

## USO DAS NORMAS NBR ISO/IEC 27017 E 27018 PARA GARANTIR A SEGURANÇA DA COMPUTAÇÃO EM NUVEM

Souza, H.<sup>1</sup>, Silva, S.<sup>1</sup>.

<sup>1</sup> Escola Politécnica e de Artes

Pontifícia Universidade Católica de Goiás

Goiânia-GOÍÁS-Brasil

**RESUMO:** O objetivo deste artigo é o de apresentar uma visão geral sobre a computação em nuvem e de mostrar como as normas ABNT NBR ISO/IEC 27017 e 27018 garantem a segurança no ambiente em nuvem. Foi realizada uma revisão bibliográfica sobre a segurança em nuvem e a implementação de medidas para garantir que os dados armazenados e processados na nuvem sejam protegidos. O estudo permitiu concluir que o uso destas normas citadas pode ajudar a manter tais dados seguros e aumentar a confiança na tecnologia de segurança. Apesar de não serem obrigatórias, as normas estabelecem diretrizes e orientações para tratar os serviços e as informações no ambiente em nuvem. Seguir estes padrões trazem maior segurança para o ambiente em nuvem e para a privacidade dos dados.

**Palavras-chave:** Computação em nuvem, segurança da informação, Políticas de Segurança, Normas.

**ABSTRACT:** The purpose of this article is to present an overview of cloud computing and to show how the ABNT NBR ISO/IEC 27017 and 27018 standards guarantee security in the cloud environment. A literature review was carried out on cloud security and the implementation of measures to ensure that data stored and processed in the cloud is protected. The study led to the conclusion that the use of these cited standards can help keep such data safe and increase confidence in security technology. Although not mandatory, the standards establish guidelines and guidelines for handling services and information in the cloud environment. Following these standards brings greater security to the cloud environment and to data privacy.

**Keywords:** Cloud computing, information security, Security Policies, Standards.

### 1. Introdução

O aumento de informações e dados nos ambientes corporativos trouxe a necessidade de tecnologias com maior capacidade de processamento e armazenamento sem que tivessem que investir em grandes estruturas de hardware e software que ocupariam um extenso espaço na empresa e gerariam gastos com manutenção [1].

Tendo em vista tal necessidade, a computação em nuvem ou *cloud computing*, surgiu com o objetivo de disponibilizar sob demanda um conjunto compartilhado de recursos através da Internet, poupando gastos com, por exemplo, energia, manutenção, espaço de infraestrutura entre outros. Estes recursos podem ser facilmente alocados sem muito esforço de gerência e o cliente paga apenas por aquilo que ele usa [2].

Levando em conta a demanda da empresa, a computação em nuvem oferece três tipos de modelo de serviços, sendo eles Plataforma como serviço (PaaS), Software como serviço (SaaS) e Infraestrutura como serviço (IaaS). Cada um deles tem risco, benefícios e utilidades diferentes [3].

Ao utilizar o serviço de computação em nuvem uma questão muito importante é colocada em pauta, a segurança dos dados. Por ser um serviço que reúne informações de um ou mais clientes, ele se torna um alvo para ataques. Tendo acesso aos dados de uma empresa a pessoa ou grupo mal-intencionado pode apagar, modificar ou até mesmo compartilhá-los [4].

A norma ABNT NBR ISO/IEC 27017, dentre outras, estabelece um código de boas práticas para melhorar a segurança de serviços em nuvem para o cliente e para o provedor. Esta norma fornece diretrizes para diferentes tipos de implementações de serviços em nuvem para evitar ameaças. No entanto, para certificar que os serviços estejam seguros é necessário combinar o uso destas normas com outras, que abordem também questões de segurança e computação em nuvem [5].

O objetivo geral deste artigo é apresentar uma visão geral sobre a computação em nuvem, além de mostrar como as normas ISO/IEC 27017 e 27018 garantem a segurança neste ambiente.

