UNIVERSIDADE FEDERAL DE SANTA
CATARINACENTRO TECNOLÓGICO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Jouson Barreto José

IMPLEMENTAÇÃO DE POLÍTICAS DE SEGURANÇA EM REDES DE COMPUTADORES: ABORDAGENS EFICAZES PARA PROTEGER DADOS E SISTEMAS CONTRA AMEAÇAS CIBERNÉTICAS.

Orientador: Carlos Bekel Westphal. Phd

Resumo:

A implementação de políticas de segurança em redes de computadores é essencial para proteger a integridade e confidencialidade das informações, bem como garantir que os sistemas estejam disponíveis quando necessários. Essas políticas envolvem a definição de regras e procedimentos para proteger ativos digitais, como dados confidenciais, propriedade intelectual e informações estratégicas. Além disso, as organizações precisam estar preparadas para detectar e responder a possíveis incidentes de segurança, como tentativas de invasão, malware ou phishing.

A implementação eficaz dessas políticas pode envolver a utilização de tecnologias como firewalls para controlar o tráfego de rede, antivírus para proteção contra malware, sistemas de detecção de intrusões para identificar atividades suspeitas e a adoção de práticas de segurança em todos os níveis da organização. É um tema crucial no contexto atual, em que as ameaças cibernéticas estão em constante evolução e representam riscos significativos para empresas e instituições.

1.INTRODUÇÃO

1.1.MOTIVAÇÃO

A implementação de políticas de segurança em redes de computadores desempenha um papel essencial na proteção de dados e sistemas contra ameaças cibernéticas cada vez mais sofisticadas e frequentes. Com o aumento da conectividade e a crescente dependência de ambientes digitais, empresas e organizações enfrentam desafios constantes em garantir a integridade, confidencialidade e disponibilidade de suas informações. Nesse contexto, é fundamental adotar abordagens eficazes que abrangem não apenas a implementação de tecnologias e ferramentas de segurança, mas também a conscientização e treinamento de colaboradores, a criação de políticas claras e procedimentos de resposta a incidentes, a avaliação contínua de vulnerabilidades, entre outros aspectos. A combinação de medidas técnicas, humanas e organizacionais é essencial para fortalecer a postura de segurança de uma rede de computadores. Ao considerar a implementação de políticas de segurança, é importante avaliar as necessidades específicas de cada ambiente, levando em conta fatores como o tipo de dados armazenados, as regulamentações que devem ser seguidas, o perfil de ameaças mais comuns, entre outros aspectos. Além disso, a colaboração com profissionais de segurança da informação e a atualização constante das práticas adotadas são fundamentais para garantir a eficácia das medidas de proteção. A escolha do tema "Implementação de políticas de segurança em redes de computadores: abordagens eficazes para proteger dados e sistemas contra ameaças cibernéticas", com base na referência de Brown e Lee em 2024 sobre "Cyber Threat Intelligence: Strategies for Effective Implementation", é motivada pela importância crescente da cibersegurança em um mundo cada vez mais conectado digitalmente. A abordagem de inteligência de ameaças cibernéticas oferece uma visão estratégica e proativa para lidar com os desafios da segurança da informação. Ao explorar estratégias eficazes de implementação descritas por Brown e Lee, os profissionais de segurança de rede podem aprimorar suas práticas e fortalecer as defesas contra as ameaças cibernéticas emconstante evolução. A crescente sofisticação dos ataques cibernéticos e as potenciais repercussões dos incidentes de segurança destacam a necessidade de adotar medidas abrangentes para proteger

os dados e sistemas em redes de computadores. A implementação de políticas de segurança baseadas em estratégias de inteligência de ameaças pode fornecer uma vantage significativa na detecção precoce, resposta eficaz e mitigação de riscos de segurança.

1.2JUSTIFICATIVA

A escolha do tema "Implementação de políticas de segurança em redes de computadores" para o meu trabalho é altamente relevante e justificável por diversas razões. Primeiramente, a segurança cibernética é um dos principais desafios enfrentados pelas organizações atualmente, devido ao constante aumento de ameaças, ataques e vulnerabilidades nas redes de computadores. Proteger os dados e sistemas contra essas ameaças é essencial para garantir a continuidade das operações e a confiança dos stakeholders. Além disso, a implementação de políticas de segurança em redes de computadores é um processo complexo que envolve a definição de diretrizes, procedimentos e controles para mitigar riscos de segurança. Compreender as abordagens eficazes nesse contexto é fundamental para uma gestão adequada da segurança da informação. (Kienen, 2019).

