RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

DESAFIOS NA GESTÃO DA SEGURANÇA CIBERNÉTICA: O PAPEL ESTRATÉGICO DO GESTOR DE TECNOLOGIA NA ERA DA COMPUTAÇÃO EM NUVEM

CHALLENGES IN CYBERSECURITY MANAGEMENT: THE STRATEGIC ROLE OF THE TECHNOLOGY MANAGER IN THE ERA OF CLOUD COMPUTING

DESAFÍOS EN LA GESTIÓN DE CIBERSEGURIDAD: EL ROL ESTRATÉGICO DEL GESTOR DE TECNOLOGÍA EN LA ERA DE LA COMPUTACIÓN EN LA NUBE

Jonathan Messias Santos[1], Felipe Alexandre Cardoso Pazinatto[2], Luiz Egidio Costa Cunha[3]

e5105665
https://doi.org/10.47820/recima21.v5i10.5665

PUBLICADO: 10/2024

RESUMO

A transformação digital impulsionou a comunicação instantânea e a adoção da *cloud computing*, mas também trouxe consigo um aumento nas ameaças cibernéticas, com destaque para o *ransomware*. Apesar dos avanços tecnológicos, a segurança da informação enfrenta desafios significativos, especialmente no ambiente de nuvem, onde uma parcela considerável das falhas é atribuída aos próprios clientes. Nesse contexto, destaca-se a importância de integrar o Plano de Continuidade de Negócios (PCN) com estratégias de proteção digital. O PCN oferece uma camada adicional de defesa, auxiliando na prevenção, detecção e resposta a incidentes, e, assim, fortalece a resiliência das organizações. A partir de uma análise bibliográfica e de dados relevantes sobre segurança digital, *ransomware*, computação em nuvem e PCN, este artigo visa evidenciar a importância da proteção de dados no cenário de transformação digital e adoção do ambiente de armazenamento em nuvem. Além disso, enfatiza a necessidade de combinar o PCN com medidas de segurança para aumentar a resistência das organizações contra ameaças como o *ransomware*

PALAVRAS-CHAVE: Computação em nuvem. Gestão estratégica de TI. Plano de continuidade de negócios.

ABSTRACT

Digital transformation has accelerated instant communication and the adoption of cloud computing, but it has also brought an increase in cyber threats, with ransomware being a notable concern. Despite technological advances, information security faces significant challenges, especially in the cloud environment, where a considerable portion of failures is attributed to the clients themselves. In this context, the importance of integrating the Business Continuity Plan (BCP) with digital protection strategies becomes evident. The BCP provides an additional layer of defense, aiding in the prevention, detection, and response to incidents, thus enhancing organizational resilience. Based on a bibliographic review and relevant data on digital security, ransomware, cloud computing, and BCP, this article aims to highlight the importance of data protection in the context of digital transformation and cloud adoption. Furthermore, it emphasizes the need to combine the BCP with security measures to increase organizations' resistance to threats such as ransomware.

KEYWORDS: *Cloud Computing. Strategic IT Management. Business Continuity Plan.*

RESUMEN

La transformación digital ha impulsado la comunicación instantánea y la adopción de la computación en la nube, pero también ha traído consigo un aumento en las amenazas cibernéticas, destacando el ransomware. A pesar de los avances tecnológicos, la seguridad de la información enfrenta desafíos significativos, especialmente en el entorno de la nube, donde una parte considerable de las fallas se

[1] Graduado em Gestão Empresarial com Ênfase em Sistemas da Informação, com MBA em Gestão da Segurança da Informação e pós-graduação em Gestão da Tecnologia da Informação.
[2] Graduado em Tecnologia em Processamento de Dados, com especialização em Sistemas de Informação, mestrado em Ciência da Computação e doutorado em Engenharia Biomédica.
[3] Graduado em Processamento de Dados, com pós-graduações em Análise de Sistemas, Avaliação e Educação, além de treinamento em B2B na Alemanha e mestrado em Ciência, Tecnologia e Sociedade.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

atribuye a los propios clientes. En este contexto, destaca la importancia de integrar el Plan de Continuidad de Negocios (PCN) con estrategias de protección digital. El PCN proporciona una capa adicional de defensa, ayudando en la prevención, detección y respuesta a incidentes, y así, fortalece la resiliencia de las organizaciones. Basado en una revisión bibliográfica y en datos relevantes sobre seguridad digital, ransomware, computación en la nube y PCN, este artículo tiene como objetivo resaltar la importancia de la protección de datos en el contexto de la transformación digital y la adopción de la nube. Además, enfatiza la necesidad de combinar el PCN con medidas de seguridad para aumentar la resistencia de las organizaciones frente a amenazas como el ransomware.

