UNIVERSIDADE FEDERAL FLUMINENSE
JÉSSICA LIMA GOMES DE SOUZA

COMPUTAÇÃO EM NUVEM: PRINCIPAIS CONSIDERAÇÕES SOBRE SEGURANÇA

Niterói
2016

JÉSSICA LIMA GOMES DE SOUZA

COMPUTAÇÃO EM NUVEM: PRINCIPAIS CONSIDERAÇÕES SOBRE SEGURANÇA

Trabalho de Conclusão de Curso submetido ao Curso de Tecnologia em Sistemas de Computação da Universidade Federal Fluminense como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Computação.

Orientador (a):
JULIANA MENDES NASCENTE E SILVA ZAMITH

NITERÓI
2016

Ficha Catalográfica elaborada pela Biblioteca da Escola de Engenharia e Instituto de Computação da UFF

S729 Souza, Jéssica Lima Gomes de
Computação em nuvem : principais considerações sobre segurança / Jéssica Lima Gomes de Souza. – Niterói, RJ : [s.n.], 2016.
75 f.

Projeto Final (Tecnólogo em Sistemas de Computação) – Universidade Federal Fluminense, 2016.
Orientadora: Juliana Mendes Nascente e Silva Zamith.

1. Computação em nuvem. 2. Segurança da informação. 3. Tecnologia da informação. I. Título.

CDD 004.36

JÉSSICA LIMA GOMES DE SOUZA

COMPUTAÇÃO EM NUVEM: PRINCIPAIS CONSIDERAÇÕES SOBRE SEGURANÇA

Trabalho de Conclusão de Curso submetido ao Curso de Tecnologia em Sistemas de Computação da Universidade Federal Fluminense como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Computação.

Niterói, ___ de _____ de 2016.

Banca Examinadora:

_____

Prof.ª Juliana Mendes N S Zamith, DSc. – Orientadora

UFF – Universidade Federal Fluminense

_____

Prof. Bruno José Dembogurski, DSc. – Avaliador

UFRRJ – Universidade Federal Rural do Rio de Janeiro

AGRADECIMENTOS

A Deus, dedico o meu maior agradecimento, pelo maravilhoso presente que é a vida e pelas oportunidades concedidas ao longo dessa caminhada.

A minha Orientadora Prof.ª Juliana Mendes Nascente e Silva Zamith por suas correções, incentivos e toda a atenção que me concedeu, durante a elaboração deste trabalho.

Aos meus pais, irmã e avós, pelo amor, incentivo, apoio incondicional e compreensão nos momentos que precisei estar ausente.

Aos meus amigos por todo apoio dado, em particular meu namorado, Pedro Filipe, que de uma forma especial, me deu força e coragem, fundamentais no decorrer do curso.

“As tecnologias mais importantes são aquelas que desaparecem. Elas se integram à vida no dia a dia até serem indistinguíveis dele.”
Mark Weiser

RESUMO

A Computação em Nuvem possui notável potencial para fornecer serviços de forma econômica, elástica e de fácil gerenciamento. Oferecendo ao mercado um ambiente de armazenamento de dados e a capacidade de processamento computacional escalável, atendendo conforme a demanda. Os benefícios mencionados e muitos outros despertaram as organizações para a adoção desse modelo em seus negócios. No entanto, uma implementação bem-sucedida, requer o gerenciamento efetivo da segurança nas aplicações em nuvem, pois a alocação de informações fora do controle administrativo e em um ambiente compartilhado, implica em ameaças adicionais à segurança. O objetivo deste trabalho é fornecer conhecimento aos usuários que desejam adotar a Nuvem. Elaborado através de pesquisas em livros, artigos e em publicações de empresas conceituadas no mercado de TI. A fim de proporcionar uma perspectiva global dos conceitos dessa tecnologia, como também seus benefícios e riscos. Ela aborda principalmente as questões de segurança peculiares, decorrentes das características diferenciadas da Computação em Nuvem, que devem ser devidamente abordadas e gerenciadas para que todos os potenciais benefícios oferecidos, sejam alcançados seguramente. Foi possível destacar também a situação mundial e em específico a do Brasil, quanto a adoção da Computação em Nuvem, incluindo suas perspectivas futuras.

Palavras-chaves: Computação em Nuvem, Segurança da Informação, Riscos.

ABSTRACT

Cloud Computing has remarkable potential to deliver services in a cost-effective, elastic, and manageable way. Providing the market with a data storage environment and scalable computing power that will meet demand. The mentioned benefits and many others have awakened organizations to the adoption this model in their business. However, a successful implementation requires the effective management of security in the cloud applications, since the allocation of information outside of administrative control and in a shared environment implies additional security threats. The objective of this work is to provide knowledge to users who wish to adopt the Cloud. Elaborated through researches in books, articles and publications of reputable companies in the IT market. In order to provide a global perspective on the concepts of this technology, as well as its benefits and risks. It addresses mainly the specific security issues arising from the differentiated characteristics of Cloud Computing and should be properly addressed and managed so that all the potential benefits offered are safely achieved. It was also possible to highlight the world situation and specifically Brazil, regarding the adoption of Cloud Computing, including its future perspectives.

Key words: Cloud Computing, Information Security, Risks.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACCA – *Asia Cloud Computing Association*

ACL – *Access Control List*

API – *Application Programming Interface*

APTs – *Advanced Persistent Threats*

ATM – *Asynchronous Transfer Mode*

AWS – *Amazon Web Service*

CDN – *Content Delivery Network*

CEO – *Chief Executive Officer*

COSO's – *Committee of Sponsoring Organizations of the Treadway Commission*

CSA – *Cloud Security Alliance*

CSRF – *Cross-Site Request Forgery*

DaaS – *Data as a Service*

DDoS – *Distributed Denial of Service*

DLP – *Data Loss Prevention*

DoS – *Denial of Service*

EUA – Estados Unidos da América

HTTPS – *Hyper Text Transfer Protocol Secure*

IaaS – *Infrastructure as a Service*

IBM – *International Business Machines*

IDaaS – *Identity as a Service*

IDS – *Intrusion Detection System*

IoT – *Internet of Things*

IPS – *Intrusion Prevention System*

IPSec – *IP Security Protocol*

NaaS – *Network as a Service*

NIST – *National Institute of Standards and Technology*

OWASP – *Open Web Application Security Project*

PaaS – *Platform as a Service*

PME – Pequenas e médias empresas

SaaS – *Software as a Service*

SecaaS – *Security as a Service*

SERPRO – Serviço Federal de Processamento de Dados

SFTP – *SSH File Transfer Protocol*

SISP – Sistema de Administração dos Recursos de Tecnologia da Informação

SLA – *Service Level Agreement*

SSL – *Secure Socket Layer*

TI – Tecnologia da Informação

TLS – *Transport Layer Security*

UIs – *User Interfaces*

USB – *Universal Serial Bus*

VPN – *Virtual Private Network*

XSS – *Cross-Site scripting*

SUMÁRIO

1 INTRODUÇÃO

O avanço tecnológico dos últimos anos e a necessidade de recursos computacionais compartilhados, com alta disponibilidade, acessibilidade e grande capacidade de armazenamento, contribuíram para a expansão da utilização da Computação em Nuvem (*Cloud Computing*, em inglês). Um modelo que surgiu para atender estas necessidades, tornando os recursos computacionais mais flexíveis e acessíveis, permitindo a redução de custos com equipamentos.

A proporciona um fácil acesso aos serviços ou recursos computacionais, independentemente da plataforma e da arquitetura. Os usuários têm a ilusão de que os recursos computacionais e armazenamento de dados são infinitos. Os serviços oferecidos pelo provedor da nuvem são escaláveis, ou seja, um usuário que inicialmente contratou um serviço simples pode expandir quando necessário, de uma maneira mais fácil e com um gasto menor caso utilizasse o modelo tradicional de *hardware* próprio. Nessa nova tecnologia o fornecimento da infraestrutura, plataforma e *softwares* como serviço são sob demanda, com o pagamento baseado no uso [1].

Apesar das inúmeras vantagens, ainda existe resistência, por parte das empresas, para a migração para esse novo modelo. O mercado brasileiro apresenta desafios a serem considerados. De acordo com vários observadores da indústria e usuários do mercado, o maior deles é a preocupação com a confidencialidade e segurança dos dados armazenados na nuvem [2].

Tendo em vista esse grande desafio, ciente que a proteção de dados é de grande importância para a utilização de recursos computacionais de forma segura, o presente trabalho visa estudar os principais modelos e procedimentos de segurança e privacidade das informações que estão armazenadas na nuvem.

O trabalho se organiza como segue. O Capítulo 2 aborda os conceitos de Computação em Nuvem, seus modelos de serviço, modelos implantação e principais atores. No Capítulo 3 serão estudados os benefícios e os riscos da nuvem. A questão da

segurança em ambientes na nuvem será abordada no Capítulo 4. O cenário atual Mundial e Brasileiro quanto a adoção da Computação em Nuvem no Capítulo 5. O Capítulo 6 apresenta os principais provedores de infraestrutura em Nuvem. Finalmente o Capítulo 7 apresenta a conclusão do trabalho e possíveis trabalhos futuros.

2 CONCEITOS DE COMPUTAÇÃO EM NUVEM

A ideia principal da Computação em Nuvem não é recente, na década de 1960, o John McCarthy havia previsto que as instalações de computação seriam fornecidas ao público como um utilitário (*computing as a utility*). No entanto, o termo "*Cloud Computing*" ganhou popularidade em 2006, quando foi utilizado em uma palestra de Eric Schmidt, ex-CEO da Google, que apresentava como era a gerência de seus centros de dados [3].