### 1.1 *Computação em nuvem*

O rápido desenvolvimento e agregação de tecnologias no cotidiano das pessoas pode ser definido pelo termo Tecnologia da Informação (TI). Alecrim [6], define este termo como atividades e soluções que foram produzidas por meios tecnológicos possibilitando gerenciar informações.

O conceito de computação em nuvem pode ser definido como o fornecimento de recursos de TI, tais como processamento, armazenamento entre outros, através da internet. Tais recursos podem ser alocados de forma rápida e elástica para atender a necessidade dos usuários. O que

possibilita o funcionamento dessa tecnologia é a operação em conjunto de diversos servidores, físicos ou virtuais, geralmente espalhados por várias localidades [7]. A Figura 1 ilustra as principais vantagens da computação em nuvem.

Figura 1 – Vantagens da computação em nuvem



Fonte: TI OPEN, 2021.

Não obstante, apesar da grande quantidade de vantagens do uso da computação em nuvem é importante perceber que isso tudo torna o quesito segurança extremamente necessário. Por armazenar e circular muitos dados, garantir a segurança da computação em nuvem tornou-se algo crucial. Nesse sentido, os provedores de nuvem devem buscar conhecer os riscos de ciberataques existem a fim de evitá-los [2].

Um ciberataque é um crime. Ele consiste em ações não autorizadas dirigidas contra um sistema de informação, com objetivo de prejudicar a pessoa ou organização, de alguma forma. Tais ações podem ser realizadas de diversos tipos como, por exemplo, ataque a banco de dados ou criptografia de dados, buscando extorquir, destruir informações, expor ou alterar dados, entre outros [8].

## 1.2 Modelos de nuvem

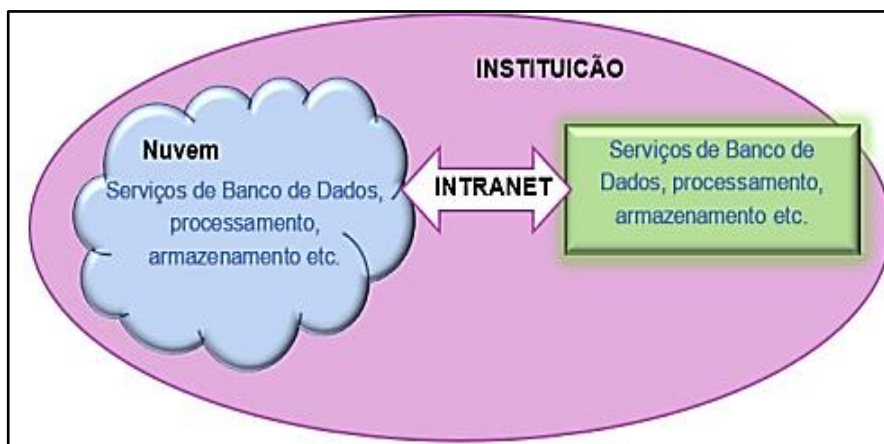
Segundo Lorenzi [9], existem três modelos de implantação da computação em nuvem, sendo eles privada, pública e híbrida. A escolha de qual será usada depende da necessidade de cada cliente, pois cada modelo tem suas vantagens e desvantagens.

De acordo com Tavbulatova [10], a nuvem privada é definida como aquela cujo recursos são usados e pertencem a uma organização em particular. Nesse sentido, os serviços fazem parte de uma rede privada de usuários com infraestrutura dedicada a organização. Estes recursos podem ser tanto físicos, hospedados no ambiente da empresa nos data centers, quanto terceirizados por um provedor de nuvem.

O uso da nuvem privada traz consigo vantagens, mas a que mais se destaca é a questão de ter maior controle. Devido ao fato de que os recursos são compartilhados apenas com os usuários internos, torna-se possível personalizar e controlar os recursos de acordo com a necessidade da organização para garantir maior produtividade [11].

Outra vantagem é que a nuvem privada garante mais segurança. O tráfego de informações é limitado às operações da organização. Embora não seja impossível, é menos provável que haja tráfego malicioso, já que o público em geral não tem acesso à rede. Quanto à segurança física da nuvem, este modelo de nuvem consegue lidar melhor com isto, pois o equipamento em geral é gerenciado pela organização e os computadores que têm acesso fazem parte de um grupo restrito [12]. A Figura 2 ilustra o esquema de uma nuvem privada.