1.3 OBJETIVOS

1.4 OBJETIVO GERAL

O objetivo geral deste trabalho é analisar e propor abordagens eficazes para a implementação de políticas de segurança em redes de computadores a fim de proteger dados e sistemas contra ameaças cibernéticas.

1.5 OBJETIVOS ESPECÍFICOS

• Realizar um estudo sobre os principais desafios e ameaças de segurança em redes de computadores.

• Analisar as melhores práticas e diretrizes para elaboração e implementação de políticas de segurança da informação.

• Propor estratégias e medidas específicas para aumentar a proteção de dados e sistemas em ambientes de rede.

• Avaliar a eficácia das políticas de segurança implementadas por meio de testes e simulações de ataques cibernéticos.

1.6 ORGANIZAÇÃO DO ARTIGO

O presente trabalho estará estructurado da seguinte forma: uma introdução, seis capítulos.

Capítulo 1 Introdução, objetivos, estrutura

Capítulo 2 Conceitos básicos de segurança da informação

Capítulo3 Principais desafios e ameaças cibernéticas em redes de computadores e diretrizes e melhores práticas para implementação de políticas de segurança.

Capitulo 4 estratégias importantes para uma implementação eficaz de inteligência de ameaças cibernéticas.

Capitulo 5 segurança em redes de computadores

capítulo 6 serão apresentados os trabalhos relacionados, com suas devidas analises.

documento culmina com as conclusões, recomendações, referências bibliográficas e apêndices.

CAPÍTULO 2 CONCEITOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

2.1 DADOS E INFORMAÇÃO

Não podemos falar de segurança da informação sem antes compreender o que são dados e informações . Dados: São a base fundamental da informação. Os dados são os elementos brutos e distintos coletados e registrados, geralmente sem contexto ou significado. Eles são a matéria-prima sobre a qual as organizações operam e geram valor. Informação: É o resultado do processamento e interpretação dos dados. A informação agrega contexto, significado e relevância aos dados, tornando-os compreensíveis e utilizáveis para tomada de decisões e execução de processos. (Laudon, p 5 , 2021).

2.2 SEGURANÇA DE INFORMAÇÃO E OS SEUS PILARES

A Segurança da Informação é a proteção da informação de diferentes tipos de ameaças e se concentra na proteção da integridade, confidencialidade e disponibilidade das informações. Os principais conceitos e pilares da segurança da informação são:

1. Confidencialidade: Refere-se à proteção das informações contra acessos não autorizados. Para garantir a confidencialidade, é essencial implementar políticas de controle de acesso, criptografia, firewalls e outras medidas de segurança.

2. Integridade: Consiste em garantir que as informações permaneçam precisas e íntegras ao longo do tempo e não sejam modificadas por pessoas não autorizadas. O uso de assinaturas digitais, checksums e controle de versões são práticas comuns para manter a integridade dos dados.

3. Disponibilidade: Envolve garantir que as informações estejam acessíveis quando necessário. Para assegurar a disponibilidade, é importante implementar mecanismos de backup, redundância de sistemas e planos de continuidade de negócios.

4. Autenticidade: Refere-se à verificação da identidade de uma entidade, como um usuário ou um sistema. A autenticação pode ser feita por meio de senhas, tokens de segurança, biometria e outros métodos de verificação de identidade.

5. Não repúdio: Significa garantir que uma entidade não possa negar a autoria de uma ação realizada. A utilização de assinaturas digitais e registros de

auditoria são medidas comuns para evitar o repúdio de transações. (27001, 2013).

3 PRINCIPAIS DESAFIOS E AMEAÇAS CIBERNÉTICAS EM REDES DE COMPUTADORES.

Com o avanço da tecnologia, a utilização de redes de computadores se tornou indispensável para as empresas. No entanto, juntamente com a conveniência proporcionada por essas redes, surgem também desafios e ameaças cibernéticas que podem comprometer a segurança e a privacidade dos dados.

