DANIEL ARAUJO DE ANDRADE

O FRAMEWORK CCM DA CSA COMO UM GUIA PARA A CONTRATAÇÃO DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM SEGURO

Ensaio Acadêmico apresentado ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do certificado do Curso Superior de Segurança e Defesa Cibernética.

Rio de Janeiro

2023

CSSDC2023 ESG

_____

DANIEL ARAUJO DE ANDRADE

RESUMO

A adoção da computação em nuvem traz uma mudança significativa na forma como as organizações e os indivíduos gerenciam seus dados e recursos tecnológicos, proporcionando elasticidade, escalabilidade, flexibilidade no local de trabalho e colaboração em tempo real. Considerando a importância da segurança cibernética na adoção desse modelo de serviço, esta pesquisa teve como objetivo analisar em que medida o cumprimento de requisitos mínimos de cibersegurança pode ser garantido ao contratar-se um provedor de serviço de nuvem que utiliza o framework *Cloud Controls Matrix* (CCM) da *Cloud Security Alliance* (CSA) como recurso de segurança. Inicialmente, identificou-se os aspectos conceituais relacionados à computação em nuvem, a fim de facilitar a compreensão das atribuições de responsabilidade. Posteriormente, realizou-se um levantamento das principais ameaças cibernéticas, com base em relatório especializado da CSA, que identificou questões relacionadas tanto aos provedores como aos clientes de serviços de nuvem. Por fim, examinou-se o CCM, como ferramenta para implementação de controles, categorizados em 17 domínios de segurança. O resultado da pesquisa indicou que a aplicação do *framework* CCM da CSA pode ajudar a garantir a segurança cibernética na contratação de serviços de computação em nuvem, pois a implementação dos controles estão alinhados com as melhores práticas e são capazes de mitigar os principais riscos associados a cibersegurança na computação em nuvem.

Palavras-chave: cibersegurança; segurança da informação; computação em nuvem.

ABSTRACT

The adoption of cloud computing brings a significant change in the way organizations and individuals manage their data and technological resources, providing elasticity, scalability, workplace flexibility, and real-time collaboration. Considering the importance of cybersecurity in the adoption of this service model, this research aimed to analyze to what extent compliance with minimum cybersecurity requirements can be guaranteed when contracting a cloud service provider that uses the Cloud Controls Matrix (CCM) framework from the Cloud Security Alliance (CSA) as a security resource. Initially, the conceptual aspects related to cloud computing were identified in order to facilitate the understanding of responsibility assignments. Subsequently, information on the main cybersecurity threats was gathered, based on a specialized CSA report, which identified issues related to both cloud service providers and customers. Finally, the CCM was examined as a tool for implementing controls, which are categorized into 17 security domains. The research result indicated that the application of the CSA's CCM framework can help to ensure cybersecurity in the contracting of cloud computing services, as the implementation of the controls are aligned with best practices and are able to mitigate the main risks associated with cybersecurity in cloud computing.
Keywords*: cybersecurity framework; cloud security; cloud computing.*

LISTA DE ABREVIATURAS E SIGLAS

API	*Application Programming Interface*
APT	*Advanced Persistent Threat*
CCM	*Cloud Controls Matrix*
CIS	*Center for Internet Security*
CSA	*Cloud Security Alliance*
CSC	*Cloud Service Customer*
CSP	*Cloud Service Provider*
CSRM	*Cloud Shared Resource Model*
IaaS	*Infrastructure as a Service*
ISO	*International Organization for Standardization*
NIST	*National Institute of Standards and Technology*
PaaS	*Platform as a Service*
SaaS	*Software as a Service*
SLA	*Service Level Agreement*

SUMÁRIO

1 INTRODUÇÃO

A computação em nuvem representa uma mudança na forma como organizações e indivíduos gerenciam seus dados e recursos tecnológicos. Ao adotar esse modelo, ganha-se a capacidade de ajustar seus recursos de acordo com a demanda, proporcionando elasticidade e escalabilidade. Ela pode facilitar o trabalho remoto e a colaboração em tempo real, permitindo maior flexibilidade no local de trabalho. A eliminação da necessidade de infraestrutura física resulta em uma redução de custos operacionais, e as atualizações automáticas de *software* garantem acesso às últimas inovações tecnológicas. A utilização dessa ferramenta pode aumentar a eficiência, agilidade e alcance dos serviços prestados.