***PALABRAS CLAVE**: Computación en la Nube. Gestión Estratégica de TI. Plan de Continuidad de Negocios.*

INTRODUÇÃO

Com o avanço tecnológico, a velocidade e a praticidade tornaram-se essenciais nas comunicações do dia a dia. Desde o declínio das cartas físicas até a era das mensagens instantâneas em dispositivos móveis, a demanda por informações precisas e instantâneas cresceu exponencialmente. Esse cenário reflete a importância crescente da informação, especialmente para as empresas, onde a rapidez e a precisão na comunicação são fatores cruciais para a competitividade em todos os setores.

O início do Século XXI marcou uma crescente utilização de *smartphones* e *tablets*, impulsionados pela infraestrutura de banda larga sem fio. Esse cenário desencadeou uma nova transformação no setor de tecnologia da informação e comunicação, resultando no surgimento de novos modelos de negócios, focados na oferta de serviços aos usuários e na comercialização de publicidade direcionada exclusivamente para nichos de mercado. A computação em nuvem *(cloud computing)* emergiu como uma resposta a essa tendência, disponibilizando toda a infraestrutura e informações digitalmente na Internet, abrangendo desde aplicativos de *software* até ferramentas de busca, redes de comunicação, provedores e centros de armazenamento e processamento de dados. No entanto, é crucial ressaltar que existem riscos associados, especialmente relacionados à segurança e à proteção dos dados (TIGRE; NORONHA, 2013).

Este artigo tem como objetivo demonstrar a relevância de integrar um PCN com medidas de segurança cibernética no contexto da computação em nuvem. Tal integração fortalece a resiliência da organização e ajuda a mitigar ameaças, como *malware* e, especificamente, *ransomware*, que podem impactar diretamente a continuidade dos negócios.

FUNDAMENTAÇÃO TEÓRICA

O aumento do uso de *smartphones* para compras, interações em mídias sociais, transações *online* e compartilhamento de dados com plataformas digitais, despertou o interesse de empresas, organizações governamentais e não governamentais, bem como de indivíduos mal-intencionados, que veem nesses dados e informações uma valiosa matéria-prima para seus negócios, seja de forma

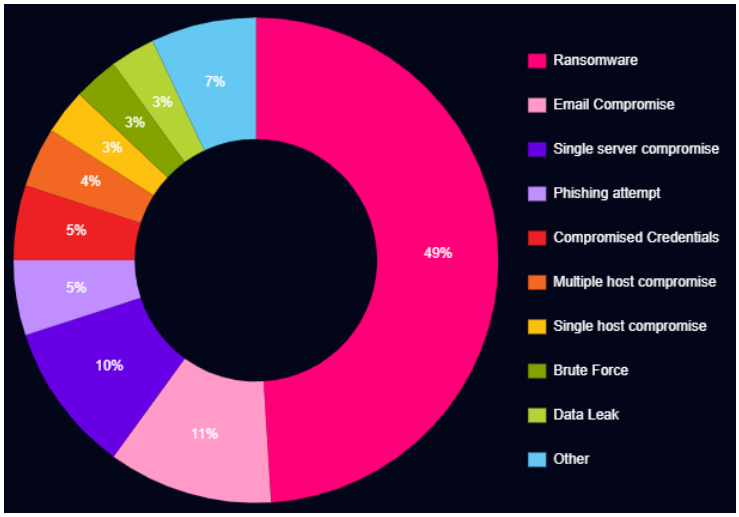
RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

lícita ou ilícita. Esse interesse é impulsionado pelo fato de que praticamente todas as atividades cotidianas estão agora interligadas à internet.