Um dos principais desafios enfrentados pelas redes de computadores é a vulnerabilidade dos sistemas. Com o aumento constante das ameaças cibernéticas, como malware, phishing e ransomware, torna-se fundamental implementar políticas de segurança eficazes para proteger as informações sensíveis. Além disso, a falta de conscientização dos utilizadores sobre os riscos cibernéticos é outra ameaça significativa. Muitas vezes, os funcionários não estão devidamente informados sobre as práticas seguras de navegação na internet e acabam expondo a rede a possíveis ataques.

Para mitigar esses desafios e ameaças, é essencial seguir diretrizes e melhores práticas para implementar políticas de segurança. Entre as medidas recomendadas estão a utilização de:

Firewall: O firewall é uma barreira de segurança que monitora e controla o tráfego de rede com base em um conjunto de regras de segurança. Ele ajuda a impedir que ameaças externas acessem a rede e protege os dados contra acessos não autorizados.

Antivírus: O software antivírus é projetado para detectar, prevenir e remover programas maliciosos, como vírus, worms, trojans e spyware. Ele ajuda a manter os sistemas protegidos contra malware e a garantir a integridade dos dados.

Sistema de Detecção de Intrusão em Rede (IDS): O IDS monitora o tráfego de rede em busca de atividades suspeitas ou padrões de comportamento maliciosos. Ele é capaz de identificar possíveis ameaças e alertar os administradores para ações corretivas.

Backups: Os backups são essenciais para garantir a disponibilidade e a integridade dos dados em caso de perda ou corrupção. Realizar backups regularmente e armazená-los de forma segura é uma prática fundamental para a recuperação de dados em situações de emergência.

Esses elementos, quando implementados de forma integrada e em conjunto com outras práticas de segurança, contribuem significativamente para proteger uma rede de computadores contra ameaças e garantir a continuidade das operações.

Outro aspecto importante é a criação de políticas de segurança claras e atualizadas, que devem ser comunicadas regularmente aos colaboradores. Treinamentos e simulações de ataques também são fundamentais para garantir a conscientização e preparação da equipe para lidar com possíveis incidentes de segurança.

https://www.mundodigital.net.br/desafios-e-ameacas-ciberneticas-em-redes-de-computadores/ data da pesquisa 5/4/2024.

4 ESTRATÉGIAS IMPORTANTES PARA UMA IMPLEMENTAÇÃO EFICAZ DE INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS:

A inteligência de ameaças cibernéticas, desempenha um papel crucial na segurança cibernética, fornecendo informações valiosas sobre ameaças em potencial, permitindo que as organizações se preparem e respondam de forma eficaz a incidentes de segurança. A seguir citamos algumas estratégias importantes para uma implementação eficaz de Inteligência de Ameaças Cibernéticas:

Estabelecer uma estrutura organizacional: Definir papéis e responsabilidades claros dentro da organização é fundamental para garantir que a inteligência de ameaças cibernéticas seja coletada, analisada e compartilhada de forma eficaz.

Coleta e análise de dados: É importante reunir informações de várias fontes, incluindo feeds de inteligência de ameaças, análise de vulnerabilidades, padrões de tráfego de rede, entre outros. Análise detalhada dos dados coletados ajudará a identificar possíveis ameaças e a antecipar potenciais ataques.

Compartilhamento de informações: Colaborar com outras organizações e entidades do setor para compartilhar informações de inteligência de ameaças é essencial para obter insights mais abrangentes e fortalecer a postura de segurança cibernética.

Implementar soluções de automação: Utilizar ferramentas de automação para coleta, análise e correlação de dados de inteligência de ameaças pode acelerar o processo de identificação de ameaças e melhorar a tomada de decisão.

Integração com medidas de segurança existentes: A inteligência de ameaças cibernéticas deve ser integrada às soluções de segurança existentes, como firewalls, sistemas de detecção de intrusão e prevenção de intrusões (IDPS), para fortalecer as defesas da organização.

Avaliação contínua e adaptação: As estratégias de inteligência de ameaças cibernéticas devem ser avaliadas regularmente para garantir que estejam alinhadas com as necessidades e ameaças em constante evolução. A

capacidade de adaptação é essencial para manter a eficácia da estratégia de CTI. (Brown, 2024).