Figura 2 – Modelo de nuvem privada

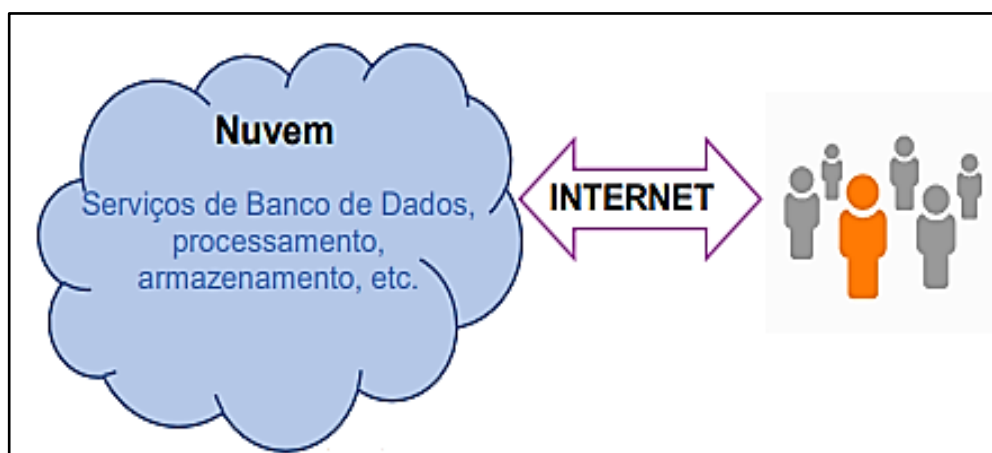


Fonte: SILVA, 2019.

Tendo como uma das principais características uma arquitetura multi-inquilino, o modelo de nuvem pública é gerenciado por um provedor de serviços terceirizado. Por este motivo, a gerência de recursos e infraestrutura é de responsabilidade do provedor, cabendo ao cliente apenas o acesso pela Internet [9].

Este modelo de nuvem oferece serviços do tipo “pague pelo que usar”, os recursos requisitados pelo cliente são sob demanda. Nesse viés, pode-se destacar vantagens como maior escalabilidade de recursos conforme a necessidade do cliente. Ao contrário da nuvem privada, a pública possui uma grande vantagem financeira, ela reduz de custos da empresa com hardware, software, infraestrutura e manutenção [9]. A Figura 3 mostra o esquema de uma nuvem pública.

Figura 3 - Modelo de nuvem pública



Fonte: SILVA, 2019.

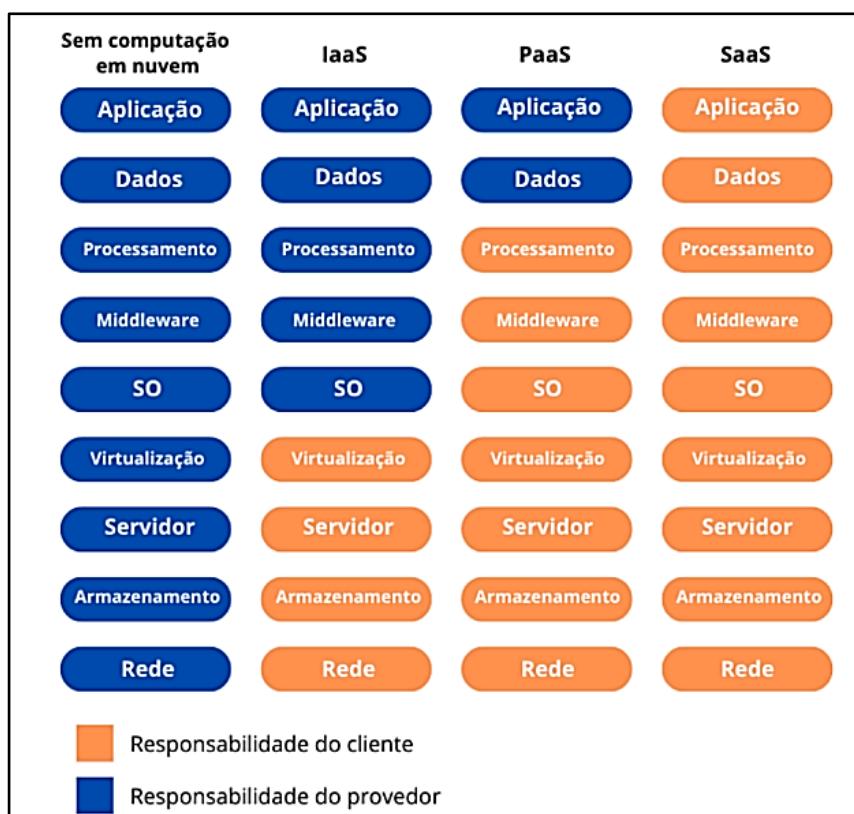
A nuvem híbrida é uma combinação da privada e pública. O uso deste modelo se destaca pela vantagem de aproveitar pontos positivos de ambas, ao mesmo tempo. As organizações podem aproveitar a infraestrutura de uma nuvem privada garantindo maior segurança e mantendo alguns recursos de baixa prioridade na pública [13].