Segundo informações divulgadas em 2023 pela *Check Point Software's*, que é uma empresa especializada em soluções de cibersegurança, os ataques cibernéticos globais aumentaram em 38% em 2022 em comparação com 2021. Para Horowitz (2023), esse crescimento substancial no mercado de credenciais e *cookies* roubados está intimamente ligado à evolução contínua do ciclo de vida dos intermediários de acesso, afiliados de *ransomware* e fornecedores de *Robots as a Service* (RaaS). Como resultado, observou-se um aumento significativo na popularidade dos *infostealers*, que são *malware* projetados para roubar informações confidenciais de computadores comprometidos. Ainda de acordo com Horowitz (2023), há uma tendência crescente no uso desses *infostealers*, afetando 18% das redes corporativas em 2020, 21% em 2021 e chegando a 24% de todas as organizações em 2022. Esse fenômeno está diretamente correlacionado ao crescimento do mercado de *ransomware (*HOROWITZ, 2023).

Dentre os principais tipos de *malware* estão os vírus, cavalos de Troia *(trojans*), *ransomware*, *backdoors*, *worms*, *bots*, *spyware e rootkits* (CERT.BR, 2023). Conforme pode ser visto na figura 1, o *ransomware* destaca-se como uma ameaça particularmente significativa devido ao seu crescimento exponencial em popularidade. Sua operação geralmente começa com a exploração de uma pequena vulnerabilidade no dispositivo da vítima. Uma vez infectado, se esse dispositivo estiver conectado a outros na rede, os invasores podem explorar novas vulnerabilidades, causando um efeito cascata e infectando mais dispositivos. O termo *ransomware* deriva da palavra inglesa *ransom*, que significa resgate pago por algo ou alguém que foi sequestrado. Neste caso, os dados das vítimas são sequestrados, ilustrando o *modus operandi* desse tipo de *malware*.

Figura 1. Distribuição de casos por indicação inicial de ameaça em 2022



Fonte: Horowitz, 2023

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

O *ransomware*, segundo Garrett (2021), foi criado para restringir ou limitar o acesso do usuário aos seus próprios dados, exigindo um pagamento/resgate para liberá-los. Essa categoria de *malware* tornou-se cada vez mais sofisticada e disseminada, acarretando prejuízos significativos tanto para empresas quanto para indivíduos. Geralmente, manifesta-se em formas como *locker ransomware*, que bloqueia totalmente o acesso ao computador exibindo uma tela de bloqueio, e *crypto-ransomware*, que criptografa arquivos importantes no sistema do usuário. (ROMAR; SILVA, 2022).

Um relatório do FBI (2021) revelou que os prejuízos totais causados pelo *ransomware* chegaram a US$ 49,2 milhões, com a expectativa de aumento à medida que esse tipo de *malware* continua a evoluir. Devido à sua natureza distinta e rápida adaptação, o *ransomware* apresenta enormes desafios para as abordagens tradicionais de detecção, dificultando significativamente a identificação e a resposta eficaz. (BAIG *et al*., 2012)

No entanto, mesmo com os avanços tecnológicos e as promessas de segurança das empresas e provedores de serviços em nuvem, é evidente que todos enfrentam riscos e desafios significativos na área de segurança cibernética. Muitos clientes erroneamente acreditam que, ao migrar para a nuvem, estarão automaticamente protegidos. Essa ideia é muitas vezes sugerida pelos fornecedores e provedores de serviços em nuvem, porém, até mesmo as empresas de tecnologia mais renomadas não estão imunes a problemas de segurança. Basta uma rápida pesquisa na internet para encontrar numerosos relatos de ataques de *ransomware* que deixaram a *Cloud A* ou *Cloud B* inoperantes.

Até mesmo empresas especializadas em cibersegurança estão suscetíveis a esse tipo de ataque, uma vez que o *ransomware* está em constante evolução em suas táticas, e pode se beneficiar do fator humano. Mesmo com todos os protocolos de segurança implementados e configurações corretas, ainda assim pode haver vulnerabilidades. Como foi o caso da *Ativy Digital* que é referência em nuvem na América Latina, com mais de 20.000 usuários gerenciados nas plataformas de cloud pública, privada e híbrida que em 28/03/2023 sofreu um ataque *ransomware* causando indisponibilidade de todos seus serviços afetando os mais de 20.000 usuários (LOBO, 2023). À medida que os provedores expandem sua oferta de serviços, uma única configuração incorreta pode abrir brechas significativas para novos ataques. Mesmo diante de todas as precauções, as violações de dados persistem, seja por ataques diretos, vazamentos acidentais ou outras vulnerabilidades.

De acordo com Panetta (2019), até 2025, 99% das falhas de segurança na *Cloud Computing* serão atribuídas aos clientes. Isso significa que a maioria dos problemas de segurança relacionados à nuvem será resultado de ações ou decisões tomadas pelos próprios usuários e organizações que utilizam os serviços.