5 SEGURANÇA EM REDES DE COMPUTADORES

A segurança de informação em redes diz respeito às práticas e medidas adotadas para proteger os dados e a comunicação que ocorre em redes de computadores. Isso inclui a prevenção de acessos não autorizados, a proteção contra ataques cibernéticos, a garantia da confidencialidade, integridade e disponibilidade dos dados, bem como a autenticação dos usuários e dispositivos para garantir que apenas indivíduos autorizados tenham acesso às informações. A segurança de informação em redes envolve a implementação de firewalls, antivírus, criptografia, chaves criptográficas, chave simétrica e assimétrica .

5.1 CRIPTOGRAFIA

Criptografia palavra vinda do grego “kryptós” e “gráphein”, que significa respectivamente “escondido” e “escrita”, portanto, escrita oculta (Duly, apud Machado 2021). A criptografia ou o ato da escrita oculta, é o termo utilizado para a codificação de uma mensagem. Segundo Nakamura e Geus (2017), a codificação é a ciência de manter as mensagens seguras. Logo, esse método pode embaralhar caracteres e também substituí-los por outros, tanto por letras quanto por números aleatórios, para que a mensagem se torne não entendível, caso haja um acesso não esperado.

5.2 Chaves criptográficas

Em criptografia, “chaves” é um termo similar a senha, que é utilizado como forma de prevenção contra ataques mal-intencionados a arquivos e mensagens salvos no sistema (DOCUSIGN., 2019) . A criptografia faz uso de dois tipos de chaves, no qual são elas: simétricas e assimétricas.

5.3 Chave simétrica

A criptografia de chave simétrica, também chamada de criptografia de chave privada, é um método responsável pelo sigilo das informações, que faz uso de uma única chave secreta, para codificar e decodificar dados fornecidos (Duly, apud NAKAMURA 2021).

Conforme o (CERT, 2017), “a criptografia de chave simétrica, quando comparado com a de chaves assimétricas, é a mais indicada para garantir a confidencialidade de grandes volumes de dados, pois seu processamento de dados é mais rápido”. Contudo, com o uso dessa chave deve-se manter cuidado, pois, a chave precisa ser previamente compartilhada entre a origem e o destino antes de estabelecer o meio de criptografia. Logo, é importante saber que durante o processo de compartilhamento essa chave pode ser interceptada pelo atacante (MACHADO, 2019). Outro problema relacionado a esta chave é a não permissão do uso da assinatura digital e do certificado digital, podendo colocar o usuário em situação de perda de integridade, autenticidade e repúdio.

5.4 Chave assimétrica

A criptografia de chave assimétrica, também conhecida como criptografia de chave pública, é diferenciada da chave simétrica pelo uso de um par de chaves, sendo uma dessas chaves pública e a outra privada. Logo, outro diferencial dessa chave em relação a chave simétrica, é a possibilidade do uso da assinatura digital e do certificado digital, fazendo com que a garantia da integridade, autenticidade e o não repúdio sejam maiores.

CAPÍTULO VI: MAPEAMENTO DOS TRABALHOS RELACIONADOS.

6. processo de revisão da sistemática

A função de realizar um estudo da arte ou fazer um mapeamento sistemático da literatura nesta área, é buscar uma compilação abrangente de estudos e pesquisas relevantes, esta revisão pode ajudar a establecer diretrizes e boas práticas para a proteção das redes de computadores e os dados dos usuários.

Um estudo sistemático ou metanálise é um método estatístico que busca combinar e sintetizar dados de várias pesquisas independentes para responder uma pergunta de pesquisa específica. Ela envolve a análise de dados primários de diversas fontes para formular uma resposta ou uma nova hipótese. (- Borenstein, 2011).

O processo de mapeamento sistemático, por sua vez, é uma abordagem sistemática que busca identificar, avaliar e resumir as evidências disponíveis em uma determinada área de pesquisa. A ideia é criar um mapa das informações existentes para entender as lacunas existentes no conhecimento e orientar futuras investigações. (- Petticrew, 2006).

6.1 O processo de mapeamento sistemático estará dividido em três etapas:

- ✓ Planejamento e construção do protocolo;
- ✓ Seleção de critérios de inclusão e exclusão;
- ✓ Escrita dos resultados da revisão;

6.1.1 planejamento e construção do protocolo.
Justificativa da necessidade.

A implementação de políticas de segurança em redes de computadores é fundamental devido ao aumento constante das ameaças cibernéticas que visam comprometer a integridade, confidencialidade e disponibilidade de dados e sistemas. Sem políticas e medidas de segurança adequadas, as organizações correm o risco de serem alvos de ataques cibernéticos, resultando em perda de informações sensíveis, danos à reputação e prejuízos financeiros significativos.