No entanto, a adoção da computação em nuvem traz consigo alguns desafios inerentes à segurança. Uma das principais preocupações reside nas potenciais vulnerabilidades que podem ser exploradas, o que pode incluir falhas de configuração inadequada, interfaces e API (Application Programming Interface) inseguras, recursos de terceiros inseguros e vulnerabilidades do próprio sistema (BHARADWAJ; BHATTACHARYA; CHAKKARAVARTHY, 2018). Além disso, um efetivo controle de permissões é crucial para prevenir acessos não autorizados ou atividades maliciosas dentro do ambiente em nuvem, que podem resultar na exfiltração de dados de armazenamento em nuvem.

Para buscar a conformidade com os padrões de segurança estabelecidos, os provedores de serviço de computação em nuvem implementam controles de segurança, de modo a oferecer a seus clientes um serviço seguro e confiável. Uma das formas comumente utilizadas, é o uso de um estrutura (*framework*) que pode ser entendida como um guia ou plano para implementação dos controles.

1.1 Problema de Pesquisa

Diante do contexto apresentado, surgiu a inquietação e motivação para pesquisa do tema exposto, propiciando a formulação do seguinte problema de pesquisa: em que medida a utilização do *framework* de controle de cibersegurança CCM (*Cloud Controls Matrix*) da *Cloud Security Alliance* (CSA) pode garantir o atendimento dos requisitos mínimos de segurança cibernética na contratação de serviços de computação em nuvem?

1.2 Objetivos

1.2.1 Objetivo Geral

Exposto o problema de pesquisa, este estudo buscou como objetivo geral analisar em que medida o cumprimento de requisitos mínimos de cibersegurança pode ser garantido ao contratar-se um provedor de serviço de nuvem que utiliza como recurso de segurança a aplicação do *framework* CCM da CSA.

1.2.2 Objetivos Específicos

Para tanto, foram definidos os Objetivos Específicos a seguir:

OE1) Identificar os aspectos conceituais relacionados à computação em nuvem.

OE2) Identificar as principais ameaças relacionadas à segurança cibernética na computação em nuvem.

OE3) Descrever os domínios que compõem a estrutura do *framework* CCM.

1.3 Delimitação do estudo

Diversos tipos de estruturas e padrões como: o CIS Controls, do Center for Internet Security (CIS); o *Cybersecurity Framework* do *National Institute of Standards and Technology* (NIST); ou mesmo a Norma ISO 27001 da *International Organization for Standardization* (ISO), são considerados referências internacionais na área de cibersegurança. No entanto, visando manter o foco nas soluções voltadas para a nuvem, este estudo limitou-se à análise do *framework Cloud Controls Matrix* (CCM) desenvolvido pela *Cloud Security Alliance* (CSA), um grupo sem fins lucrativos que se concentra na promoção das melhores práticas de segurança em relação à computação em nuvem (STEWART, 2021, p. 453).

1.4 Justificativa

A avaliação de risco é um passo crucial para os gestores ao considerar a contratação de um serviço de computação em nuvem, especialmente no que diz respeito à conformidade com os padrões de segurança estabelecidos. Garantir que o

provedor de nuvem cumpra os requisitos mínimos de segurança é essencial para proteger os dados sensíveis da organização contra ameaças cibernéticas. Dessa forma, quando o provedor de serviço busca atender aos padrões de segurança estabelecidos, não apenas reduz o risco de violações de dados, mas também demonstra um compromisso com a integridade, disponibilidade e confidencialidade das informações.