O cenário atual, marcado por ameaças como o *ransomware*, demanda que as empresas estejam preparadas para enfrentar os desafios da segurança cibernética. O relatório *America's Data*

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Held Hostage: *Case Studies in Ransomware* Attacks *on American Companies* ilustra como os ataques de *ransomware* podem ter consequências devastadoras para as organizações, resultando na perda de dados críticos e na interrupção dos negócios.

O gestor de tecnologia desempenha um papel crucial na resposta a esses desafios. Para Silva (2013), anteriormente associado a um perfil mais técnico, o gestor de tecnologia agora incorpora características de um "homem de negócios", sendo sua responsabilidade garantir a otimização dos custos, a redução dos riscos na adoção de tecnologias e a integração entre o negócio e novas tendencias tecnológicas. Uma vez que a contratação de uma Solução *Cloud Computing* envolve riscos e adoção de novas tecnologias, o gestor tem a responsabilidade de definir uma estratégia de segurança cibernética alinhada aos objetivos da empresa. Isso inclui a escolha de ferramentas, políticas e procedimentos para proteger os dados, avaliação dos riscos, implementação de medidas de segurança, realização de treinamentos e conscientização de todo o pessoal, monitoramento contínuo e, principalmente, ter em mãos um bom PCN.

Além dessas responsabilidades, é crucial reconhecer que a segurança cibernética se tornou um elemento vital para o sucesso operacional de qualquer empresa. Conforme delineado pela ISO 22301 (2019), o PCN desempenha um papel fundamental na garantia da resiliência das operações da organização em face de incidentes que possam interromper suas atividades normais.

Ladeira (2021) define o PCN como um processo interativo desenvolvido para identificar as funções críticas do negócio, bem como as políticas, processos, planos e procedimentos essenciais para garantir a continuidade das operações da organização diante de eventos e imprevistos. Em resumo, o PCN visa assegurar que a empresa possa manter suas atividades mesmo diante de situações adversas seja ela causa por fatores internos ou externos.

Para D'Addario (2023), o PCN, é um elemento essencial da Gestão de Riscos Empresariais, concebido para prevenir, preparar e responder eficazmente a situações disruptivas que possam desencadear crises ou desastres. Composto por uma variedade de estratégias, acordos e arranjos, o PCN visa garantir a manutenção da operação mesmo diante de eventos adversos como de um ataque *ransomware*. A Gestão da Continuidade de Negócios desempenha um papel fundamental na governança corporativa e na gestão de riscos, influenciando diretamente a resiliência organizacional. A capacidade de uma empresa de lidar com adversidades pode determinar seu nível de risco, percebido pelos investidores e clientes. Em avaliações de fornecedores, o PCN pode ser um diferencial crucial, pesando na decisão final de compra (D'ADDARIO, 2023).

O PCN pode atuar como uma camada adicional de proteção, fornecendo um conjunto de procedimentos específicos para lidar com interrupções nos negócios causadas por ataques cibernéticos. Ao integrar o PCN com medidas de prevenção, detecção e resposta a incidentes, as organizações podem criar uma abordagem mais abrangente e eficaz para garantir a resiliência contra ameaças cibernéticas. Em termos de prevenção, o PCN pode ajudar as organizações a identificarem e mitigarem potenciais vulnerabilidades que poderiam ser exploradas por cibercriminosos (ISO

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

22301, 2019). Por exemplo, ao analisar os processos de negócios e as dependências de sistemas críticos, as equipes responsáveis pela segurança podem identificar pontos de falha e implementar controles adequados para reduzir o risco de ataques.

Na detecção de incidentes, o PCN pode definir protocolos claros para o monitoramento contínuo de sistemas e redes, permitindo que as equipes de segurança identifiquem rapidamente atividades suspeitas ou anômalas que possam indicar um ataque em andamento. Isso pode incluir a implementação de sistemas de detecção de intrusões, análise de registros de atividades e uso de ferramentas de análise de segurança cibernética (PAK, 2024).

Para Ricadela (2024), quando se trata de resposta a incidentes, o PCN pode fornecer um roteiro detalhado para lidar com ataques cibernéticos, incluindo procedimentos para isolar sistemas comprometidos, restaurar *backups* de dados, comunicar-se com partes interessadas relevantes e acionar autoridades competentes, conforme necessário. Ter um plano estruturado e bem documentado pode acelerar a resposta a incidentes e minimizar o impacto nas operações comerciais.