3.1.2 objetivo e questões de pesquisa.

O objetivo desta pesquisa é analisar e propor abordagens eficazes para a implementação de políticas de segurança em redes de computadores, com o intuito de proteger dados e sistemas contra ameaças cibernéticas. Desta forma,

busca-se contribuir para a criação de ambientes de rede mais seguros e resilientes, capazes de enfrentar e mitigar os desafios impostos pelo cenário de ameaças digitais em constante evolução.

Com base neste objetivo, foram definidas as questões de pesquisa (qpe):

QP 1 Quais são as principais ameaças cibernéticas enfrentadas pelas redes de computadores atualmente e como essas ameaças evoluíram ao longo do tempo?

QP2: Quais são os princípios fundamentais das políticas de segurança em redes de computadores e como elas podem ser adaptadas para enfrentar novos desafios de segurança cibernética?

QP3. Quais são as melhores práticas e abordagens recomendadas para implementar e manter políticas de segurança eficazes em ambientes de rede complexos e dinâmicos?

QP4. Como a conformidade e a auditoria de segurança podem ser integradas às políticas de segurança de rede para garantir a conformidade regulatória e a eficácia das medidas de segurança implementadas?

3.1.3 string de busca e base de pesquisa

A busca de artigos relacionados ao nosso tema foi feita mediante as seguintes;

"Network security" AND "Cybersecurity policies" "Computer network security" AND "Effective security measures" "Data protection" AND "Network security implementation" *"Cyber threats" AND "Security policy enforcement" "Information security" AND "Network defense strategies"*

Essas strings ajudaram Para encontrar artigos relacionados ao tema "Implementação de Políticas de Segurança em Redes de Computadores: Abordagens Eficazes para Proteger Dados e Sistemas contra Ameaças Cibernéticas" em bases de dados acadêmicas.

A busca foi feita em 3 bases de dados diferentes, as mesmas são apresentadas na tabela1.

Escolhemos essas plataformas porque deram melhores resultados na busca de trabalhos relacionados ao nosso tema.

Tabela 1

Bases de dados	Url
Google scholar	Https://scholar.google.com.br/
Acm	Https://dl.acm.org/
Ieee	Https://ieeexplore.org/xplore/home.jsp

3.1.4 seleção e execução

Encontramos 30 artigos, para reduzir esse numero na etapa 1 removemos os duplicados, em seguida atendemos os artigos que atenderam os seguintes critérios:

Critérios de avaliação dos artigos.

Critérios de inclusão:

Relevância do estudo para o tema em questão, ou seja, se o artigo trata especificamente da implementação de políticas de segurança em redes de computadores e proteção contra ameaças cibernéticas.

Utilização de abordagens eficazes e práticas para proteger dados e sistemas.

Métodos e técnicas utilizados para a implementação das políticas de segurança.

Ano de publicação - dependendo da atualidade e relevância dos dados.

Critérios de exclusão:

Estudos que não abordam diretamente o tema das políticas de segurança em redes de computadores e proteção de dados contra ameaças cibernéticas.

Artigos duplicados ou com informações redundantes.

Estudos desatualizados ou obsoletos que não refletem as práticas modernas de segurança cibernética.

Na segunda etapa, analisamos manualmente o titulo e o resumo dos 23 artigos resultantes da etapa 1 e removemos os que não atendem os critérios acima listados.

Na etapa 3 revisamos 19 artigos e selecionamos 14 artigos que se encontram na tabela 2.

3.1.5 escrita dos resultados da revisão.

Tabela 2

Trabalhos
1- 27001, I. (2013). *Information technology — Security techniques — Information security management systems — Requirements.*
2 Laudon, K. C. (p 5 , 2021). *Management Information Systems: Managing the Digital Firm. Pearson.*
3. Borenstein, M. H. (2011). *Introduction to meta-analysis. John Wiley & Sons.*
4. Brown, C. &. (2024). *Cyber Threat Intelligence: Strategies for Effective Implementation.*
5 CERT. (2017). *Criptografia de chave simétrico e de chaves assimétricas. In: CERT. Criptografia. CERT.br*
6. DOCUSIGN. (2019). *Quando a criptografia deve ser usada?.*
7. Duly. (apud Machado 2021). *MACHADO, Felipe Nery Rodrigues. Segurança da informação: Princípios e Controle de Ameaças*
8- Petticrew, M. &. (2006). *Systematic reviews in the social sciences: A practical guide. John Wiley & Sons*
9. Duly. (apud NAKAMURA 2021). *Segurança de Redes em ambientes cooperativos.*
10 Brown, C., & Lee, D. (2024). "Cyber Threat Intelligence: Strategies for Effec tive Implementation.
11. Thomas, R., & Park, C. (2022). "Endpoint Security in Remote Work Envi ronments: Challenges and Solutions.