2 CONCEITOS DA ARQUITETURA DE COMPUTAÇÃO EM NUVEM

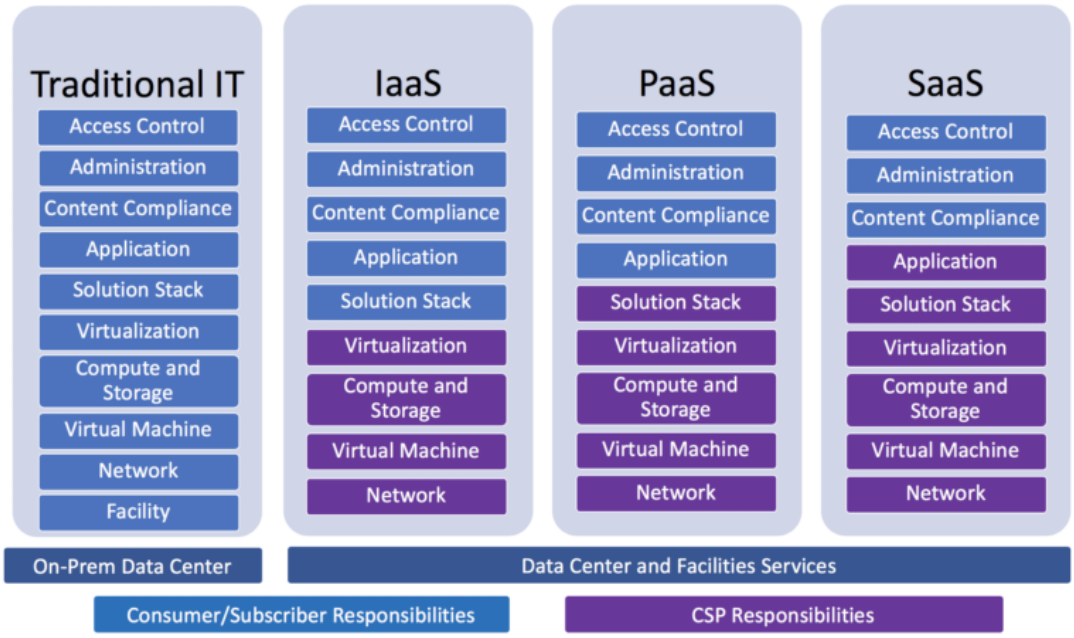
A utilização da computação em nuvem e da virtualização acarreta riscos significativos, uma vez que informações confidenciais passam a depender da segurança do provedor. É imperativo optar por um provedor de serviços em nuvem (CSP) com um histórico sólido de segurança e implementar controles de proteção apropriados. As principais inquietações em termos de segurança associadas à computação em nuvem envolvem a definição e a clarificação das responsabilidades de segurança entre o CSP e o cliente de serviços em nuvem (CSC). Estes detalhes devem ser minuciosamente estabelecidos no Acordo de Nível de Serviço (SLA) ou contrato (STEWART, 2021, p. 139).

Segundo Mushtaq *et al.* (2017) a arquitetura de computação pode ser entendida tanto no nível implantação, como em termos de modelo de serviço. Os tipos de implantação são classificados em: nuvem pública, nuvem privada, nuvem comunitária e nuvem híbrida. Essas categorias representam a maneira como a infraestrutura de computação fornece os serviços em nuvem.

A nuvem pública representa uma plataforma de computação em nuvem de acesso aberto ao público em geral, sendo administrada por um provedor de serviços especializado na área. Por sua vez, a nuvem privada é uma plataforma de computação em nuvem exclusivamente dedicada a uma única organização, com gestão realizada internamente ou através de um CSP designado. A nuvem comunitária se configura como uma plataforma de computação em nuvem compartilhada por diversas organizações que compartilham interesses ou requisitos de segurança similares. Por fim, a nuvem híbrida constitui uma fusão de duas ou mais nuvens (sejam elas públicas, privadas ou comunitárias), que mantêm sua individualidade, mas estão interconectadas, permitindo a transferência de dados e aplicativos entre elas (STEWART, 2021, p. 140).

Quanto ao modelo de serviço de nuvem, são oferecidos em três principais tipos distintos. O primeiro é o IaaS (*Infrastructure as a Service*), no qual o provedor disponibiliza a infraestrutura de TI, como servidores, armazenamento e sistemas operacionais, enquanto o cliente fica responsável por implantar e gerenciar suas próprias aplicações e dados. O segundo modelo é o PaaS (*Platform as a Service*), no qual o provedor oferece uma plataforma de desenvolvimento, incluindo ferramentas e suporte, e cabe ao cliente a responsabilidade de desenvolver e implantar suas aplicações. Por fim, o SaaS (*Software as a Service*) envolve o fornecimento de *software* acessível por meio de um navegador web ou aplicativo, sem que o cliente precise se preocupar com a infraestrutura ou plataforma de desenvolvimento utilizada (LEE; BOHN; MICHEL, 2020).

Figura 1 - The Cloud Shared Resource Model (CSRM)



Fonte: SCOTT, 2018.

Com o intuito de definir as responsabilidades, os principais fornecedores de serviços de computação em nuvem desenvolveram o Modelo de Recursos Compartilhados em Nuvem (CSRM). Dentro deste modelo as atribuições ficam claras, de forma que a responsabilidade pela segurança e proteção dos dados compartilhados é dividida entre o CSP e o CSC, dependendo do modelo de serviço de nuvem escolhido (BHARADWAJ; BHATTACHARYA; CHAKKARAVARTHY, 2018).