Um artigo publicado pelo *Business Development Bank of Canada*, em seu site com 8 etapas para planejar seu plano de emergência e desastre enfatiza que, um bom PCN precisa estar integrado com práticas de segurança cibernética, e que as organizações podem criar uma abordagem mais resiliente e adaptável para enfrentar ameaças de acordo com sua realidade. Em vez de depender exclusivamente de medidas de segurança individuais, como firewalls e antivírus, o PCN permite uma resposta coordenada e estratégica a incidentes, fortalecendo a postura de segurança geral da organização, frente a clientes, fornecedores e funcionário.

Por fim, em um cenário onde a operação está na nuvem, a responsabilidade é compartilhada entre os provedores de serviço e seus clientes. Os provedores oferecem medidas de segurança em infraestrutura e serviço, mas cabe também aos usuários a obrigação de fazer sua parte, garantindo a segurança de suas próprias configurações e dados (PAK, 2024).

METODOLOGIA DA PESQUISA

Esta pesquisa foi conduzida utilizando uma abordagem de revisão bibliográfica abrangente, com o objetivo de identificar e analisar as tendências, desafios e práticas recomendadas na área de segurança cibernética, especificamente no contexto da cloud computing e sua interseção com o PCN. Para isso, foram consultadas diversas fontes de informação, onde buscou-se trazer o que há de mais novo no âmbito da continuidade de negócios, foi utilizado artigos, sites, livros, normas, entre outros.

RESULTADOS E DISCUSSÃO

Observa-se que a segurança cibernética é um componente essencial no cenário de transformação digital e adoção de *cloud computing.* Proteger dados e sistemas contra ameaças é vital para garantir a continuidade e a resiliência das operações. Integrar o PCN com medidas de

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

segurança não só fortalece a defesa contra-ataques, como também prepara a organização para responder de maneira eficaz e eficiente a qualquer incidente.

Um exemplo prático é o caso da Coca-Cola que durante a ocorrência do furacão Katrina em 2005. A empresa conseguiu manter suas operações graças a um robusto plano de continuidade de negócios, que incluía um centro de recuperação de dados externo ao local e uma equipe de resposta a emergências. Este exemplo ilustra como a preparação e a implementação de um PCN podem mitigar significativamente os impactos de desastres naturais (LAW, 2024).

À medida que as organizações aderem aos serviços em cloud, aumenta a dependência de terceiros para a gestão e proteção de dados sensíveis. Qualquer falha por parte desse fornecedor pode comprometer a existência da organização. Destaca-se a percepção equivocada de que migrar para a nuvem garante segurança absoluta, quando, na realidade, nenhum sistema está imune a ataques cibernéticos e falhas.

Ressalta-se a importância de uma abordagem abrangente e proativa para proteger os dados e garantir a continuidade dos negócios. Isso inclui não apenas a implementação de medidas técnicas de segurança, mas também a conscientização da equipe e o desenvolvimento de PCN que aborde cenários de perda total de dados na *Cloud Computing.* Comprovou-se que, em um cenário onde a *Cloud* esteja completamente indisponível, ou seja, não permitindo nenhum acesso, um PCN bem alinhado é essencial para assegurar que as operações possam continuar ou serem rapidamente retomadas após uma interrupção.

Como foi o caso da *Netflix* que em 2012, durante uma interrupção generalizada dos serviços da *Amazon Web Services* (AWS), sua principal provedora de serviços em nuvem, minimizou o impacto em seus clientes graças a um plano eficaz. A empresa implementou uma estratégia de implantação de nuvem multirregional, redirecionando automaticamente o tráfego para áreas não afetadas e garantindo um serviço ininterrupto para seus assinantes (LAW, 2024).

Observa-se ainda que a integração permite uma resposta coordenada e ágil a incidentes de segurança. No caso de um ataque *ransomware*, as equipes podem agir de acordo com um plano predefinido e devidamente testado, minimizando o impacto e acelerando a recuperação. Incorporar práticas de segurança cibernética no PCN também facilita a identificação e mitigação de riscos antes que eles causem danos significativos. Isso inclui a realização de avaliações regulares de vulnerabilidades e a implementação de medidas proativas de segurança. Como o caso da rede hoteleira Marriott, que em 2018 sofreu uma violação massiva de dados que expôs as informações pessoais de milhões de seus hóspedes, e mesmo com tamanha gravidade o PCN da empresa permitiu que eles respondessem de forma eficaz protegendo seus clientes e a marca (LAW, 2024).