12 . Liu, X., & Nguyen, H. (2023). "Security Orchestration in Network Environments: Best Practices.
13 Adams, K., & Zhao, W. (2023). "Ransomware Defense Strategies for Critical Infrastructure Networks."
14 Garcia, M., & Patel, S. (2024). "Securing IoT Devices in Network Environments: Challenges and Solutions.

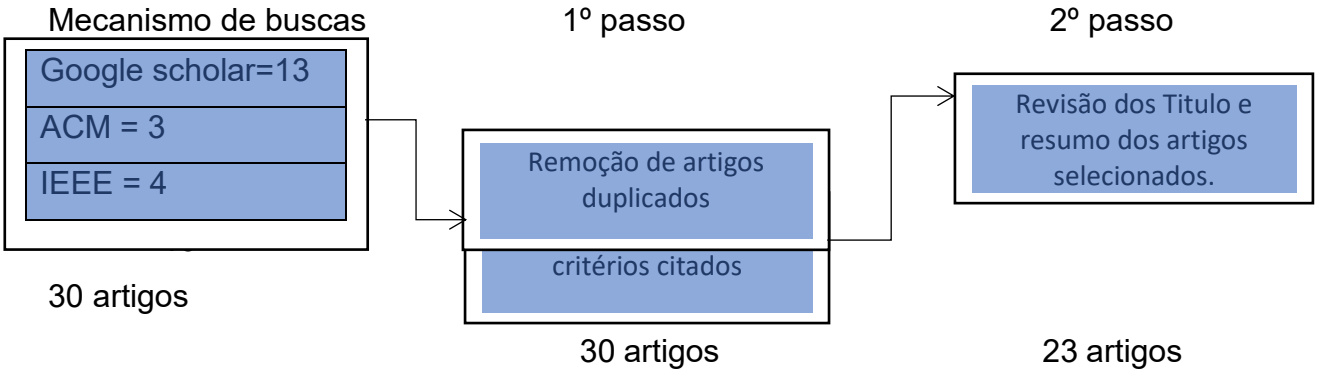

Fig 1: processo empregado para localizar localizar e selecionar os artigos analisados nesta pesquisa.

3.1.5 CLASSIFICAÇÃO DOS ARTIGOS.

Os artigos podem ser classificados com base na abordagem utilizada para proteger dados e sistemas contra ameaças cibernéticas. Alguns artigos se concentram em técnicas de criptografia, enquanto outros abordam a detecção de anomalias de segurança ou práticas de gestão de riscos.

Tecnologias Utilizadas: Alguns artigos classificam as políticas de segurança com base nas tecnologias específicas que são empregadas, como firewalls, antivírus, sistemas de prevenção de intrusões, entre outros.

Nível de Proteção: Artigos também são classificados com base no nível de proteção que as políticas de segurança visam oferecer. Isso pode incluir desde medidas básicas de segurança cibernética até estratégias de defesa avançadas.

3.1.6 PRINCIPAIS ASPECTOS DAS ABORDAGENS DO TEXTO.

No texto sobre "Implementação de Políticas de Segurança em Redes de Computadores: Abordagens Eficazes para Proteger Dados e Sistemas contra Ameaças Cibernéticas", os principais aspectos das abordagens incluiem:

Identificação de Ameaças Cibernéticas: As abordagens podem abordar a importância de identificar e compreender as diversas ameaças existentes no cenário cibernético, tais como malware, phishing, ransomware, entre outros.

Implementação de Medidas de Controle: Descrever como as políticas de segurança podem incluir a implementação de medidas de controle, como firewalls, sistemas de detecção de intrusões, criptografia e autenticação multifatorial.

Gestão de Acesso e Privilégios: Destacar a necessidade de uma adequada gestão de acesso e privilégios dos usuários dentro da rede, visando limitar o acesso aos recursos e dados sensíveis.