Conforme apresentado na Figura 1, na medida em que avança-se de um modelo tradicional de TI para um arquitetura SaaS (da esquerda para a direita), as funções operacionais e de gestão e a responsabilidade dos recursos da nuvem

passam do contratante do serviço para o provedor, resultando em uma necessidade alinhamento e mudança na forma com que as equipes tradicionais de cibersegurança atuam na sustentação do negócio (SCOTT, 2018).

3 AMEAÇAS CIBERNÉTICAS RELACIONADAS À COMPUTAÇÃO EM NUVEM

A natureza compartilhada e interconectada da computação em nuvem traz à tona preocupações significativas sobre a segurança desses sistemas. A sofisticação crescente de ataques cibernéticos apresenta um desafio constante para os CSPs, exigindo medidas rigorosas de proteção e monitoramento contínuo. Apesar dos esforços contínuos de equipes de operações e engenharia, hackers empregam táticas inovadoras para comprometer sistemas altamente seguros, chegando a capturar sistemas industriais e financeiros inteiros. A complexidade de proteger a segurança em múltiplos domínios emerge como um desafio crítico para empresas que operam na nuvem (AHANGER; ALJUMAH, 2020).

A *Cloud Security Alliance* (CSA) publicou em 2022, um relatório que identifica as 11 principais ameaças, riscos e vulnerabilidades em ambientes de nuvem, com base em uma pesquisa com mais de 700 especialistas do setor, conforme apresentado no Quadro 1 (CSA, 2022).

Quadro 1 - Principais Ameaças à Computação em Nuvem

Ameaças	Descrição
Gerenciamento inadequado de identidade, credenciais, acesso, gerenciamento de chaves e contas privilegiadas	Ocorre quando as organizações não implementam ou gerenciam adequadamente suas políticas e controles de IAM (*Identity and Access Management*). Isso pode levar a acesso não autorizado aos recursos na nuvem, o que pode resultar em comprometimento de dados, perda de dados ou ataques maliciosos.
Interfaces e APIs inseguras	As interfaces e APIs da nuvem são frequentemente alvos de ataques. As organizações devem tomar medidas para proteger essas interfaces e APIs, incluindo a implementação de autenticação e autorização fortes, a criptografia de dados em trânsito e a detecção de anomalias.
Configurações incorretas e controle de alterações inadequado	As configurações incorretas e o controle de alterações inadequado podem levar a vulnerabilidades de segurança. As organizações devem implementar processos rigorosos para configurar e gerenciar seus recursos na nuvem.
Ameaças	Descrição
Falta de arquitetura e estratégia de segurança da nuvem	As organizações devem ter uma arquitetura e estratégia de segurança da nuvem abrangentes. Isso inclui o

	desenvolvimento de um plano de segurança da nuvem, a implementação de controles de segurança e a realização de testes de segurança regulares.
Desenvolvimento de *software* inseguro	O desenvolvimento de *software* inseguro pode levar a vulnerabilidades de segurança na nuvem. As organizações devem implementar práticas de desenvolvimento seguro, incluindo a revisão de código, a análise de segurança estática e a implementação de testes de segurança.
Recursos de terceiros inseguros	Os recursos de terceiros podem ser uma fonte de vulnerabilidades de segurança. As organizações devem realizar avaliação aprofundada em seus fornecedores de terceiros e implementar medidas para proteger seus recursos.
Vulnerabilidades de sistema	As vulnerabilidades de sistema são uma ameaça constante à segurança da nuvem. As organizações devem manter seus sistemas atualizados com as últimas correções de segurança.
Divulgação acidental de dados na nuvem	A divulgação acidental de dados na nuvem pode ocorrer por diversos motivos, como erros de configuração, erros humanos ou falhas de segurança. As organizações devem implementar medidas para prevenir a divulgação acidental de dados, como criptografia de dados, controle de acesso e monitoramento de atividades.
Falha de configuração e exploração de cargas de trabalho sem servidor e contêineres	A falha de configuração e exploração de cargas de trabalho sem servidor e contêineres ocorre quando as configurações de um serviço de computação em nuvem são incorretas ou não seguras. Essa vulnerabilidade pode ser explorada por hackers para obter acesso aos recursos do serviço, como dados, código ou infraestrutura.
Crime organizado, *hackers* e ameaças persistentes avançadas (APTs)	Grupos de crime organizado, hackers e ameaças persistentes avançadas (APTs) são sofisticados e estão constantemente desenvolvendo novas técnicas de ataque. As organizações devem implementar medidas para se proteger contra esses ataques, como monitoramento de segurança, detecção de ameaças e resposta a incidentes.
Exfiltração de dados do armazenamento em nuvem	A exfiltração de dados do armazenamento em nuvem pode ocorrer por diversos motivos, como ataques maliciosos, erros humanos ou falhas de segurança. As organizações devem implementar medidas para prevenir a exfiltração de dados do armazenamento em nuvem, como criptografia de dados, controle de acesso e monitoramento de atividades.