Deste modo, torna-se possível atender necessidades de escalonamentos rápidos para atender alguma demanda, flexibilidade e redução de custo e ao mesmo tempo ter controle sobre seus dados mais sensíveis. No entanto, sua implementação é algo mais complexo. É necessária uma boa equipe de gestão para administrar e integrar as várias plataformas e dados utilizados pela empresa, o que acaba não saindo barato para o cliente [1].

### 1.3 Modelos de serviços

Se tratando dos serviços oferecidos pela computação em nuvem, eles podem ser divididos em três modelos diferentes, sendo eles Infraestrutura como Serviços ou em inglês *Infrastructure as a service* (IaaS), Software como Serviço ou em inglês *Software as a service* (SaaS) e plataforma como serviço ou em inglês *Platform as a service* (PaaS). Cada um destes possui suas vantagens dependendo da demanda de serviços da empresa [7]. A Figura 4 mostra uma comparação entre os modelos, destacando os principais itens fornecidos por cada um.

Figura 4 - Comparação dos modelos de serviço



Fonte: BANDEIRA, 2022.

Para empresas de porte menor, nem sempre era viável financeiramente manter um datacenter próprio na organização. Os recursos que tinham disponíveis não eram utilizados totalmente, então manter gastos com hardwares e manutenções não seria o ideal [14]. Nesse sentido, entra a IaaS oferecendo a infraestrutura necessária para o funcionamento da empresa. Esse serviço é possível devido a virtualização. Com ela o cliente pode acessar os recursos adquiridos tais como armazenamento, processamento, máquinas virtuais entre outros pela Internet [2].

Este serviço se tornou atraente para as empresas devido a vantagem da redução de gastos. O cliente se livra da responsabilidade de cuidar de equipamentos físicos, alugando apenas aquilo que sua demanda carece pelo tempo que for necessário. A provedora de serviços em nuvem fica sendo a responsável pelo gerenciamento da infraestrutura [7].

Um modelo de negócio é muito buscado pela sua integração simplificada e demais vantagens se trata de SaaS. O produto oferecido pelo serviço é software, acessado pela Internet, para realização de diversas tarefas. O cliente não precisa se preocupar com licenças, renovações, atualizações etc., pois tudo isso é de responsabilidade do provedor de serviços [15].

O serviço SaaS se destacou bastante em relação as empresas de softwares convencionais. Enquanto estas necessitavam que seus clientes instalassem o software localmente, com o SaaS isso foi deixado de lado, passando a ser hospedado na nuvem, permitindo que o usuário acesse o software de qualquer dispositivo pela Internet [16].

Buscada principalmente por empresas desenvolvedoras de software, a PaaS diferentemente do SaaS, oferece uma plataforma completa para desenvolvimento na nuvem. Como o próprio nome já diz, o principal item oferecido é uma plataforma bem equipada com ferramentas para desenvolvimento de aplicações [17].