Em suma, percebe-se a urgência de lidar com os desafios emergentes da segurança cibernética, especialmente na era da computação em nuvem. Evidencia-se ainda que o PCN oferece *insights* sobre as estratégias necessárias para mitigar os riscos e fortalecer a resiliência e a imagem

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

da organização, não só diante das ameaças digitais em constante evolução, mas também diante dos clientes, fornecedores e colaboradores.

CONSIDERAÇÕES

O cenário da segurança cibernética, especialmente no contexto da *cloud computing,* é desafiador e está em constante evolução. O *ransomware* emergiu como uma das ameaças mais prejudiciais, capaz de se proliferar rapidamente e causar danos significativos, incluindo o sequestro de dados sensíveis. No armazenamento em *cloud computing*, onde os dados estão sob a responsabilidade de terceiros, os desafios se tornam ainda mais complexos.

Embora as soluções de espelhamento e *backup* ofereçam algumas formas de proteção contra falhas catastróficas, como incêndios ou problemas de *hardware*, é importante reconhecer que o *ransomware* pode comprometer essas medidas de segurança, afetando tanto o ambiente principal quanto o espelhado, como foi, dentre os casos já citados, o da empresa *Ativy Digital* que, de acordo com uma matéria publicado pelo site 13SEC NEWS (2023), o *ransomware* criptografou não apenas os dados, mas também o *Hypervision e o backup.* Entender e mapear todos esses riscos, coloca o gestor a um passo à frente. Ao elaborar um plano, é essencial implementar sistemas de monitoramento contínuo e desenvolver planos de resposta a incidentes. Dessa forma, será possível identificar e mitigar rapidamente atividades suspeitas, minimizando o impacto de possíveis ataques. Além disso, ao considerar todos os cenários possíveis ao elaborar o PCN, a organização estará melhor preparada para enfrentar qualquer eventualidade.

Embora existam inúmeras ferramentas disponíveis para prevenir e mitigar os riscos cibernéticos, incluindo aquelas oferecidas pelas provedoras de serviços de cloud computing, é crucial que os gestores desenvolvam planos de contingência abrangentes. Esses planos devem abordar até mesmo a perda total do ambiente cloud, garantindo assim a continuidade dos negócios em qualquer situação. Isso envolve não apenas a implementação de medidas técnicas, mas também a adoção de práticas de conscientização e treinamento, a fim de educar os funcionários em práticas seguras de computação sobre os riscos cibernéticos, incentivando uma cultura de segurança em todo o ambiente organizacional.

A segurança cibernética é uma responsabilidade compartilhada entre provedores de serviços e clientes, exigindo uma abordagem proativa e multifacetada para proteger os dados e garantir a continuidade dos negócios. A conscientização sobre os riscos e a adoção de medidas preventivas são essenciais para que as organizações fortaleçam sua resiliência e mitiguem os impactos adversos das ameaças, especialmente em um ambiente de cloud computing. É fundamental reavaliar continuamente os processos de segurança existentes para garantir que eles sejam eficazes contra as ameaças emergentes. Com base na análise realizada, pode-se concluir que o objetivo do trabalho foi alcançado, demonstrando a importância de um PCN robusto e bem estruturado para enfrentar os desafios da segurança cibernética na era da *cloud computing.*

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

REFERÊNCIAS

13SEC NEWS. Ativy Digital empresa brasileira de cloud sofre ataque *ransomware*. **13SEC NEWS**, abr. 2023. Disponivel em: https://www.13secnews.com/ativy-digital-empresa-brasileira-de-cloud-sofre-ataque-*ransomware*/. Acesso em: 11 jun. 2024.

AMERICA'S. **America's data held hostage**: Case Studies in *Ransomware* Attacks on American Companies. United States: Committee on Homeland Security and Governmental, 2022.

BAIG, M. *et al*. The study of evasion of packed pe from static detection. **Researchgate** 10 jun. 2012. Disponível em: https://www.researchgate.net/profile/Pavol_Zavarsky/publication/259647266_The_Study_of_Evasion_of_Packed_PE_from_Static_Detection/links/58d2bba5458515e6d900bffa/The-Study-of-Evasion-of-Packed-PE-from-Static-Detection.pdf. Acesso em: 22 maio 2024.