Monitoramento e Resposta a Incidentes: Abordar a importância do monitoramento contínuo da rede e da capacidade de resposta a incidentes, incluindo a investigação de possíveis violações de segurança e ações corretivas imediatas.

Atualização e Treinamento Constantes: Enfatizar a importância da atualização regular das políticas de segurança, dos softwares e do treinamento contínuo dos usuários para conscientização sobre práticas seguras na utilização da rede.

Esses são alguns dos principais aspectos que podem ser abordados nas diferentes abordagens propostas para proteger dados e sistemas contra ameaças cibernéticas, visando garantir a integridade, confidencialidade e disponibilidade das informações na rede de computado

3.1.7 TRABALHOS RELACIONADOS

O artigo "Segurança de Redes em Ambientes Cooperativos" de Nakamura (2021) trata da importância e das estratégias relacionadas à segurança cibernética em ambientes onde diferentes entidades colaboram e compartilham recursos de rede. O autor discute questões como proteção contra ameaças cibernéticas, controle de acessos e outras práticas para garantir a segurança da informação nesses ambientes. Sobre o livro "Management Information Systems: Managing the Digital Firm" de Laudon (2021), que discute sistemas de informação de gestão, há uma clara interseção com o tema de segurança de redes em ambientes cooperativos. A segurança da informação é um componente fundamental dos sistemas de informação de gestão, e a discussão entre os

autores poderia explorar como a segurança cibernética influencia a gestão da informação em ambientes digitais. No livro "Introduction to Meta-Analysis" de Borenstein (2011), que aborda a meta-análise como uma técnica de síntese estatística de evidências de pesquisa, poderia haver uma discussão interessante sobre a análise de dados relacionados à segurança cibernética em redes cooperativas. A meta-análise poderia ser aplicada para combinar resultados de estudos sobre estratégias de segurança cibernética eficazes em ambientes colaborativos. O livro "Cyber Threat Intelligence: Strategies for Effective Implementation" de Brown (2024) oferece insights sobre estratégias para lidar com ameaças cibernéticas, o que poderia complementar o conteúdo discutido no artigo de Nakamura. Uma discussão entre os autores poderia explorar como as estratégias de inteligência de ameaças cibernéticas podem ser aplicadas para melhorar a segurança de redes em ambientes cooperativos. Em relação ao livro "Systematic Reviews in the Social Sciences: A Practical Guide" de Petticrew (2006), que fornece orientações sobre a realização de revisões sistemáticas em ciências sociais, uma discussão poderia explorar a importância da abordagem sistemática na avaliação de estratégias de segurança cibernética em redes colaborativas. A aplicação de métodos rigorosos de revisão sistemática poderia contribuir para a identificação e análise de melhores práticas em segurança de redes em contextos cooperativos.

3.1.8 Análise comparativa dos artigos selecionados.

A tabela a seguir mostra um resumo dos trabalhos correlatos Técnicas de de classificação utilizadas: nome dos autores e ano, tipo de pesquisa, metodologia, domínio.

Trabalho	Domínio	Metodologia	Tipo de pesquisa
27001 (2013)	Segurança de informação	Revisão teorica	Não especificada
Laudon k, c Jane p (2021)	Gestão da informação digital	Revisão teorica	Gestão de sistemas de informação

Borenstein ,M,et al(2011)	Segurança	Revisão bibliográfica	Metanálise
S. 27032 (2014)	Segurança em ti	Revisão bibliográfica	relatório
Cert(2022)	Criptografia e Segurança	Revisão bibliográfica.	Relatório
Docusign (2018)	Segurança de documentos eletronicos	Revisão bibliográfica	Prática de segurança

3.1.9 Respostas das questões de pesquisa

Na presente seção será abordado as respostas as questões de pesquisa definidas na subseção

RQ1: As principais ameaças cibernéticas enfrentadas pelas redes de computadores atualmente incluem malware, ataques de phishing, ransomware, ataques de negação de serviço (DDoS), ataques de engenharia social, vulnerabilidades de software e hardware, violações de dados e espionagem cibernética. Essas ameaças evoluíram ao longo do tempo devido ao avanço da tecnologia, mudança de comportamento dos cibercriminosos, aumento da conectividade e complexidade das redes, e novas vulnerabilidades que surgem com o uso de dispositivos IoT e a computação em nuvem.