O termo "nuvem" já era utilizado em diversos contextos, descrevendo grandes redes de ATM (*Asynchronous Transfer Mode*), desde 1990 [3]. Atualmente, "nuvem" é uma representação para a internet ou infraestrutura de comunicação entre os componentes arquiteturais, baseada em uma abstração que oculta a complexidade da infraestrutura. Esta infraestrutura é composta por um número elevado de máquinas físicas ou nós físicos, conectados através de uma rede. Parte dessa infraestrutura é disponibilizada como serviço e geralmente armazenadas em centro de dados, com o *hardware* compartilhado para computação e armazenamento [4].

Segundo Vaquero [5], a Computação em Nuvem é um grande conjunto de recursos virtuais, que são facilmente utilizáveis e acessíveis, como *hardware*, plataformas e serviços. Os recursos podem ser reconfigurados de forma dinâmica, conforme a carga de trabalho, permitindo que seu uso seja otimizado. Este conjunto de recursos é normalmente disponibilizado por um modelo de "pague-pelo-uso", onde somente são pagos os recursos solicitados durante o tempo de uso.

A utilização da nuvem possibilita que os usuários executem suas aplicações sem que seja necessário o uso de máquinas com alto desempenho, o que poderia ser necessário para execução de algumas aplicações alocadas localmente, pois o trabalho computacional é realizado na nuvem. Dessa forma, a máquina do usuário tem como finalidade a inserção de dados e exibição de resultados [6].

O *National Institute of Standards and Technology* (NIST) divulgou em janeiro de 2011, uma definição para Computação em Nuvem, que se tornou a mais aceita na comunidade acadêmica e que cobre os aspectos essenciais desse modelo. Ele o de-

finiu como um modelo que possibilita acesso à rede de maneira onipresente, conveniente e sob demanda, como também à um conjunto de recursos de computação compartilhado, que são configuráveis e que permitem serem alocados e liberados rapidamente com esforço mínimo de gerenciamento ou interação com o provedor de serviço [7].

O modelo de Computação em Nuvem, definido pelo NIST, é composto ainda por suas cinco características essenciais, como também três modelos de serviço e quatro modelos de implantação, que serão abordados a seguir.

2.1 CARACTERÍSTICAS ESSENCIAIS

Características essenciais demonstram as vantagens oferecidas pela Computação em Nuvem. Algumas características, em conjunto, trazem a definição dessa tecnologia, distinguindo-a de outros paradigmas [4].

Segundo o NIST [7], o modelo estudado deve conter as seguintes características essenciais:

- **Autoatendimento sob demanda:** Recursos computacionais, como armazenamento no servidor ou tempo de processamento, podem ser adquiridos unilateralmente, à medida que houver necessidade, sem a interação humana com o prestador de serviço [7].

- **Acesso amplo a serviços de rede:** Recursos computacionais são disponibilizados através da rede e acessados por mecanismos padronizados, possibilitando a utilização por computadores e diversos dispositivos [7].
  A interface de acesso à nuvem, permite que os usuários mantenham suas condições e ambientes de trabalho, como sistemas operacionais ou linguagens de programação. Já que os *softwares* clientes que são instalados nas estações locais, para realizar o acesso à nuvem são leves, como um navegador de Internet [4].

- **Pool de recursos:** Os recursos do provedor são organizados para servir a múltiplos usuários, utilizando o modelo *Multi-tenancy* ou Multi-inquilino, onde os recursos computacionais, físicos e virtuais, são dinamicamente alocados e realocados conforme a demanda dos usuários. Os usuários não precisam ter a ciência de onde está localizado fisicamente os recursos disponibilizados, podem apenas especificar a localização em um nível mais alto de abstração, tais como o país, estado ou centro de dados [7].

- **Rápida elasticidade:** Recursos computacionais podem ser disponibilizados rápido e elasticamente. Em alguns casos, de acordo com a demanda de consumo, podem ser automaticamente liberados. A impressão dos usuários é que possuem recursos ilimitados, que podem ser adquiridos em qualquer momento e quantidade [7].

- **Serviços mensuráveis:** Os sistemas em nuvem controlam automaticamente e monitoram o uso dos recursos através de uma medição, para cada tipo de serviço, como armazenamento, processamento, largura de banda e contas de usuários. O monitoramento é realizado de forma transparente para o provedor de serviços, assim como para o usuário do serviço utilizado [7].

O guia da *Cloud Security Alliance* [8], indica também como característica da Computação em Nuvem, a arquitetura *Multi-tenancy* ou Multi-inquilino, apesar de não ser referenciada como uma característica essencial pelo NIST.

Na Arquitetura Multi-inquilino, recursos computacionais ou aplicações são utilizados por múltiplos consumidores, pertencentes a uma mesma organização ou distintas. Cada inquilino interage com a aplicação como se fosse o único usuário utilizando-a, sendo assim um inquilino não pode acessar ou visualizar dados de outro inquilino [8].

Segundo Veras [9], trata-se de uma arquitetura de aplicações onde apenas uma instância do *software* é executada em um centro de dados e diversos inquilinos podem acessá-la.

Modelos de serviço em nuvem, com arquitetura Multi-inquilino implicam na aplicação de políticas, governança, segmentação, isolamento, níveis de serviços para o acesso distinto dos usuários e modelos de faturamento para determinado consumo [8].

Aos provedores de nuvem, são sugeridos a adoção de um *design* e arquitetura que possibilite economias de escala, disponibilidade, gestão, segmentação, isolamento e eficiência operacional, usufruindo do compartilhamento de dados, serviços, aplicações e infraestrutura por meio de vários consumidores distintos [8].

2.2 MODELOS DE SERVIÇO

Ambientes computacionais em nuvens são compostos por três modelos de serviços, que definem um padrão arquitetural para essa solução [10]. São classificados de acordo com os recursos fornecidos ao usuário e como são utilizados.

2.2.1 SOFTWARE COMO UM SERVIÇO (SaaS)

O consumidor utiliza as aplicações que são fornecidas pelo provedor, que funcionam hospedadas em uma infraestrutura na nuvem. Podendo ser acessadas por vários dispositivos do cliente, por meio de uma interface do *thin client*, como o *browser*. A administração e gerenciamento da infraestrutura básica, como a rede, sistemas operacionais, servidores, armazenamento ou características individuais da aplicação, exceto configurações que são específicas, não são realizados pelo consumidor, e sim pelo provedor do serviço [7]. Permitindo que o cliente concentre seus projetos para inovação em seus sistemas e não na infraestrutura.

O modelo SaaS, proporciona serviços na camada de aplicação, podendo ser executado completamente em nuvem, sendo assim uma alternativa a executar um

software em uma estação local. Este modelo leva a redução de custos, pois dispensa a aquisição de licença de sistemas de *softwares*.

2.2.2 PLATAFORMA COMO UM SERVIÇO (PaaS)

O modelo de PaaS oferece sistema operacional, linguagens de programação, e um ambiente para o desenvolvimento das aplicações. Fornecendo ao consumidor um auxílio para implementar sistemas. A gerência e controle da infraestrutura, não são permitidas ao usuário, pois somente terão controle sobre as aplicações que foram implantadas e, possivelmente, as configurações de aplicações hospedadas [7].

O objetivo desse modelo é criar uma plataforma para desenvolvimento de aplicações, para facilitar e agilizar o processo de implantação de aplicações sem os custos e complexidade de gerenciamento do *hardware*.

2.2.3 INFRAESTRUTURA COMO UM SERVIÇO (IaaS)

O IaaS tem como objetivo o fornecimento de recursos como, servidores, armazenamento, rede e outros recursos fundamentais para construção de um ambiente de aplicação sob demanda. Provendo a infraestrutura necessária para o PaaS e o SaaS. O consumidor não possui gerência ou controle da infraestrutura, mas possui controle dos sistemas operacionais, armazenamento e aplicativos implantados. Possivelmente, possui um controle limitado dos componentes de rede [7].

2.3 MODELOS DE IMPLANTAÇÃO

Segundo o NIST [7], existem quatro principais modelos de implantação de Computação em Nuvem, listadas a seguir.

2.3.1 NUVEM PRIVADA

A utilização da infraestrutura de uma nuvem privada, é exclusivo de uma organização. A gerência pode ser realizada pela própria empresa ou terceiros, que podem estar no local ou remotamente [7].

Políticas de acesso aos serviços são empregadas neste modelo, que possui como principais características, gerenciamento de redes, configurações dos provedores de serviços e a utilização de tecnologias de autenticação e autorização.

2.3.2 NUVEM PÚBLICA

Modelo de implantação onde a infraestrutura é de uso aberto para o público em geral, onde qualquer usuário pode acessar. Pode ser gerenciada e operada por uma empresa, comunidade acadêmica ou organização governamental [7].

Como neste modelo a infraestrutura é disponibilizada ao público, não são aplicadas restrições de acesso quanto ao gerenciamento de redes, técnicas para autenticação e autorização.

2.3.3 NUVEM COMUNITÁRIA

No modelo de implantação comunitária, a infraestrutura de nuvem é compartilhada por organizações, sendo a nuvem suportada por uma comunidade específica que partilha interesses em comum, tais como missão, requisitos de segurança, políticas e considerações sobre flexibilidade. Este modelo pode existir localmente ou remotamente, podendo ser gerenciada por uma empresa da comunidade ou terceiros [7]. A utilização das políticas de segurança e tecnologias de autenticação e autorização são semelhantes ao modelo de Nuvem privada.

2.3.4 NUVEM HÍBRIDA

As Nuvens Híbridas são compostas de duas ou mais nuvens (privada, comunitária ou pública) que permanecem como entidades únicas, ligadas por uma tecnologia padronizada ou proprietária, que permite a portabilidade de dados e aplicações [7].

