empresas industriais**. Brasília: 2021. 88 p. Disponível em: https://static.portaldaindustria.com.br/media/filer_public/8b/d1/8bd1f9bd-be2f-44a2-8dc9-b9b54c89cb8f/ciberseguranca_-_diagnostico_e_recomendacoes_para_as_empresas_industriais.pdf. Acesso em: 05/11/2023

DI LORENZO, A. **Ataques cibernéticos crescem quase 70% no Brasil em um ano.** Olhar Digital. 2024. Disponível em: https://olhardigital.com.br/2024/07/19/seguranca/ataques-ciberneticos-crescem-quase-70-no-brasil-em-um-ano/. Acesso em: 24/07/2024.

FORTINET. **FortiGuard Labs Threat Landscape Report.** 2022. Disponível em: https://www.fortinet.com/br/demand/gated/threat-report-2h-2022. Acesso em 02/06/2024

IBM SECURITY. **Cost of a Data Breach Report 2021.** Armonk: IBM, 2021. Disponível em: https://www.ibm.com/security/data-breach. Acesso em: 10/12/2023.

KASPERSKY. **Estatísticas de ameaças na América Latina em 2021: o que mudou?** 2022. Disponível em: https://latam.kaspersky.com/blog/estatisticas-kal-2021/22860/. Acesso em: 05/11/2023

KITCO NEWS. **CrowdStrike says deployed fix for issue causing global tech outage.** Disponível em: https://www.kitco.com/news/off-the-wire/2024-07-19/crowdstrike-says-deployed-fix-issue-causing-global-tech-outage. Acesso em: 24/07/2024.

PMI. Project Management Institute. **Um guia do conhecimento em gerenciamento de projetos. Guia PMBOK**. 7. ed. Newton Square. 2021.

RAPPLER. **CrowdStrike deploys fix for issue causing global tech outage**. Disponível em: https://www.rappler.com/technology/crowdstrike-deploys-fix-issue-causing-global-tech-outage-july-19-2024. Acesso em: 24/07/2024.

SBT NEWS. **Especialistas dão dicas de como pequenas e médias empresas podem se proteger de ciberataques.** 2024. Disponível em: https://www.sbtnews.com.br/noticia/economia/258416-especialistas-dao-dicas-de-como-pequenas-e-medias-empresas-podem-se-proteger-de-ciberataques. Acesso em: 02/07/2024.

SEBRAE. **Cibersegurança para pequenos negócios.** 2022. Disponível em: https://www.sebrae.com.br/sites/PortalSebrae/artigos/ciberseguranca-para-pequenos-negocios . Acesso em: 10/12/2023.