Os clientes que adquirirem esta tecnologia pagam apenas pelo que usam. Os itens a serem contratados podem variar desde apenas sistemas operacionais á plataformas completas com servidores. Eles possuem a disposição banco de dados, ferramentas de desenvolvimento e segurança, middlewares entre outros itens [16].

## **2. Materiais e Métodos**

Este artigo segundo sua natureza é um resumo de assunto. Fundamenta-se em trabalhos da área de conhecimento do projeto, buscando reunir, analisar, avaliar e discutir conhecimentos e informações [18].

De acordo com Pereira [19], segundo seus objetivos este artigo classifica-se como descritivo. Ele é caracterizado pela explicação dos fatos como eles são sem a interferência do pesquisador.

Segundo seus procedimentos técnicos, este artigo é bibliográfico. Estuda-se artigo, teses, livros entre outras publicações. Tal estudo é necessário, pois é com ele que o pesquisador vai fundamentar-se para prosseguir com sua pesquisa [19].

Foi realizada uma revisão bibliográfica em bases como Google Scholar, IEEE Xplore, ABNT Coleção, Periódicos da Capes entre outros. Nestas bases foi possível encontrar artigos, teses, livros, normas, entre outras fontes, sobre o tema para a elaboração deste artigo.

### **3. Resultados e Discussão**

A segurança da computação em nuvem é um assunto importante e existem diversas normas e padrões que estabelecem orientações e melhores práticas para garantir a segurança de dados e sistemas em ambientes de nuvem [3].

ABNT NBR ISO/IEC 27017:2015 é uma norma que desenvolve diretrizes para segurança da informação (SI) em serviços de computação em nuvem. Foi desenvolvida de acordo com a norma ISO/IEC 27002, que é um conjunto de boas práticas para segurança da informação [20].

Esta norma fornece um conjunto de controles de segurança específicos para um ambiente em nuvem, incluindo orientações de como deve ser o gerenciamento de segurança, a governança, o gerenciamento de riscos, o gerenciamento de incidentes, a proteção de dados, privacidade e conformidade. O padrão é aplicado a todos os tipos de serviços oferecidos pela nuvem, e se aplica também a organizações e provedores que usam ou fornecem serviços de computação em nuvem [21].

De acordo com a ABNT [22], o uso da ISO/IEC 27017 ajuda as organizações a manterem as informações seguras em seus ambientes de nuvem, fornecendo uma boa estrutura para a implementação de controles de segurança específicos da nuvem. Além disso, pode ajudar a aumentar a confiança do cliente porque demonstra que as organizações estão tomando as medidas para proteger os dados.

Entre os principais tópicos abordados pela ISO/IEC 27017, pode-se destacar:

- Gerenciamento de segurança: a norma estabelece diretrizes para a definição de políticas e procedimentos para gerenciar a SI em ambientes de nuvem, incluindo a definição de responsabilidades e de papéis.



- Governança: é estabelecido instruções para o estabelecimento de uma estrutura de governança para a SI em ambientes de nuvem, incluindo a definição de objetivos de segurança e a realização de avaliações de riscos.
- Gerenciamento de riscos: a norma fornece orientação para a gestão de riscos em ambientes de nuvem, incluindo a avaliação de riscos, a seleção de controles de segurança e a implementação de medidas de mitigação.
- Gestão de incidentes: a norma estabelece diretrizes para a gestão de incidentes de segurança em ambientes de nuvem, incluindo a definição de procedimentos para detectar, responder e relatar incidentes.
- Proteção de dados: a norma fornece orientação para a proteção de dados em ambientes de nuvem, incluindo a criptografia de dados em trânsito e em repouso, a definição de políticas para o uso de senhas e a realização de backups regulares.
- Privacidade: a norma estabelece diretrizes para a proteção da privacidade em ambientes de nuvem, incluindo a definição de políticas e procedimentos para o tratamento de informações pessoais.
- Conformidade: a norma fornece orientação para garantir a conformidade com requisitos regulatórios e legais em ambientes de nuvem.