2.4 ATORES DA COMPUTAÇÃO EM NUVEM

A arquitetura de referência proposta pelo NIST, é um modelo conceitual de alto nível. Ela apresenta a definição dos cinco atores principais (pessoa ou organização) e como eles atuam na Computação em Nuvem.

A Figura 1 permite uma visão geral da arquitetura de referência, demonstrando as atividades e funções de cada ator.

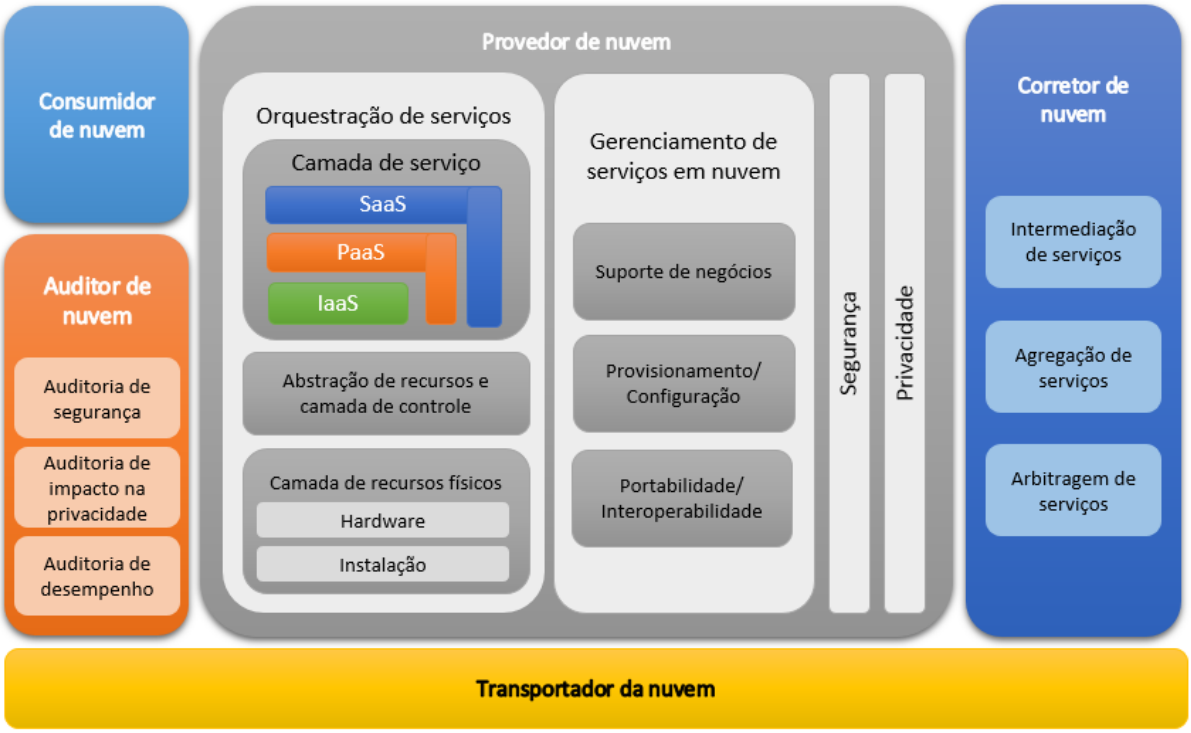

Figura 1: Concepção do Modelo de Referência do NIST [7]

2.4.1 CONSUMIDOR

O consumidor da nuvem, trata-se do indivíduo ou organização que possui interesse no produto final fornecido pela nuvem. O seu papel é utilizar o serviço que foi solicitado a um provedor de nuvem, podendo ser faturado pelo serviço utilizado [7].

A forma de utilização dos recursos poderá ser distinta entre os consumidores, de acordo com os serviços solicitados, como pode ser observado em cada modelo de serviço [7]:

- Serviços SaaS, geralmente são hospedados e os consumidores acessam através de uma rede que os conecta com o provedor do serviço. Os consumidores poderão ser os usuários finais, os administradores da aplicação ou a organização que disponibiliza o acesso a aplicação a todos os membros. O acesso e uso dos serviços são sob demanda.
- Os consumidores que utilizam serviços PaaS, podem usar os recursos para desenvolver, testar, implementar e gerenciar os seus aplicativos que estão hospedados na nuvem.
- Os consumidores de serviços IaaS, possuem acesso às máquinas virtuais, armazenamento, componentes de infraestrutura de rede e outros recursos computacionais que são fundamentais.

2.4.2 PROVEDOR

O provedor é responsável por disponibilizar serviços em nuvem, podendo ser um indivíduo ou uma organização. Os serviços podem ser *softwares*, plataformas e serviços de infraestrutura. De acordo com o modelo de serviço oferecido, o provedor desempenhará tarefas distintas, são elas [7]:

- Para o modelo de serviço SaaS, o provedor é responsável pela implantação, configuração e atualização dos *softwares* em nuvem que ele disponibiliza. Já os consumidores possuem o controle administrativo limitado das aplicações.

- Para o modelo de serviço PaaS, o provedor de nuvem gerencia uma plataforma, provendo ferramentas e recursos para os consumidores desenvolverem, testarem, implantarem e administrarem seus aplicativos. Esse tipo de serviço permite aos consumidores o controle sobre as aplicações e sobre as configurações do ambiente de hospedagem, mas não podem acessar a infraestrutura da plataforma, como rede, sistema operacional ou armazenamento.
- Para o modelo de serviço IaaS, é responsabilidade do provedor de uma nuvem, o processamento físico, o armazenamento, as redes e outros recursos computacionais fundamentais, também como o gerenciamento do ambiente de hospedagem. Nesse modelo, os consumidores implantam, executam aplicativos, e possuem um controle maior sobre o ambiente e sobre a operação de hospedagem, mas não controlam a infraestrutura.

2.4.3 AUDITOR

Segundo o NIST [7], o auditor de nuvem pode realizar avaliações de serviços, desempenho e segurança de uma implementação em nuvem.

As organizações possuem controles de segurança, que são o gerenciamento, técnicas, garantias ou contramedidas operacionais, com o objetivo de proteger a confidencialidade, integridade e disponibilidade de seus sistemas e informações.

A auditoria de segurança pode ser realizada através de uma avaliação dos controles de segurança, para verificar se estão implementados corretamente, funcionando como o previsto e gerando o resultado desejado, respeitando as regras de segurança para o sistema. Verificando também se o sistema está conforme a regulamentação e a política de segurança.

2.4.4 CORRETOR

O consumidor pode realizar o contato com o corretor para solicitar o serviço de nuvem, ao invés de ir diretamente ao provedor. O corretor de nuvem irá gerenciar o uso, o desempenho e a entrega dos serviços em nuvem. Realizando negociações entre provedores e consumidores [7].

O corretor geralmente fornece três tipos de serviços, são eles [7]:

- **Intermediação do serviço:** O corretor pode melhorar o serviço fornecido, aumentando o valor do mesmo. Algumas dessas melhorias podem ser, gerenciamento de identidade, relatórios de desempenho e melhor segurança.
- **Agregação de serviço:** O corretor realiza a integração de serviços. Ele oferece uma integração e movimentação segura dos dados, entre o consumidor e outros provedores.
- **Arbitragem do Serviço:** Permite a integração de serviços, mas possui a flexibilidade de escolher serviços de várias agências.

2.4.5 TRANSPORTADOR

Para o NIST [7], o transportador realiza uma intermediação entre os consumidores e provedores, fornecendo a conectividade e o transporte dos serviços.

Um agente de transporte pode realizar a distribuição de serviços em nuvem, assim como as operadoras de rede e de telecomunicações. O agente de transporte, trata-se de uma organização fornecedora de transporte físico de armazenamento, como discos rígidos com alta capacidade.

Um provedor define um acordo do nível de serviço com um portador de nuvem, para que os serviços sejam fornecidos de maneira consistente aos consumidores, podendo exigir que o transportador de nuvem forneça conexões criptografadas entre provedores e consumidores.

3 BENEFÍCIOS E RISCOS DA COMPUTAÇÃO EM NUVEM

A Computação em Nuvem têm sido uma grande estratégia para empresas, pois vem ganhando cada vez mais espaço no mercado oferecendo uma série de benefícios para os seus usuários. Porém é importante também compreender os seus potenciais riscos.

Esse capítulo irá detalhar os principais benefícios que a esse modelo pode oferecer e os riscos que ele pode apresentar.

3.1 BENEFÍCIOS

A Computação em Nuvem apresenta inúmeros benefícios que a tornam um modelo adequado para muitas organizações, alguns deles são:

Economia

O modelo utilizado pela Computação em Nuvem, onde os usuários pagam apenas pelos recursos que forem usados, permite grande economia para os consumidores, como também fornece facilidade para os que estão iniciando, pois não necessitam investir em infraestruturas tecnológicas, apenas alugam os recursos na nuvem que atendam suas necessidades [3].

O investimento em infraestruturas tecnológicas demanda um planejamento do consumo em períodos de uso elevado, resultando em tecnologias subutilizadas quando a demanda normaliza. Com a utilização da nuvem, pagando de acordo com o utilizado, o investimento que seria empregado em infraestruturas pode ser realocado para oportunidades operacionais [11].

Segundo Veras [9], a economia em escala é um dos mais importantes benefícios dessa tecnologia, e ela se dá em três âmbitos distintos, do lado do fornecimento, da demanda e da arquitetura Multi-inquilino.

A economia de escala no âmbito do fornecimento, se dá pela redução do custo de energia, pois os provedores poderão escolher a localidade que terão um menor custo com eletricidade. Também pela redução dos custos de pessoal, pois um grupo menor poderá administrar mais servidores. E pela redução de custo na aquisição de componentes de TI, já que grandes provedores possuem um maior poder de compra, assim podem negociar melhores preços para adquirir equipamentos [9].