Fonte: O Autor, 2023 (adaptado de CLOUD SECURITY ALLIANCE, 2022).

Segundo a *Cloud Security Alliance* (2022, p. 6) há uma mudança no foco das questões tradicionais de segurança em nuvem, que passou da responsabilidade dos provedores de serviços para as circunstâncias diretamente sob o controle do cliente: gerenciamento de identidade e acesso, criptografia, gerenciamento de configuração, práticas de codificação inadequadas e falta de estratégia de desenvolvimento seguro.

O aumento do uso de métodos ágeis em projetos e de abordagens integradas de desenvolvimento e operações, levaram esses problemas combinados diretamente às equipes finais de *software*. A distinção de organizações de nuvem de alto desempenho, está na ênfase dada ao gerenciamento de mudanças, aumento do treinamento cruzado de funcionários, incorporação de profissionais de cibersegurança nas equipes e implementação de uma cultura de segurança e conformidade.

4 FRAMEWORK DE CONTROLE DE CIBERSEGURANÇA CCM

O *framework* de segurança cibernética é a estrutura necessária para que uma organização se proteja contra ataques cibernéticos. Alguns *frameworks* de segurança cibernética são mandatórios, enquanto outros são frequentemente recomendados pelos órgãos reguladores. Dessa forma, os *frameworks* orientam as organizações no processo de implementação para atender aos requisitos padrão. O principal objetivo de um *framework* de segurança cibernética é reduzir o risco de ameaças cibernéticas através do aprendizado com as melhores práticas (TAHERDOOST, 2022).

O *Cloud Controls Matrix* (CCM) é um *framework* de controle de segurança desenvolvido pela CSA para atender à lacuna de uma estrutura de segurança e conformidade relevante para a nuvem. O CCM visa ajudar os provedores de serviços e os clientes de serviços em nuvem a avaliar os riscos gerais de segurança dos serviços em nuvem. Ele inclui conceitos e princípios de segurança detalhados alinhados com o Guia de Segurança CSA v4. O *framework*, no contexto dos CSPs, representa a definição de diretrizes de excelência para promover a implementação segura de infraestrutura e serviços em nuvem. Já para os CSCs, viabiliza uma avaliação mais precisa e abrangente dos CSPs, levando em consideração seus controles de segurança.(CLOUD SECURITY ALLIANCE, 2021, p. 7).

A *Cloud Computing Alliance* (2021, p. 8) estruturou o CCM versão 4.0 em 17 domínios de segurança, abrangendo um total de 197 controles. Esses domínios foram delineados com base no guia de segurança da CSA e se inspiraram em *frameworks* relevantes, como o ISO/IEC 27001 e o ISO/IEC 27002. Dentro dessa estrutura, cada controle é atribuído a um domínio específico, como apresentado no Quadro 2. A concepção intencional do CCM foi torná-lo similar aos *frameworks* de segurança da informação mais amplamente reconhecidos, que não se limitam à nuvem, a fim de capitalizar a familiaridade com esses *frameworks* já estabelecidos.