Nesse contexto, a ISO/IEC 27017 é um padrão importante para a SI de serviços de computação em nuvem porque fornece uma estrutura clara para a implementação de controles de segurança específicos da nuvem. Esta norma complementa outras normas da série ISO/IEC 27000, como a ISO/IEC 27001 e a ISO/IEC 27002, que fornecem orientação para a implementação de sistemas de gerenciamento de segurança da informação [20].

A ISO/IEC 27017 foi desenvolvida por especialistas em segurança da informação de todo o mundo para ajudar as organizações a enfrentar os desafios específicos da SI em ambientes de nuvem. A norma é aplicável a organizações de todos os setores e portes, podendo ser utilizada em conjunto com outras normas e regulamentações, como a Lei Geral de Proteção de Dados (LGPD) do Brasil e o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia [23].

De acordo com a ABNT NBR ISO/IEC 27018:2019 [24], esta norma técnica estabelece requisitos para a proteção da privacidade de dados pessoais em nuvens públicas, com base nos princípios estabelecidos na ISO/IEC 27002 e na Lei Geral de Proteção de Dados (LGPD).

É definido um guia composto por um conjunto de diretrizes que os provedores de serviços de computação em nuvem e os clientes devem seguir para garantir a proteção dos dados pessoais armazenados em nuvens públicas. Dentre as principais diretrizes desenvolvidas por esta norma, destacam-se [24]:

**Política de privacidade:** uma política clara e compreensível para os provedores de serviços de nuvem pública processarem dados pessoais, incluindo informações como a finalidade do processamento, o tipo de dados coletados, as medidas de segurança aplicadas e os direitos dos titulares dos dados.

**Segurança da Informação:** são medidas de segurança para proteger os dados pessoais armazenados em nuvens públicas contra acesso não autorizado ou divulgação de informações. Os provedores de serviços de nuvem pública devem garantir a integridade e a confidencialidade dos dados pessoais e tomar medidas para garantir a disponibilidade dos dados.

**Gerenciamento de incidentes:** estabelece um procedimento claro de notificação de violação de dados, determine a causa raiz de um incidente e implemente ações corretivas para evitar futuras violações. Os provedores de serviços de nuvem pública devem notificar imediatamente os clientes e departamentos relevantes em caso de violação de dados e ter planos de contingência para lidar com incidentes de segurança.

**Governança de dados:** estabelece uma responsabilidade clara entre provedores de serviços de nuvem pública e clientes e defina práticas para coletar, armazenar e processar dados pessoais. Os provedores de serviços de nuvem pública devem garantir que as práticas de proteção de dados estejam em conformidade com a LGPD e outras leis aplicáveis.

A implementação da ABNT NBR ISO/IEC 27018:2019 é importante para garantir a privacidade dos dados pessoais na nuvem pública e cumprir as obrigações legais relacionadas à proteção de dados. Ao seguir as diretrizes definidas na norma, os provedores de serviços de nuvem pública podem garantir a confiança e a satisfação de seus clientes, além de proteger sua reputação e evitar sanções legais por violações de privacidade [25].

Tenelema [26] aborda alguns exemplos práticos de implementação destas normas. Pode-se destacar situações como o controle de acesso dos usuários. As normas recomendam controles de segurança que se seguidos evita que usuários não autorizado tenham acesso aos dados em nuvem. Outro exemplo é sobre a detecção e tratamento de ameaças, com o devido preparo a empresa conseguira lidar com mais eficiência a ataques e mitigá-los. Por fim, há também a proteção de dados dos clientes, as normas recomendam padrões a serem seguidos para evitar problemas como, por exemplo, vazamento de dados.

#### **4. Conclusão**

O objetivo geral deste artigo foi o de apresentar uma visão geral sobre a computação em nuvem, além de mostrar como as normas ABNT NBR ISO/IEC 27017 e 27018 garantem a segurança neste ambiente.