A economia de escala no âmbito da demanda, ocorre devido a redução da variabilidade de carga, onde o uso dos recursos é aperfeiçoado pela virtualização, quando suas cargas variam pelo tempo. Os recursos computacionais podem ser melhores aproveitados, considerando que o pico de utilização dos serviços na nuvem varia entre os países, por causa do fuso horário distinto [9].

Ainda no âmbito da demanda, o desperdício de recursos computacionais que foram estabelecidos aguardando um crescimento na demanda de utilização de um serviço é evitado [9].

A economia de escala no âmbito da arquitetura Multi-inquilino, nos casos dos aplicativos preparados para essa arquitetura o custo do aplicativo e o custo da utilização de servidores são amortizados por serem compartilhados por diversos usuários. Como o custo é compartilhado, os fornecedores de infraestrutura, plataforma e serviços em nuvem podem investir no desenvolvimento e gerenciamento de soluções de alto nível, mais econômicas, eficazes, eficientes, seguras e resilientes [9].

Altamente escalável

O conceito “pague pelo uso” adotado pela Computação em Nuvem a torna facilmente dimensionável. O consumidor pode solicitar uma expansão dos serviços em grandes escalas ou em alguns casos realizar a subtração dos recursos de pronto, podendo ser realizado até mesmo sem que o provedor intervenha [12].

Os usuários dos serviços da nuvem determinam as suas necessidades específicas e optam por utilizar infraestruturas, plataformas ou serviços. Se desejar poderá apenas complementar suas capacidades de sistema de informação existentes através de infraestruturas que atenderão as atividades específicas [11].

Imediatismo

A disponibilização imediata dos recursos, é citada como um benefício da Computação em Nuvem, pois permite o fornecimento e utilização de um serviço, em tempo real. Enquanto o método tradicional, pode levar um tempo muito superior, necessitando de semanas ou até meses para que os recursos se tornem utilizáveis [13].

O imediatismo na liberação de recursos favorece a implantação de novas aplicações e no aumento da capacidade daquelas que já existem, fornecendo maior agilidade nos negócios e reduzindo os custos relacionados aos atrasos.

Disponibilidade

Provedores de serviços em nuvem devem oferecer uma solução bem gerenciada e implantada, com infraestrutura e largura de banda suficientes para suportar os requisitos dos consumidores, independentemente de onde estejam localizados. Geralmente os provedores possuem caminhos redundantes, realizando o balanceamento de carga para a garantia de que os serviços não serão sobrecarregados e sofrerem atrasos [11].

Uma arquitetura em nuvem implementada pelos fornecedores, com dispersão geográfica, que possua os dados e aplicativos duplicados em outros servidores localizados em diversos lugares e com a capacidade de transferi-los imediatamente, podem gerar uma solução resistente a interrupções e falhas nos seus serviços [11].

Fácil Acesso

Como grande parte dos serviços alocados na nuvem, serviços são *web-based*, se tornam facilmente acessíveis, a qualquer momento e lugar, através de uma variedade de dispositivos com conexão à internet [3].

Eficiência

A Computação em Nuvem oferece às empresas uma oportunidade única, pois com a realocação de atividades operacionais para a nuvem, permite que seus esforços sejam dedicados para inovação, pesquisa e desenvolvimento. O que possibilita um melhor aproveitamento da equipe, a redução do tempo para execução e um aumento da produtividade. Gerando assim um crescimento comercial, que poderá ser melhor do que as vantagens financeiras adquiridas com a implantação do sistema de nuvem [13].

Resiliência

Com a infraestrutura terceirizada para as nuvens, o fornecedor do serviço assume a responsabilidade de alguns riscos de negócios, tais como falhas de *hardware* [3]. Em um cenário de desastre, podem ser utilizadas soluções de espelhamento, bem como no balanceamento de carga de tráfego. Os provedores de nuvem, garantem ter resiliência e capacidade para manter a sustentabilidade, caso ocorra situações inesperadas, como um desastre natural [13].

A Tabela 1 apresenta uma síntese dos benefícios que foram detalhados.

Tabela 1: Síntese dos Benefícios da Computação em Nuvem

BENEFÍCIOS	**DESCRIÇÃO**
Economia	Diminuição de gastos através do pagamento do que apenas é utilizado.
Altamente escalável	Expansão ou subtração dos recursos conforme a necessidade de consumo.
Imediatismo	Liberação de recursos em tempo real.
Disponibilidade	Serviço estará sempre disponível para o acesso.

Fácil acesso	Acessível em diversos lugares e por vários dispositivos conectados à internet.
Eficiência	Oportunidade de não gastar esforços com atividades operacionais e sim em inovação, pesquisas e desenvolvimento.
Resiliência	Provedor assume a responsabilidade de garantir a segurança do negócio sob alguns riscos, tais como falhas de *hardware* e desastres naturais.

3.2 RISCOS

Risco representa para COSO's [14] "a possibilidade de que um evento irá ocorrer e afetar negativamente a realização dos objetivos". Essa ameaça ao negócio pode ser um evento imprevisto, falha ou mau uso da TI. A adoção da Nuvem, embora possua muitos benefícios, não há como separar os riscos que acompanham a solução [9].

Segundo Chaves [12], os riscos da Computação em Nuvem podem ser classificados em três grupos. O grupo de riscos operacionais, que se refere aos riscos que podem atingir a rotina do fornecimento de serviços. O grupo de riscos de negócio, que está relacionado ao posicionamento empresarial do provedor, diante de circunstâncias críticas. E o grupo de riscos estruturais, que engloba os riscos suscetíveis a comprometer o fornecimento dos serviços a longo e médio prazo, em virtude de decisões que foram tomadas sem concordância e/ou respeito à legislação ou a um senso comum.

Os riscos que foram considerados pelo autor, em sua tese de mestrado cujo título é "A questão dos riscos em ambientes de Computação em Nuvem", podem ser observados na Tabela 2:

Tabela 2: Riscos apresentados por Chaves em 2011 [12]

RISCOS OPERACIONAIS	
Falta de Privacidade	Uma deficiência no isolamento do ambiente, pode ocasionar acessos não autorizados às informações de clientes.
Falhas de Integridade	Uma autorização indevida de um agente mal-intencionado pode afetar a integridade dos dados e *softwares*.
Erros	A ocorrência de falhas no serviço prestado pode acarretar na necessidade de um novo processamento das rotinas, como também a recuperação dos dados afetados.
Suporte inadequado	Problemas podem ser ocasionados pela falta de preparo da equipe de suporte do provedor.
Baixo desempenho	Serviços contratados que não apresentam desempenho satisfatório, por motivos de picos no uso da nuvem, balanceamento incorreto dos recursos, entre outros fatores.
Ataques por saturação	O atraso para detectar ataques, pode ocasionar uma saturação dos servidores, por conta das inúmeras tentativas de interpretação das solicitações que possuem a intenção de prejudicar o ambiente.
Dificuldade para escalar	Dificuldades no provisionamento ou liberação de recursos, ou atrasos prolongados para a realização do mesmo.
Baixa Interoperabilidade	Comunicação de dados ou aplicações entre provedores diferentes dificultada ou impossibilitada.
RISCOS DE NEGÓCIO	
Indisponibilidade	Prestação de serviços interrompida temporariamente, por diversos motivos da parte do provedor.
Não-continuidade	A prestação de serviços é interrompida definitivamente.
RISCOS ESTRUTURAIS	

Não-conformidade	Descumprimento da legislação ou padrões estabelecidos.
Licenciamento de *software*	Contratos para o licenciamento de *softwares* realizados de forma inadequada, ocasionado limitações quanto ao uso de *softwares*.
Aprisionamento	Provedores possuem particularidades em seus ambientes, o que pode causar dificuldade ou até mesmo a impossibilidade de substituição de provedor.

O avanço da Computação em Nuvem criou novos desafios na área de segurança, amplificando vulnerabilidades que já existiam em ambientes convencionais e acrescentando novas questões de segurança provindas de características específicas da nuvem.

O CSA [15], publicou um relatório chamado "*The Treacherous 12 – Cloud Computing Top Threats in 2016*", elaborado a partir de uma pesquisa sobre os principais problemas de segurança, realizada com 271 especialistas. As 12 principais ameaças à segurança de uma implementação em nuvem apresentadas no relatório, classificadas em ordem de severidade, são:

- **1ª ameaça - Violação de dados:** Ocorre quando informações de qualquer espécie, que não foram destinadas à divulgação pública são acessadas, roubadas ou utilizadas por uma pessoa que não possui autorização para realizar estas ações.

  A violação pode ser fruto de um ataque cujo objetivo era o acesso dos dados, vulnerabilidades de aplicativos, práticas insuficientes de segurança ou até mesmo falhas humanas.

  O ambiente em nuvem além de estar sujeito às mesmas ameaças que um ambiente convencional, acrescenta novos meios de ataque como através dos recursos compartilhados, funcionários dos provedores e parceiros terceirizados. A acessibilidade e a hospedagem de um número elevado de informações dos ambientes em nuvem, o tornam um alvo em potencial [15].

- **2ª ameaça - Identidade fraca, gerenciamento de credenciais e acesso**: A ausência de um gerenciamento de acesso de identidades, falhas na utilização de autenticação multifatorial, a não utilização de senhas fortes e a inexistência de substituição automáticas das chaves criptográficas, senhas e certificados podem permitir o acesso não autorizado a dados, gerando danos que podem ser grandiosos para a organização ou usuário final [15].

- **3ª ameaça - Interfaces e APIs inseguras:** As interfaces de usuário (UIs) e as interfaces de programação de aplicativos (APIs) são a parte com maior exposição, pois é por intermédio delas que os clientes podem gerenciar e interagir com os serviços em nuvem. APIs e UIs são alvos de ataques devido a sua exposição fora do limite organizacional confiável, caso não possuam controles adequados para a proteção podem colocar em risco várias questões de segurança relacionadas à confidencialidade, integridade, disponibilidade e responsabilidade [15].