Quadro 2 - Descrição dos Domínios do CCM

Domínio	Aspectos Gerais dos Controles
Auditoria e Garantia	Fornecer evidências da eficácia dos controles de segurança da nuvem por meio de auditorias internas e externas.
Segurança de Aplicativos e Interfaces	Proteger aplicativos e interfaces de APIs contra ataques e vulnerabilidades por meio de controles de autenticação, autorização e codificação segura.
Gerenciamento de Continuidade de Negócios e Resiliência Operacional	Garantir que a organização possa continuar operando em caso de interrupções nos serviços de nuvem por meio de planos de contingência e testes de recuperação.
Controle de Mudanças e Gerenciamento de Configuração	Garantir que as mudanças na infraestrutura e nos aplicativos da nuvem sejam feitas de forma segura e controlada por meio de processos de aprovação e teste.
Criptografia, Codificação e Gerenciamento de Chaves	Proteger dados em repouso e em trânsito usando criptografia forte e gerenciamento seguro de chaves.
Segurança de *Data Center*	Proteger a infraestrutura física que suporta os serviços de nuvem por meio de controles de acesso físico, segurança de rede e proteção contra incêndio.
Gerenciamento do Ciclo de Vida de Segurança e Privacidade de Dados	Proteger dados ao longo de todo o seu ciclo de vida, desde a criação até a destruição, por meio de controles de identificação, autenticação, proteção contra acesso não autorizado e gerenciamento de dados de identificação pessoal.
Governança, Gestão de Riscos e Conformidade	Estabelecer um *framework* para gerenciar riscos e garantir a conformidade com as leis e regulamentos aplicáveis por meio de processos de identificação, avaliação e mitigação de riscos, e realização de auditorias de conformidade.
Recursos Humanos	Garantir que os funcionários estejam cientes das políticas e procedimentos de segurança da nuvem por meio de treinamento de segurança e promoção de uma cultura de segurança.
Gerenciamento de Acesso e Credenciais	Gerenciar o ciclo de vida de credenciais e acessos na nuvem por meio de controles de autenticação, autorização e gerenciamento de acesso privilegiado.
Interoperabilidade e Portabilidade	Garantir que os dados e aplicativos possam ser facilmente transferidos entre diferentes CSPs por meio da utilização de padrões abertos e adoção de práticas recomendadas.
Domínio	Aspectos Gerais dos Controles
Segurança de Infraestrutura e Virtualização	Proteger a infraestrutura de nuvem, incluindo servidores, redes e armazenamento, por meio de controles de segurança física, segurança de rede e proteção contra *malwares*.
Registro e Monitoramento	Registrar e monitorar eventos de segurança na nuvem por meio de

	ferramentas de registro e monitoramento e análise de dados de segurança.
Gerenciamento de Incidentes de Segurança, Evidências Eletrônicas e Forense em Nuvem	Investigar e responder a incidentes de segurança na nuvem por meio de um plano de resposta a incidentes e realização de investigações forense.
Transparência e Responsabilização na Gestão da Cadeia de Suprimentos	Garantir a transparência e responsabilização na gestão da cadeia de suprimentos de serviços de nuvem por meio de avaliação de fornecedores e realização de auditorias de segurança.
Gerenciamento de Ameaças e Vulnerabilidades	Identificar, avaliar e mitigar ameaças e vulnerabilidades na nuvem por meio de avaliações de ameaças e implementação de controles para mitigar vulnerabilidades.
Gerenciamento Universal de Endpoints	Gerenciar *endpoints* em ambientes de nuvem por meio de controles de segurança em dispositivos móveis, laptops e outros dispositivos.

Fonte: O Autor, 2023 (adaptado de CLOUD SECURITY ALLIANCE, 2021).

De acordo com a *Cloud Computing Alliance* (2021), uma avaliação de risco conduzida pela organização pode destacar a necessidade de salvaguardar a confidencialidade, integridade e disponibilidade dos ativos de informação armazenados na nuvem, levando em conta seus distintos níveis de sensibilidade e importância. Nesse contexto, o emprego do *Cloud Controls Matrix* visa a identificação de requisitos específicos relativos a políticas, procedimentos e tecnologias, bem como a formulação de metas de controle para o programa de segurança da organização. Além disso, o CCM é empregado para impor diretrizes a usuários internos, parceiros de negócios e CSPs, além de monitorar a aderência tanto às políticas internas quanto aos requisitos normativos externos.

5 CONSIDERAÇÕES FINAIS

Diante da crescente adoção do modelo de computação em nuvem, em virtude dos seus inúmeros benefícios para as organizações e indivíduos, os riscos associados à cibersegurança tornou-se uma preocupação para os gestores na contratação de serviços de computação em nuvem. Com a hipótese de que a utilização do *framework Cloud Controls Matrix* pode garantir o atendimento dos padrões mínimos de segurança, este estudo procurou identificar as principais ameaças relacionadas à cibersegurança, assim como cada domínio que estrutura o *framework* CCM.