Houve um grande aumento do uso de serviços de computação em nuvem pelas empresas, a fim de diminuir os custos e aumentar a eficiência. Apesar das vantagens do uso da computação em nuvem é importante perceber que isso tudo torna o quesito segurança extremamente necessário. Logo, as práticas de segurança contra riscos existentes se tornaram algo essencial para evitar perdas, alterações e compartilhamento de dados.

A segurança em nuvem inclui a implementação de medidas para garantir que os dados armazenados e processados na nuvem sejam protegidos. Esta é uma responsabilidade tanto do provedor de serviços em nuvem como do cliente. O provedor é responsável por proteger a infraestrutura da nuvem e o cliente é responsável por proteger seus dados na nuvem. É essencial que ambos os lados cumpram suas responsabilidades para garantir a segurança dos dados.

O estudo permitiu concluir que o uso de normas como a ABNT NBR ISO/IEC 27017 e 27018 podem ajudar a manter tais dados seguros e aumentar a confiança na tecnologia de segurança. As normas estabelecem diretrizes e orientações para tratar os serviços e as informações no ambiente em nuvem. Mesmo não sendo obrigatórias, seguir estes padrões trazem maior segurança para o ambiente em nuvem e para a privacidade dos dados.

O uso das normas pode trazer muitos benefícios como a redução do chances de violações de segurança, aumento da confiança do cliente. O padrão também pode ajudar as organizações a aumentarem a eficiência operacional e reduzir custos, estabelecendo uma estrutura clara para a implementação de controles de segurança específicos da nuvem.

## 5. Referências Bibliográficas

1. Santos, T.: Fundamentos da computação em nuvem. São Paulo: Senac; 2018. E-book.
2. Coutinho, A. A. T. R. et al. **Computação em Névoa: Conceitos, Aplicações e Desafios**. In: XXXIV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, 34, Anais: Sociedade Brasileira de Computação (SBC). pp. 266-315., Salvador, Bahia (2016).
3. De Paula, L.; Dian, M. de O.: **COMPUTAÇÃO EM NUVEM: os desafios das empresas ao migrar para a nuvem**. Revista Interface Tecnológica, 18(2), 304–315; (2021). DOI: 10.31510/inf. v18i2.1304.
4. Rosy, M. A. et al.: **Challenges, service models and deployment models of cloud computing**. JETIR Journal. Acesso em: 07 de setembro de 2022; pp.81-86. Disponível em: <<https://www.jetir.org/papers/JETIRDD06016.pdf>>.
5. Gislaine, P. F. **Requisitos para análise de segurança da informação em provedores de serviços em nuvem**. Informação & Tecnologia (ITEC). Acesso em: 02 novembro de 2022. 4(1), 89-109, (2017).
6. Alecrim, E.: **O que é tecnologia da informação (TI)?** INFOWESTER, São Paulo (2019). Acesso em: 28 de fevereiro de 2023. Disponível em: <https://www.infowester.com/ti.php>.
7. Rashid, A.; Chaturvedi, A.: **Cloud computing characteristics and services: a brief review**. International Journal of Computer Sciences and Engineering. Acesso em: 21 mar. 2023. 7(2). Disponível em: [https://www.researchgate.net/profile/Aaqib-Rashid/publication/331731714\\_Cloud\\_Computing\\_Characteristics\\_and\\_Services\\_A\\_Brief\\_Review/links/5c89f6c045851564fadca23f/Cloud-Computing-Characteristics-and-Services-A-Brief-Review.pdf](https://www.researchgate.net/profile/Aaqib-Rashid/publication/331731714_Cloud_Computing_Characteristics_and_Services_A_Brief_Review/links/5c89f6c045851564fadca23f/Cloud-Computing-Characteristics-and-Services-A-Brief-Review.pdf).
8. Martins, I. M. A.: A imputação de ciberataques aos Estados. 2022. Tese de Doutorado. Lisboa: Universidade Católica Portuguesa (2022).
9. Lorenzi, U. M., De Brito, W. G., Corcini, L. F.: **Computação em nuvem: conceitos, aplicações e novas tecnologias**. Revista das Faculdades Santa Cruz, 13(1), (2022).
10. Tavbulatova, Z. K. et al.: *Types of cloud deployment*. Journal of Physics: Conference Series. Acesso em: 14 março 2023. 012085. Disponível em: <https://iopscience.iop.org/article/10.1088/1742-6596/1582/1/012085/pdf>.
11. Nasereddin, H.: **Building of Private Cloud Computing Architecture to Support E-Learning**. High Technol, Acesso em: 14 mar. 2023. 26. Disponível em: [https://www.researchgate.net/profile/Hebah-H-O-Nasereddin/publication/348419926\\_Building\\_of\\_Private\\_Cloud\\_Computing\\_Architecture\\_to\\_Support\\_E-Learning/links/5ffe2f2e299bf140888f8be7/Building-of-Private-Cloud-Computing-Architecture-to-Support-E-Learning.pdf](https://www.researchgate.net/profile/Hebah-H-O-Nasereddin/publication/348419926_Building_of_Private_Cloud_Computing_Architecture_to_Support_E-Learning/links/5ffe2f2e299bf140888f8be7/Building-of-Private-Cloud-Computing-Architecture-to-Support-E-Learning.pdf).
12. Fernandes, M. A. P. et al.: Engenharia de produção: tecnologia e inovação em pesquisa. Vol 2. São Paulo: Científica Digital, 2022.
13. Silva, A. J.: **Segurança de informação no ambiente da computação na nuvem**. Revista Primeira Evolução. Acesso em: 09 abril 2023. 1(38). Disponível em: <http://primeiraevolucao.com.br/index.php/R1E/article/view/393>.
14. Avinte, E. F.: **Cloud computing: reducing costs in small and medium business**. Journal of Engineering and Technology for Industrial Applications, 5(18), 5-17; (2019).