- **4ª ameaça - Vulnerabilidades do Sistema:** Vulnerabilidades em um sistema são as falhas que podem ser exploradas por um invasor a fim de roubar dados, controlar o sistema ou interromper os serviços.
  A utilização do *Multi-tenancy* na Computação em Nuvem permite que recursos sejam compartilhados entre várias organizações, que terão seus sistemas colocados próximos um dos outros. Essa condição gera uma nova plataforma para ataques às vulnerabilidades que podem ser apresentadas.
  As vulnerabilidades em sistemas de informação sem correção podem gerar grandes prejuízos para uma organização [15].

- **5ª ameaça - Sequestro de contas:** Contas dos usuários podem ser capturadas por vários métodos de ataque, como por exemplo o *phishing*. As consequências são amplificadas quando as credenciais são inúmeras vezes reutilizadas. Um atacante com a posse de credencias de um serviço na nuvem, po-

derão acessar suas áreas críticas, espionando as atividades executadas, acessar os dados, redirecionar clientes para sites falsos, entre outras ações indesejáveis [15].

- **6ª ameaça - Ataques internos maliciosos:** Uma ameaça interna trata-se de um funcionário atual, ex-funcionário, fornecedores ou parceiros de negócios, que usufruem do acesso autorizado à rede para prejudicar a organização ou beneficiar-se financeiramente através de práticas desonestas.
  Ameaças internas também podem ser de caráter não intencional, como no caso de um empregado acidentalmente colocar em risco informações confidenciais de uma organização [15].

- **7ª ameaça - Avançadas ameaças persistentes:** Conhecidas como APTs, sigla originada do termo em inglês *"Advanced Persistent Threats"*, são ameaças que se infiltram em um sistema para atingir seus objetivos furtivamente por longos períodos, até mesmo se adaptando às regras de segurança que deveriam impedi-los.
  Algumas formas para APTs acessarem o sistema são: *Spearphishing*, códigos fornecidos de dispositivos USB, infiltração por intermédio da rede de parceiros e uso de rede insegura [15].

- **8ª ameaça - Perda de dados:** A perda permanente dos dados pode ser ocasionada não somente por ataques, mas também por exclusão acidental do provedor ou uma catástrofe física. A perda também pode ser ocasionada pelo cliente, caso ele envie dados criptografados para a nuvem e perca a chave.
  Para uma empresa, a informação é o ativo mais valioso, a perda dela poderá trazer grandes consequências, até mesmo a extinção do negócio [15].

- **9ª ameaça - Diligência insuficiente:** Uma avaliação sem diligência das tecnologias em nuvem e dos provedores de serviço, para o qual se deseja migrar, poderá acarretar em riscos comerciais, financeiros, técnicos, legais e de conformidade que poderão comprometer o sucesso da empresa [15].

- **10ª ameaça - Abuso e uso indevido de serviços em nuvem:** Uma pessoa mal-intencionada poderá utilizar os serviços da nuvem, com o intuito de atingir os usuários, organizações ou até mesmo outros provedores de nuvem. Alguns exemplos de uso indevido dos recursos em nuvem são os ataques DDoS, spam em e-mail, fraude automatizada em grande escala, ataques de força bruta a banco de dados de credenciais e armazenamento de conteúdo ilegal [15].

- **11ª ameaça - Negação de serviço:** Os ataques de negação de serviço (DoS), tem como objetivo impossibilitar o acesso dos usuários aos seus serviços. Através de requisições que fazem o serviço consumir exageradamente os seus recursos, tais como processamento, memória e largura de banda. Tornando o serviço inacessível por causa de uma lentidão intolerável [15].

- **12ª ameaça - Vulnerabilidades de tecnologias compartilhadas:** A Computação em Nuvem tem como característica, o compartilhamento de infraestrutura entre vários clientes. Os componentes compartilhados podem não ter sido projetados para realizar isolamentos fortes para uma arquitetura compartilhada. O que pode gerar vulnerabilidades técnicas compartilhadas, que ao serem exploradas poderão comprometer uma nuvem por completo [15].

A Tabela 3 apresenta uma síntese das 12 ameaças citadas pela CSA (2016)

Tabela 3: Síntese das ameaças apresentadas por CSA em 2016 [15]

COLOCAÇÃO	AMEAÇAS	DESCRIÇÃO
1ª	Violação de dados	Acesso, roubo ou utilização de informações, por pessoas não autorizadas.
2ª	Identidade fraca, gerenciamento de credenciais e acesso	Ausência ou falhas de um forte gerenciamento de identidades e acesso.

3ª	Interfaces e APIs inseguras	APIs ou UIs sem um controle de proteção adequado.
4ª	Vulnerabilidades do Sistema	Falhas suscetíveis a exploração por um invasor.
5ª	Sequestro de contas	Roubo de contas através de ataques, para realizar acessos ao sistema.
6ª	Ataques internos maliciosos	Acesso mal-intencionado de uma pessoa interna à organização.
7ª	Avançadas ameaças persistentes	Infiltrações em um sistema que persistem por longos prazos.
8ª	Perda de dados	Perda de informações ocasionadas por diversos fatores, sejam eles, intencionais, acidentais ou por fenômenos físicos.
9ª	Diligência insuficiente	Falta de cuidado na avaliação de tecnologias e provedores, antes da migração.
10ª	Abuso e uso indevido de serviços em nuvem	Utilização dos serviços da nuvem para atos indevidos, tais como atingir outros usuários.
11ª	Negação de serviço	Ataques por saturação com intuito de indisponibilizar o serviço da nuvem.
12ª	Vulnerabilidades de tecnologias compartilhadas	Vulnerabilidades geradas pelo uso dos recursos compartilhados por vários usuários.

4 SEGURANÇA EM COMPUTAÇÃO EM NUVEM

A Computação em Nuvem se tornou atraente desde o momento da sua criação, pelo seu grande potencial em proporcionar enormes benefícios às empresas, como a redução de custos, escalabilidade, acesso independente de localização, compartilhamento de recursos, facilidade de uso, provisionamento de recursos sob demanda, entre outros. Apesar de suas vantagens, como descrito em maiores detalhes no Capítulo 3, essa tecnologia não é isenta dos riscos, sendo o maior deles a segurança [16]. Os potenciais benefícios podem ser eliminados, caso existam falhas ao garantir a segurança adequada para utilização dos serviços em nuvem, que poderão ocasionar custos elevados e perda potencial de negócios [17].

Um dos maiores fatores que impedem a adoção generalizada da Computação em Nuvem é a segurança, pois muitas empresas e organizações relutam em confiar plenamente em um provedor, a ponto de realizar a transferência dos seus ativos para a nuvem [16]. A confiança de um cliente em uma organização poderia ser definida como a certeza de que a organização será capaz de proporcionar serviços que atendam às necessidades com precisão e infalibilidade. Ao mesmo tempo reconhecendo um fator mínimo de risco, onde todos os possíveis riscos tendem a ser eliminados ou reduzidos ao mínimo absoluto [18].

A nuvem possui uma grande variedade de informações que pertencem a um ou mais clientes, essa característica pode torná-la alvo para ataques de potenciais invasores. Os ataques, podem comprometer toda a nuvem, afetando assim as exigências mínimas de segurança da informação (disponibilidade, confidencialidade e integridade) [19]. Além de ser um alvo para ataques externos, a presença de inúmeros usuários que não são da mesma organização compartilhando recursos, pode ser um fator de preocupação para um cliente, pois apesar de serem de confiança do provedor, os usuários podem não ser confiáveis entre si [16].

Os controles de segurança utilizáveis em ambientes de Computação em Nuvem, não são completamente diferentes dos controles adotados em outros ambientes de TI. Contudo, os riscos apresentados por esses ambientes, comparados aos riscos associados a ambientes tradicionais, podem ser distintos, pelo fato dos modelos de

serviço, dos modelos de implementação e as tecnologias empregadas para habilitação dos serviços, não serem iguais. Ainda, de acordo com o modelo de serviço escolhido, esses controles de segurança podem não estar a cargo do cliente e sim serem transferidos para o provedor [8].

4.1 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO EM COMPUTAÇÃO EM NUVEM

Essencialmente a segurança da informação, visa a identificação dos riscos e implementação de medidas apropriadas para proteção da informação de possíveis ameaças a sua integridade, disponibilidade e confidencialidade, de forma a garantir a continuidade do negócio e minimizar os riscos [20].

Os pilares da segurança da informação, que são: confidencialidade, integridade e disponibilidade. São aspectos importantes para a concepção de sistemas seguros. A infraestrutura da Computação em Nuvem possui características únicas, apresentando desafios a segurança que apesar de peculiares podem ser classificados de acordo com os pilares da segurança da informação [18].

4.1.1 CONFIDENCIALIDADE

Segundo Sêmola [21], conforme citado por Jesus [22], a confidencialidade é o princípio que restringe o acesso a informação tão somente àquelas entidades que possuem autorização do proprietário da informação. O conceito de confidencialidade é considerado nos casos em que um sistema, ou ativo de informação, requer proteção e não permite que suas informações sejam divulgadas sem consentimento.

A Computação em Nuvem possui como característica o compartilhamento dos recursos, onde os usuários são separados em um nível virtual, mas utilizam o mesmo *hardware*. A utilização da arquitetura Multi-inquilino, pode representar uma ameaça a

privacidade e confidencialidade. Ainda mais quando se trata de reutilização de objetos, pois necessitarão que sejam cuidadosamente controlados para que não gerem uma grave vulnerabilidade [18].