Dessa forma, para facilitar a compreensão das atribuições de responsabilidade dentro do Modelo de Recursos Compartilhados em Nuvem, foram apresentados

alguns conceitos básicos relacionados à arquitetura de computação em nuvem, tanto em termos de nível de implantação, como em relação ao modelo de serviço.

No levantamento das principais ameaças, utilizou-se como referência o relatório *Top Threats to Cloud Computing Pandemic Eleven* da CSA (2022). Por meio de um quadro, foi apresentada uma breve descrição das 11 principais ameaças escolhidas por especialistas do setor. Este relatório mostrou que a maturidade nas práticas dos provedores de serviços de nuvem, levou a uma mudança com maior foco para os recursos sob gestão do cliente.

Por último, foi apresentado o *framework* CCM, como uma ferramenta de implementação de controles que visam mitigar os riscos cibernéticos, com base no guia da própria CSA e também em padrões de segurança relevantes. Por limitação do estudo, realizou-se uma abordagem macro dos controles que compõem o *framework*, apresentando uma descrição de cada um dos domínios da estrutura.

O estudo aponta que o *Cloud Controls Matrix*, enquanto instrumento para a implementação de controles nos variados domínios que abarca, tem o potencial de mitigar os principais riscos cibernéticos e assegurar a conformidade com os requisitos mínimos de segurança cibernética ao contratar um serviço de computação em nuvem.

Os resultados apresentados neste trabalho fornecem um ponto de partida importante, mas deixam aberta a possibilidade investigação mais aprofundada dos controles que constituem o CCM, assim como de outros padrões ou *frameworks* com enfoque em soluções para a computação em nuvem.

REFERÊNCIAS

AHANGER, T.; ALJUMAH, A. Cyber Security Threats, Challenges and Defense Mechanisms in Cloud Computing. **IET Communications**, v. 14, n. 7, p. 1185-1191, 12 fev. 2020. Disponível em: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-com.2019.0040. Acesso em: 9 out. 2023.

BHARADWAJ, Deepak R.; BHATTACHARYA, Anamika; CHAKKARAVARTHY, Manivannan. Cloud threat defense: a threat protection and security compliance solution. *In:* IEEE INTERNATIONAL CONFERENCE ON CLOUD COMPUTING IN EMERGING MARKETS (CCEM), 2018. **Proceedings** [...]. *[S. l.]*: IEEE, 2018. p. 95-99. Disponível em: https://doi.org/10.1109/ccem.2018.00024. Acesso em: 2 out. 2023

CLOUD SECURITY ALLIANCE. **CCM v4.0 Implementation Guidelines**. *[S. l.]*: CSA, 2021. Disponível em: https://cloudsecurityalliance.org/artifacts/ccm-v4-0-implementation-guidelines/. Acesso em: 1 out. 2023.

CLOUD SECURITY ALLIANCE. **Top Threats to Cloud Computing Pandemic Eleven**. *[S. l.]*: CSA, 2022. Disponível em: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven/. Acesso em: 5 out. 2023.

LEE, Craig A.; BOHN, Robert B.; MICHEL, Martial. **The NIST Cloud Federation Reference Architecture**. Gaithersburg: National Institute of Standards and Technology, 2020. Disponível em: https://doi.org/10.6028/nist.sp.500-332. Acesso em: 5 out. 2023.

MUSHTAQ, Muhammad Faheem *et al*. Cloud Computing Environment and Security Challenges: A Review. **International Journal of Advanced Computer Science and Applications**, v. 8, n. 10, p. 183-195, 2017. Disponível em: https://doi.org/10.14569/ijacsa.2017.081025. Acesso em: 3 out. 2023.

SCOTT, Tom. **CSRM - Cloud Shared Resource Model.** *[S. l.]*: Open Alliance for Cloud Adoption, 2018. Disponível em: https://www.oaca-project.org/2018/10/13/csrm-cloud-shared-resource-model/. Acesso em: 6 out. 2023.

STEWART, James Michael. **CompTIA Security+ Review Guide:** Exam SY0-601. Indianapolis: John Wiley & Sons, 2021. 576 p.

TAHERDOOST, H. Understanding cybersecurity frameworks and information security standards: a review and comprehensive overview. **Electronics**, v. 11, n. 14, p. 2181, jul. 2022. Disponível em: https://www.mdpi.com/2079-9292/11/14/2181. Acesso em: 9 out. 2023.