BUSINESS DEVELOPMENT BANK OF CANADA. **Business continuity plan (BCP) in 8 steps, with templates**. Canada: BDC, s. d. Disponível em: https://www.bdc.ca/en/articles-tools/business-strategy-planning/manage-business/business-continuity-8-steps-building-plan. Acesso em: 25 mai. 2024.

CERT.BR. Codigos maliciosos. **CERT.BR**., jul. 2023. Disponivel em: https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf. Acessado em: 19 maio 2024.

CHECK POINT. **Check Point software's, cyber security report 2023**. US: Check Point, 2023. Disponível em: https://pages.checkpoint.com/cyber-security-report-2023.html. Acesso em: 20 maio 2024.

D'ADDARIO, J. A importância de um plano de continuidade de negócios para a sua empresa. **CNN BRASIL**, 29 maio 2023. Disponível em: https://www.cnnbrasil.com.br/forum-opiniao/a-importancia-de-um-plano-de-continuidade-de-negocios-para-a-sua-empresa/. Acesso em: 21 maio 2024.

FBI. **Internet crime report 2021**. [S. l.]: Departiment of justice federal bureau of investigation, 2021

GARRETT. O que é *malware*? Veja significado, tipos e saiba remover. **Techtudo**, 27 mar. 2021 Disponível em: https://www.techtudo.com.br/listas/2021/03/o-que-e-*malware*-veja-significado-tipos-e-saiba-remover.ghtml. Acesso em: 23 maio 2024.

HOROWITZ, M. **Introduction to the check point 2023 security report**. US: Check Point, 2023. Disponivel em: https://go.checkpoint.com/2023-cyber-security-report/chapter-01.php. Acesso em: 12 jun. 2024.

ISO. **ISO 22301:2019**. Security and resilience **—** Business continuity management systems — Requirements. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en. Acesso em: 27 maio. 2024.

LADEIRA, M. O que é plano de continuidade de negócios: o que é, para que serve, principais benefícios e passo a passo de como fazer. **Blog siteware**, 1 nov. 2022. Disponível em: https://www.siteware.com.br/blog/gestao-estrategica/plano-continuidade-negocios-pcn/. Acesso em: 24 maio. 2024.

LAW, O. **What are some examples of successful business continuity planning in action?** [*S. l.: s. n.*], 2024. Disponível em: https://www.fixinc.io/resources/examples-successful-bcp. Acesso em: 12 jun. 2024.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

LOBO, A. P. Ativy digital, de cloud, sofre ataque hacker na camada de virtualização. **Convergencia digital**, 03 abr. 2023. Disponível: https://www.convergenciadigital.com.br/Cloud-Computing/AtivyDigital%2CdeCloud%2Csofreataquehackernacamadadevirtualizacao62912.html?UserActiveTemplate=mobile%2Csite. Acesso em: 11 jun. 2024

PAK, J. How to create a resilient business continuity plan. **Blog Pandadoc**, 12 mar. 2024 Disponível em: https://www.pandadoc.com/blog/business-continuity-plan/. Acesso em: 21 maio 2024.

PANETTA, K. Is the cloud secure?. **Gartner**, 10 out. 2019. Disponível em: https://www.gartner.com/smarterwithgartner/is-the-cloud-secure. Acesso em: 18 maio 2024.

RICADELA, A. What is business continuity and disaster recovery?. **Oracle**, 26 abr. 2024. Disponível em: https://www.oracle.com/business-continuity/business-continuity-disaster-recovery/. Acesso em: 26 maio 2024.

ROMAR, C. E. C.; SILVA, R. C. **Estudo de métodos de detecçãoo de *ransomware* utilizando inteligência artificial**. [*S. l.: s. n.*], 2022.

SILVA, E. M. D. **Liderança e gestão em TI:** uma análise do desempenho de gestores de TI baseada em competências críticas de gestão. 2013. Tese (Doutorado em Engenharia de Produção) - Universidade de São Paulo, São Paulo, 2013.

TIGRE, P. B.; NORONHA, V. B. Do mainframe à nuvem: inovações, estrutura industrial e modelos de negócios nas tecnologias da informação e da comunicação. **Revista de Administração**, v. 48, n. 1, p. 114–127, 2013.