A violação da confidencialidade pode ser realizada involuntariamente ou maliciosamente, por exemplo, no caso de remanência dos dados em objetos que foram reutilizados. A remanência dos dados, são os resíduos de dados que foram apagados ou removidos, que podem levar à divulgação de dados privados [18].

A confidencialidade da nuvem também pode ser afetada por uma falha no processo de autenticação, que pode levar a um acesso não autorizado aos perfis de usuários em uma nuvem, comprometendo a privacidade. O acesso não autorizado pode ser ocasionado por uma vulnerabilidade da aplicação ou falta de uma identificação forte. É responsabilidade do provedor de serviços de nuvem prover instâncias de nuvem seguras [18].

4.1.2 INTEGRIDADE

Segundo Sêmola [21], conforme citado por Jesus [22], a integridade é o princípio que assegura que os dados conservem todas as suas características originais definidas pelo dono da informação, como também o controle de alterações e preservação do seu ciclo de vida (criação, alteração e descarte). O conceito de integridade é considerado quando um sistema, ou ativo de informação, possui informações que necessitam de proteção contra modificações não consentidas, ou mesmo modificações realizadas sem intenção, incluindo mecanismos que possibilitam a identificação de tais tipos de alterações.

A Computação em Nuvem, geralmente possui muitos pontos de acesso, logo um mecanismo para determinar os usuários que poderão realizar alterações e em quais informações é crucial para garantir que somente pessoas autorizadas irão interagir com os dados. Dessa forma é possível ter maior confiança na integridade dos dados e do sistema [18].

4.1.3 DISPONIBILIDADE

Segundo Sêmola [21], conforme citado por Jesus [22], a disponibilidade é o princípio que assegura que a informação estará disponível a todo momento para ser utilizada, pelos usuários que possuem acesso autorizado pelo dono daquela informação. O conceito de disponibilidade é considerado quando um sistema, ou ativo de informação necessita estar sempre acessível para atender os seus objetivos.

A disponibilidade consiste em uma habilidade dos sistemas permanecerem em operação, mesmo que alguma autoridade se comporte mal ou que exista alguma possibilidade de violação de segurança. Para os serviços de Computação em Nuvem a dependência da disponibilidade dos recursos de rede é continua [18].

4.2 GESTÃO DA SEGURANÇA EM NUVEM

A perda de controle de sistemas, aplicações, segurança de dados e outros recursos é o principal desafio para as organizações. Visto que, controles de segurança tradicionais não se aplicam da mesma forma a ambientes em nuvem, inclusive muitos não podem ser controlados pelas organizações.

Uma gerência de segurança em nuvem eficaz, leva em consideração áreas importantes, como governança da nuvem, políticas de segurança, gestão de riscos, contratos de nível de serviço (SLAs), aspectos legais e auditoria, que devem ter a devida atenção das organizações que desejam migrar seus serviços para nuvem.

4.2.1 GOVERNANÇA

A governança de um ambiente requer da organização o controle e supervisão das políticas, procedimentos e padrões para o desenvolvimento de aplicações e aquisição de serviços de TI. Compreende também na concepção, implementação, testes, uso e monitoramento dos serviços [23].

O ambiente em nuvem possui características, como a virtualização, agilidade, flexibilidade que poderão exigir questões de governança diferenciadas para garantir que os benefícios sejam alcançados com um nível de risco tolerável [24].

Quando processos de governança não são colocados em prática, questões importantes como, procedimentos de privacidade, segurança e fiscalização podem ser ignoradas, dessa forma uma organização poderá estar sujeita a uma exposição maior a riscos desconhecidos. Além disso, a falta de um monitoramento consistente poderá gerar custos desnecessários em serviços que não são mais utilizados [24].

Diferentemente de um ambiente tradicional, os serviços em nuvem compartilham papéis e responsabilidades entre a organização e o provedor, relacionados ao gerenciamento de riscos e efetivação de requisitos da organização [23].

Segundo Liu [25], existem muitos modelos de governança para nuvem, mas todos possuem um princípio básico, que é a aplicação de políticas sólidas e aderência de processos maduros ao adotar serviços e tecnologias em nuvem. O autor cita os seguintes componentes como importantes para uma estrutura eficaz de governança:

Educação da força de trabalho: Os usuários devem ser orientados quanto as medidas de segurança, para evitar violações por motivos de atitudes erradas dos usuários. A maneira mais eficaz para o controle dessa questão, é realizando o gerenciamento de identidade e acesso juntamente com uma solução que permita que todas as alterações sejam registradas e auditadas corretamente.

Gestão de risco: Processos devem ser estabelecidos a fim de detectar, gerenciar e mitigar os riscos, respondendo rapidamente a eventos esperados ou não.

Auditoria: Importante ser realizada de forma robusta para avaliar a conformidade, a qualidade e os padrões.

4.2.2 POLÍTICAS DE SEGURANÇA

Uma política de segurança em nuvem é um documento que específica o planejamento de proteção dos recursos de informação de uma determinada organização. Esse documento é continuamente atualizado conforme as mudanças de tecnologia e requisitos de negócio [25].

A política de segurança deve ser sólida, pois ela é a base para todas as atividades de segurança. É a parte crucial antes da adoção de uma nuvem, a fim de garantir o aproveitamento dos benefícios que ela oferece de forma segura. Ela deve abranger todos os aspectos relevantes para a segurança da informação, inclusive pessoal, instalações, *hardware* e *softwares* [26].

O escopo de uma política irá variar de acordo com o modelo de implantação e o modelo de serviço. A Judith M. Myerson [27] em sua publicação para a IBM, cujo o título é “Criar uma política de segurança de serviços em nuvem”, explica que a elaboração de uma política de segurança, possui diferenças no escopo conforme o modelo de serviço implementado.

A política de segurança SaaS possui o foco no gerenciamento de acesso às aplicações específicas alocadas para os consumidores, com a finalidade de redução do risco de roubo de identidade ou *spoofing.* Já a política de segurança PaaS além de gerenciar o acesso, se preocupa em proteger os dados. E a política de segurança IaaS além do gerenciamento de acesso de usuários à infraestrutura e proteção de dados, ela se concentra no gerenciamento das máquinas virtuais [27].

4.2.3 GESTÃO DE RISCOS

Gestão de riscos é o procedimento para identificar e avaliar os riscos para a organização, seus ativos e indivíduos. A partir disso, tomar as medidas necessárias para reduzi-los a um nível aceitável. O processo consiste na avaliação dos riscos, na

implementação de uma estratégia para a mitigação dos riscos e aplicação de procedimentos para o monitoramento ininterrupto da situação da segurança da informação [23].

4.2.3.1 MODELO DE GESTÃO DE RISCO

A CSA [28] desenvolveu um esquema básico de gestão de riscos para ser aplicado por aqueles que desejam adotar serviços na nuvem, com o intuito de auxiliar a avaliação inicial dos riscos e permitir a seleção das opções de segurança. O esquema está dividido em cinco etapas:

1ª Etapa - Identificar o Ativo para implantação na Nuvem

A migração dos ativos, que podem ser dados ou aplicações/funções/processamento para a nuvem pode ser realizada integralmente ou apenas partes das funções. A identificação exata dos dados ou funcionalidades que serão migrados e sua utilização, é a primeira etapa para avaliação dos riscos.

2ª Etapa - Avaliar o Ativo

Os ativos devem ser avaliados quanto ao seu grau de importância e sensibilidade. De maneira que sejam observados como serão afetados os requisitos de confidencialidade, integridade e disponibilidade ao ser utilizados na nuvem.

3ª Etapa - Mapear o Ativo ao Modelo de Implantação em Potencial

Durante a realização da escolha do modelo de implantação e modo de hospedagem, deve ser avaliado os riscos que cada modelo possui implicitamente e se são aceitáveis de acordo com a importância do ativo.

4ª Etapa - Avaliar Potenciais Modelos de Serviços na Nuvem e Provedores

Para a implementação de um gerenciamento de riscos, é necessário avaliar o nível de controle que cada modelo de serviço possuíra.

5ª Etapa - Esboçar o Potencial Fluxo de Dados

É de grande importância compreender como os dados irão entrar e sair da nuvem, por isso é necessário o mapeamento do fluxo dos dados entre a organização, o serviço de nuvem e os pontos de acesso que estão envolvidos. Para que seja possível identificar quais pontos estão expostos aos riscos.

A aplicação do esquema desenvolvido pela CSA, possibilita a compreensão da importância dos ativos que estão dispostos a serem transferidos para nuvem, como também o seu nível de tolerância aos riscos e quais modelos de implantação e serviços se enquadram no objetivo da organização.

4.2.4 ACORDOS DE NÍVEL DE SERVIÇO

Os acordos de nível de serviço, normalmente conhecidos como SLA por ser uma abreviação do termo em inglês *Service Level Agreement*, é um acordo entre o usuário e o provedor de serviços, utilizado para definir claramente as expectativas do serviço contratado, é um meio do provedor garantir a confiança do cliente.

O SLA, é um documento importante tanto para o provedor quanto para o cliente, pois ele deve abranger diversas questões, como o desempenho dos serviços prestados, gerenciamento de questões de conformidade legal, gestão de riscos, responsabilidades com a segurança, resolução de responsabilidades do cliente, recuperação de desastres e continuidade de negócios [29].

Os acordos de nível de serviço evoluíram quanto a área de segurança, antes esses acordos eram focados em aspectos relacionados a qualidade dos serviços oferecidos, agora também abordam questões especificas para a garantia da segurança, como a evidência da integridade dos dados armazenados e mecanismos de segurança utilizados, como por exemplo a criptografia [30].

Antes de uma avaliação de um SLA, é importante que o cliente desenvolva uma análise do seu negócio, isso inclui a identificação dos serviços específicos que serão

transferidos para nuvem e a compreensão de suas importâncias [25]. E com isso, serem claros quanto aos requisitos de segurança para os seus ativos e cuidadosamente acordá-los no SLA [16].