15. Loukis, E. S., Janssen, M., Mintchev, I.: *Determinants of software-as-a-service benefits and impact on firm performance*. *Decision Support Systems*, 117, 38-47; (2019).
16. Martins, R. E.: **Fundamentos da ciência da computação 2**. Vol. 2. Ponta Grossa: Atena Editora, 2019.
17. Kolb, S.: *On the Portability of Applications in Platform as a Service*. Bamberg: University of Bamberg Press, 2019.
18. Rodrigues, A. J.: **Metodologia científica: completo e essencial para a vida universitária**. São Paulo: Avercamp, 2006.
19. Pereira, A. S. et al: **Metodologia de pesquisa científica**. Santa Catarina: UFSM/NTE, 2018.
20. Tabosa, F. G. F.: Avaliação da evolução pós-pandemia da propensão ao enfrentamento de riscos de computação em nuvem por gestores da Administração Pública Federal. Dissertação de mestrado profissional. Brasília: Universidade de Brasília (2022).
21. Borges, F. A. N., Silva, G. S. T.: **Proposta de modelo de migração de sistemas on-premises para nuvem pública no Brasil**. Trabalho de conclusão de curso. Brasília: Universidade de Brasília (2019).
22. ABNT. Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27017:2015: Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem. Rio de Janeiro, 2015.
23. De Almendra Freitas, C. O.: **Riscos e proteção de dados pessoais**. Revista Rede de Direito Digital, Intelectual & Sociedade. Acesso em: 15 abr. 2023; v2(4). (2022). Disponível em: <https://revista.ioda.org.br/index.php/trddis/article/view/74>.
24. ABNT. Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27018:2019: Tecnologia da informação - Técnicas de segurança - Código de prática para proteção de dados pessoais (DP) em nuvens públicas que atuam como operadores de DP. Rio de Janeiro, 2019.
25. Aleixo, M. R.: **Alinhamento das práticas da gestão e curadoria da informação com as da segurança da informação**. Tese de Doutorado. Lisboa: Universidade Nova de Lisboa (2020).
26. Tenelema, A.; Esthela, N.: *Implementación de un modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube con base en las normas ISO 27017 y 27018*. Mestrado: Escola Politécnica de Chimborazo (2020).