RQ2: Os princípios fundamentais das políticas de segurança em redes de computadores incluem a confidencialidade, integridade, disponibilidade e autenticidade dos dados e sistemas. Essas políticas podem ser adaptadas para enfrentar novos desafios de segurança cibernética por meio da atualização constante das medidas de segurança, implementação de controles de acesso

adequados, educação e conscientização dos usuários, monitoramento contínuo dos sistemas e investimento em tecnologias de segurança avançadas.

RQ3: As melhores práticas e abordagens recomendadas para implementar e manter políticas de segurança eficazes em ambientes de rede complexos e dinâmicos incluem a segmentação de rede, atualização regular de sistemas e software, implementação de controles de acesso baseados em funções, monitoramento de tráfego em tempo real, autenticação multifatorial, backup e recuperação de dados, além de treinamento regular dos usuários em segurança cibernética.

RQ4: A conformidade e a auditoria de segurança podem ser integradas às políticas de segurança de rede por meio da definição de padrões de conformidade específicos, realização de avaliações de risco regulares, implementação de controles de segurança para atender aos requisitos regulatórios, auditorias internas e externas, registro e análise de logs de segurança, e ações corretivas imediatas em caso de violações de conformidade. Essas medidas garantem a conformidade regulatória e a eficácia das medidas de segurança implementadas na rede.

Resultado

A discussão entre os autores resulta em uma abordagem mais abrangente e integrada sobre a segurança cibernética em ambientes cooperativos. Ao combinar as perspectivas de diferentes especialistas, como a gestão de sistemas de informação, análise de dados, as estratégias de inteligência de ameaças cibernéticas e as revisões sistemáticas, os autores colaboram com as suas ideias para identificação de lacunas, desafios e oportunidades no campo da segurança de redes em contextos colaborativos. Os resultados desta discussão incluem insights sobre melhores práticas para implementar efetivamente estratégias de segurança cibernética, considerando as especificidades e complexidades dos ambientes cooperativos.

Conclusão

A implementação de políticas de segurança em redes de computadores é uma medida essencial para proteger dados e sistemas contra ameaças cibernéticas. Através de abordagens eficazes, é possível mitigar os riscos e garantir a integridade, confidencialidade e disponibilidade das informações. Uma política de segurança bem elaborada inclui uma combinação de práticas, tecnologias e treinamento adequado para os usuários. A adoção de firewalls, antivírus, criptografia e controle de acesso são exemplos de medidas técnicas que podem ser implementadas. Além disso, é necessário desenvolver políticas claras de senhas, realizar backup regularmente e manter sistemas e softwares atualizados para evitar vulnerabilidades. No entanto, é importante ressaltar que a segurança em redes de computadores é um desafio constante, uma vez que as ameaças cibernéticas estão sempre em evolução.

Referências

- Borenstein, M. H. (2011). *Introduction to meta-analysis. John Wiley & Sons.*

- Petticrew, M. &. (2006). *Systematic reviews in the social sciences: A practical guide. John Wiley & Sons.* 258554441589/

27001, I. (2013). *Information technology — Security techniques — Information security management systems — Requirements.*

Brown, C. &. (2024). *Cyber Threat Intelligence: Strategies for Effective Implementation.*

CERT. (2017). *Criptografia de chave simétrico e de chaves assimétricas. In: CERT. Criptografia. CERT.br, 16 mar. 2017. Disponível em: https://cartilha.cert.br/criptografia/.*

DOCUSIGN. (2019). *Quando a criptografia deve ser usada?. [S. l], 11 fev.2019. Disponível https://www.docusign.com.br/blog/criptografia-o-que-e-e-quando-ela-deve-ser-usada#:~.*

Duly. (apud Machado 2021). *MACHADO, Felipe Nery Rodrigues. Segurança da informação: Princípios e Controle de Ameaças. 1. ed. SP-Brasil: Beatriz M. Carneiro, 2014. 176 p. ISBN.*

Duly. (apud NAKAMURA 2021). *Segurança de Redes em ambientes cooperativos. 2. ed. SP-Brasil: Futura, 2007. 483 p. ISBN 978-85-7522-136-5.*

Laudon, K. C. (p 5 , 2021). *Management Information Systems: Managing the Digital Firm. Pearson.*