4.2.5 ASPECTOS LEGAIS

Uma organização, independentemente do modelo de computação utilizado, é responsável por operar de acordo com as leis, regulamentos, padrões e especificações estabelecidos, principalmente em torno dos dados que podem ser coletados, armazenados e processados. De forma a garantir que se encontra em conformidade legal [26].

Um fator importante na Computação em Nuvem que deve ser considerado é a localização geográfica do servidor onde ficarão armazenados os dados. Apesar da contratação ter sido realizada em um determinado país, o serviço poderá estar alocado em outro território, que possuirá uma legislação especifica para a proteção de dados [31]. Por esse motivo é essencial que um usuário tome conhecimento da localização das informações. Um problema relacionado a essa questão, por exemplo, no caso de apreensão do equipamento para investigações relacionadas a um determinado usuário, dependendo das leis locais de onde os dados se encontram, pode resultar em um risco de violação de privacidade de todos os outros usuários que possuíam informações alocadas [16].

4.2.6 AUDITORIA

Auditoria em ambientes de nuvem, trata da avaliação de políticas de segurança, procedimentos, práticas e controles técnicos para correção e completude. Isso é crucial para avaliar se os controles e procedimentos atendem a todos os aspectos operacionais de segurança, como também a conformidade, proteção e detecção [26].

O modelo de implantação na nuvem (público, privado, híbrido e comunitário) e modelo de serviço (SaaS, IaaS e PaaS) irá impactar no tipo de auditoria a ser realizada. Sendo os modelos públicos e híbridos os que possuem maior diferencial, pelo fato de dependerem mais fortemente de contratos e acordos [32].

Quando sistemas são movidos de ambientes convencionais para um ambiente em nuvem, algumas mudanças relacionadas ao escopo da auditoria devem ser realizadas. Halpert [32] apresenta seis tipos de situações que os auditores devem estar atentos quando um sistema migra para nuvem, três delas são:

Situação 1 - Os sistemas que são desenvolvidos para operar internamente e contam com a segurança fornecida pela rede, se forem movidos para nuvem sem que sejam adaptados corretamente estarão sujeitos a vários riscos de segurança, por não estarem preparados para impedir os ataques provindos do ambiente público.

Situação 2 – Os provedores podem manter seus servidores testados e corrigidos de uma forma genérica, dando margem para falhas ou riscos atingirem sistemas customizados. Sendo assim, é necessária uma interação maior entre o provedor e cliente, para evitar riscos adicionais.

Situação 3 – Os ambientes de nuvem, independente do modelo de implantação, modificam o principal escopo da auditoria do limite da rede. As comunicações entre provedor e cliente devem ser inspecionadas cautelosamente, o que requer um monitoramento aprimorado dos controles de rede.

A auditoria em uma infraestrutura na nuvem se assemelha com a auditoria de ambientes convencionais, mas será necessário dar mais atenção em aspectos de controle de acesso e autorização. Alguns novos problemas como, latência de comunicação, notificação de violação de dados e leis da localização dos dados armazenados, deverão ser levados em consideração [32].

A responsabilidade pela auditoria é principalmente do provedor de nuvem em ambientes com o modelo de serviço SaaS, mas essa responsabilidade é partilhada entre o provedor e o cliente nos ambientes IaaS e PaaS. Geralmente, as informações serão fornecidas pelo provedor para efetuação da auditoria de segurança [33].

4.3 SEGURANÇA DE REDE NA NUVEM

A segurança de rede examina os riscos que são apresentados pelo uso e acesso de redes de uma organização, realizando a proteção dos dados e sistemas, de ataques baseados em rede, mantendo também a segurança dos próprios componentes de rede [34].

O provedor de serviços em nuvem é responsável por efetuar a distinção de um tráfego de rede legítimo de um tráfego de rede mal-intencionado, realizando o bloqueio da tentativa maliciosa. Sendo assim, um ponto crucial para a segurança é o controle de acesso à rede.

Para efetuar o controle de acesso à rede é necessário o uso de mecanismos que podem ser implementados em dispositivos físicos, convergentes ou virtuais, como:

- **Controles do *Firewall* Perimetral:** Inspecionam o protocolo em tempo real e realizam a detecção dos ataques que são conhecidos. A implementação deve ser colocada dentro do perímetro de segurança do *firewall* para que seja possível o bloqueio dos ataques [34].

- **Controles de *Firewall Sub-Tier:*** O controle é baseado nas camadas de virtualização da nuvem, onde cada uma possui um limite de segurança. As políticas restringem o tráfego de rede de camada para camada, para a proteção das máquinas virtuais e das camadas de rede geradas na nuvem [34].

- **Listas de Controle de Acesso:** As listas de Controle de Acesso, conhecidas como ACLs por causa do termo em inglês *Access Control List*, fornece a capacidade para negar ou permitir um determinado tráfego de rede, promovendo uma camada de controle de segurança para proteção de máquinas virtuais contra ameaças de segurança padrão da camada 2 [34].

Uma análise mais profunda do tráfego da rede pode indicar que um tráfego está mal-intencionado e portando conteúdo malicioso, embora incialmente o firewall tenha o considerado legítimo, pois o firewall realiza uma verificação baseada em portas e conexões. Tornando assim necessário a implementação de tecnologias de controle de inspeção do conteúdo, como servidores IDS/IPS, DLP e Proxy [17].

Os serviços disponibilizados na nuvem possuem forte dependência de API e portais para gerenciamento, sendo um ponto de exposição a ambientes públicos que podem ser alvo de ataques, como o ataque DDoS (Ataque distribuído por negação de serviço).

Ataque DDoS é realizado com a finalidade de esgotar os recursos de rede ou os recursos de servidores que hospedam o aplicativo, através do envio de requisições maliciosas de inúmeros hosts comprometidos. Resultando na negação do serviço para requisições legítimas de usuários [34].

A CSA [34] realizou recomendações para mitigar os ataques DDoS, entre elas foram citadas, a implementação da mitigação de DDoS baseada em volume com largura de banda superior ao volume do ataque e realização de uma filtragem que exija perfil completo do tráfego legítimo.

Os controles de segurança de rede poderão contribuir para investigações forenses, sendo assim é importante que a conservação de informações de auditorias e registros de logs sejam protegidos por controles de segurança, para que não sejam acessados, modificados ou destruídos sem autorização. Visto que, são importantes também para medidas preventivas de segurança e para resposta a incidentes [17].

4.4 SEGURANÇA DE DADOS NA NUVEM

Os dados são a parte central das preocupações de segurança da informação, independente da organização e infraestrutura utilizada. A Computação em Nuvem possui um quesito a mais, pela característica da sua infraestrutura compartilhada. As incumbências com a segurança devem ser aplicadas aos dados em repouso, aos dados em movimento e aos dados em processo [17].

Dados em repouso, são aqueles que se encontram em um sistema de armazenamento. Os dados em movimento, são aqueles que através de uma ligação de comunicação estão sendo transferidos. Já os dados em processo, são aqueles que por exemplo, estão alocados na memória e sendo utilizados por um aplicativo [17].

A proteção da transferência dos dados pode ser realizada através de padrões de protocolos de comunicação e certificados de chaves públicas [23]. Padrões como HTTPS (para conexões regulares de clientes e serviços em nuvem, através da Internet), SFTP (para transferências de dados em massa), VPN usando IPSec e SSL (preferível para conexões de funcionários do cliente para o serviço em nuvem) e TLS (*Transport Layer Sercurity* – para conexões seguras e privadas entre duas aplicações conectadas), todos sobre criptografia da camada de transporte de dados [17].

Para a proteção dos dados em repouso, Samarati e Vimercati [30], afirmam que os provedores podem aplicar medidas de segurança para os serviços, mas essas medidas lhes permitem total acesso aos dados, então para a proteção da confidencialidade dos dados é importante a realização da criptografia dos dados antes de transferi-los e armazená-los na nuvem.

Apesar da criptografia ser eficaz em diversos ambientes, ela pode dificultar alguns cenários de recuperação de dados. Dessa forma, abordagens recentes apresentam a ideia da utilização de fragmentação, no lugar da criptografia. Nesse modelo, o dado é dividido em fragmentos e armazenados separadamente, sendo necessário o sigilo das associações dos seus valores. A fragmentação poderá ser utilizada em conjunto com a criptografia, sendo aplicadas a dados sensíveis que não podem ser armazenados em claro [30].

Controles de acesso são um meio de proteção dos dados contra usuários não autorizados, eles são normalmente baseados em identidade, o que torna a autenticação da identidade do usuário uma questão importante na Computação em Nuvem [23].

Os princípios de segurança de confidencialidade, integridade e disponibilidade devem ser aplicados para a segurança dos dados em ambientes de nuvem, através de procedimentos que garantam a sua proteção.

É de grande importância a realização do backup regular dos dados, gerenciada pelo provedor do serviço para a garantia da disponibilidade e da recuperação dos

dados em casos de desastres, que podem ser acidentais ou intencionais. O armazenamento do backup deve estar protegido, para que não seja adulterado ou acessado por pessoas não autorizadas [16].

O descarte dos dados deve ser realizado com muita cautela, pois o mesmo possui implicações para a segurança. A limpeza dos dados do local de armazenamento, pode ser feita por vários meios, como por desmagnetização ou até mesmo a destruição da mídia, mas devem ser efetuadas de maneira que não permita a recuperação das informações que ali eram contidas. O descarte também é aplicado as cópias de backup que foram realizadas para recuperação e restauração dos serviços e dados. O ambiente na nuvem pode apresentar dificuldades pela sua natureza de compartilhamento, como por exemplo, em dados do modelo SaaS. Por isso, é importante que as medidas para garantia de que o descarte dos dados será realizado de forma adequada ao longo do ciclo de vida do dispositivo, sejam definidas no acordo de prestação de serviço [23].

4.5 SEGURANÇA DE APLICAÇÕES NA NUVEM

A segurança das aplicações contra ameaças externas e internas deve percorrer todo o ciclo de vida, desde o projeto até a implementação. Através de políticas e processos de segurança bem definidos e aplicados [17].

Aplicações localizadas na nuvem possuem as mesmas vulnerabilidades que as aplicações tradicionais, mas as soluções de segurança que são empregadas em ambientes tradicionais não são adequadas para ambientes em nuvem, pois a consequência de uma vulnerabilidade poderá ser muito superior do que em ambientes tradicionais [16].

A *Open Web Application Security Project* em 2013 relacionou os dez principais riscos nas aplicações web, são eles [35]:

- Injeção de código
- Quebra de autenticação e gerenciamento de sessão
- *Cross-Site scripting* (XSS)

- Referência insegura e direta a objetos
- Configuração incorreta de segurança
- Exposição de dados sensíveis
- Falta de função para controle do nível de acesso
- *Cross-Site Request Forgery* (CSRF)
- Utilização de componentes vulneráveis conhecidos
- Redirecionamentos e encaminhamentos inválidos

Os riscos relacionados pela OWASP devem ser levados em consideração durante o desenvolvimento, gerenciamento e o uso dos aplicativos, para garantir a segurança do mesmo.

Além dos riscos mencionados, a segurança e a disponibilidade dos sistemas, depende se as APIs ou interfaces que o provedor disponibiliza para os seus clientes executarem várias operações, são projetadas adequadamente e utilizadas corretamente pelos clientes [36]. As APIs geralmente são publicadas para os usuários conhecerem componentes e funções da nuvem, mas trata de uma exposição aos atacantes, que podem se aproveitar de vulnerabilidades como credenciais fracas e autorização e validação de entrada de dados insuficientes [16].

A proteção de aplicações na Computação em Nuvem deve ser levada em consideração os modelos de serviço, pois o modelo irá influenciar no responsável pelos controles de segurança.

As aplicações e a pilha de *softwares* em um ambiente IaaS, são de responsabilidade dos clientes, como também muitas das medidas necessárias para segurança. O cliente deve solicitar ao provedor, recursos disponíveis, como por exemplo “Segurança como serviço”, firewalls e autenticação de usuários, para complementar a segurança dos seus aplicativos [17].

Em um ambiente PaaS, o código da aplicação é de responsabilidade do cliente, mas a pilha de *softwares* está sob controle do provedor. É importante que o cliente tenha o conhecimento dos recursos de segurança que são fornecidos e quais ele deve implementar [17].

Para as aplicações em um ambiente SaaS, o provedor é o responsável pela segurança dos serviços e dos dados a ele associados. Uma documentação gerada

pelo provedor relacionando os recursos de segurança fornecidos e os recursos que o cliente deve aplicar, se faz necessária nesse ambiente [17].

Para a segurança dos aplicativos em nuvem é essencial o uso de mecanismos apropriados de autenticação e gerenciamento de identidades, para impedir o acesso não autorizado aos recursos [36]. A autenticação e o gerenciamento de identidades, refere-se à criação ou verificação de identidades e a validação com credenciais, preferencialmente realizadas não apenas na conexão inicial, mas baseada no risco das transações executadas na aplicação [25].

Uma questão importante a ser considerada é a realização de testes de vulnerabilidades de segurança em aplicações na nuvem. O teste de penetração deve ser um procedimento padrão para aquelas aplicações expostas publicamente [17], essa metodologia dá ao testador uma visão sobre a força da segurança do sistema.

5 CENÁRIO MUNDIAL E BRASILEIRO DA ADOÇÃO DE COMPUTAÇÃO EM NUVEM

A Computação em Nuvem está sendo uma das maiores revoluções dos últimos anos na área de Tecnologia da Informação. Conforme a nuvem oferece mais serviços e recursos, com segurança e eficiência, a sua adoção cresce e se acelera.

A adoção dessa tecnologia no Mundo, no Brasil e no Governo Brasileiro, como também as perspectivas futuras serão abordadas em mais detalhes a seguir.

5.1 ADOÇÃO DA NUVEM NO MUNDO

A nuvem é uma realidade hoje. Diversos dispositivos eletrônicos que são utilizados no dia-a-dia consomem a Computação em Nuvem de alguma forma. O que demonstra que a adoção desse modelo é sólida e crescente.

Empresas estão utilizando cada vez mais ambientes de nuvem híbridos e todos os principais modelos de serviço: *Software* como Serviço (SaaS), Plataforma como Serviço (PaaS) e Infraestrutura como Serviço (IaaS). Incluindo também, outros modelos baseados em nuvem, derivados dos modelos tradicionais, tais como Dados como Serviço (DaaS), Segurança como Serviço (SecaaS), Rede como Serviço (NaaS) e Identidade como Serviço (IDaaS) [37].

A RightScale [38] conduziu um levantamento sobre o estado da nuvem, em janeiro de 2016. Realizado com 1.060 pessoas, representantes de organizações de diversos portes, onde 83% delas não utilizam soluções RigthScale, o que permitiu uma perspectiva abrangente do estado da nuvem.

A pesquisa obteve várias conclusões importantes, uma delas é o crescimento significativo da adoção de nuvens híbridas, quando comparado com o relatório do ano de 2015. O motivo é o aumento da adoção do modelo privado por parte de empresas que já possuíam nuvem pública, de 63% para 77% o que levou a adoção de nuvens

híbridas crescerem de 58% para 71%. O crescimento do uso de cada um dos modelos de implantação pode ser observado na Figura 2 [38].

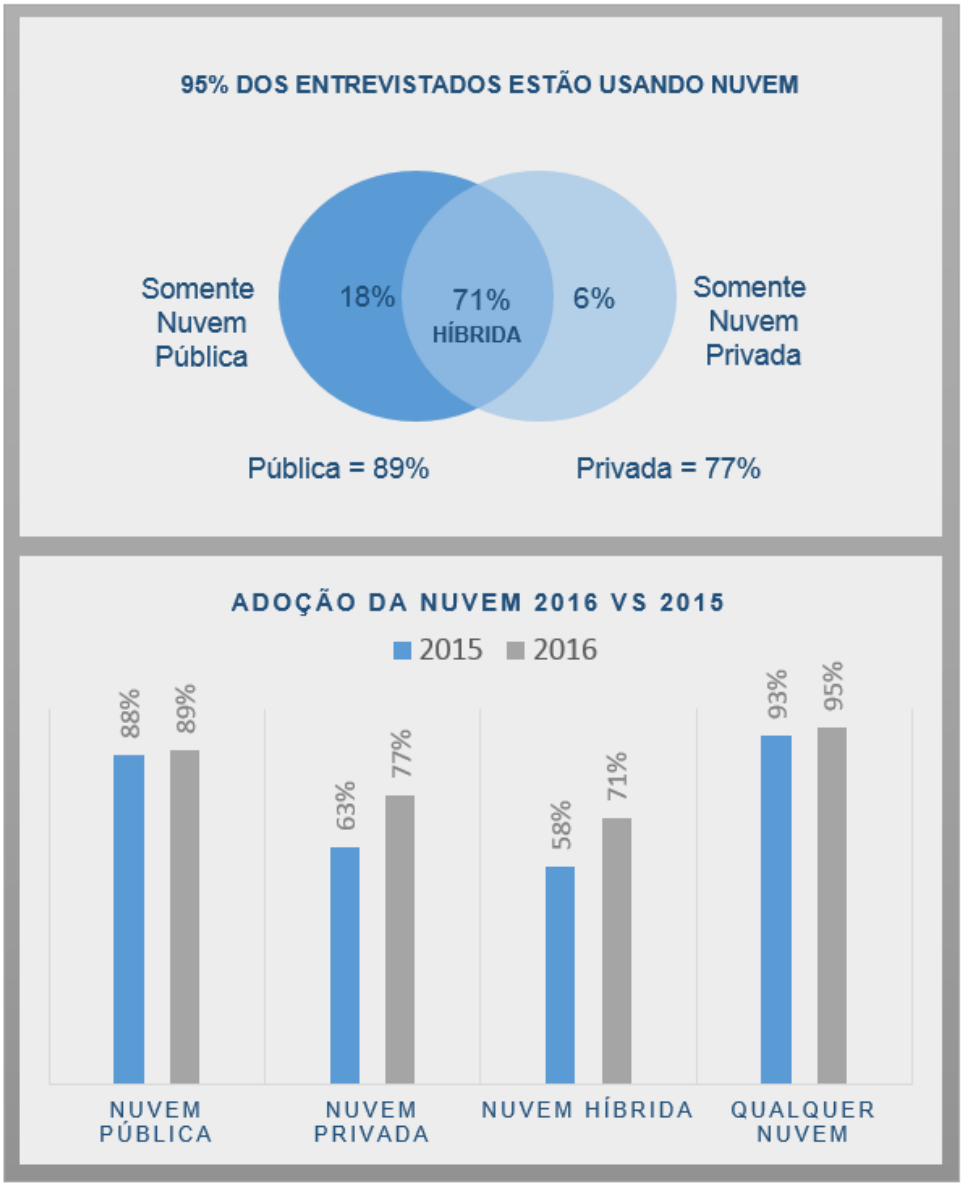

Figura 2: Crescimento do uso dos modelos de implantação [38]

Grandes empresas com mais de 1.000 funcionários estão inclinadas a utilização de nuvem privadas, enquanto pequenas e médias empresas (PME) com menos de 1.000 funcionários inclinam para nuvens públicas. Como pode ser observado na Figura 3 [38].

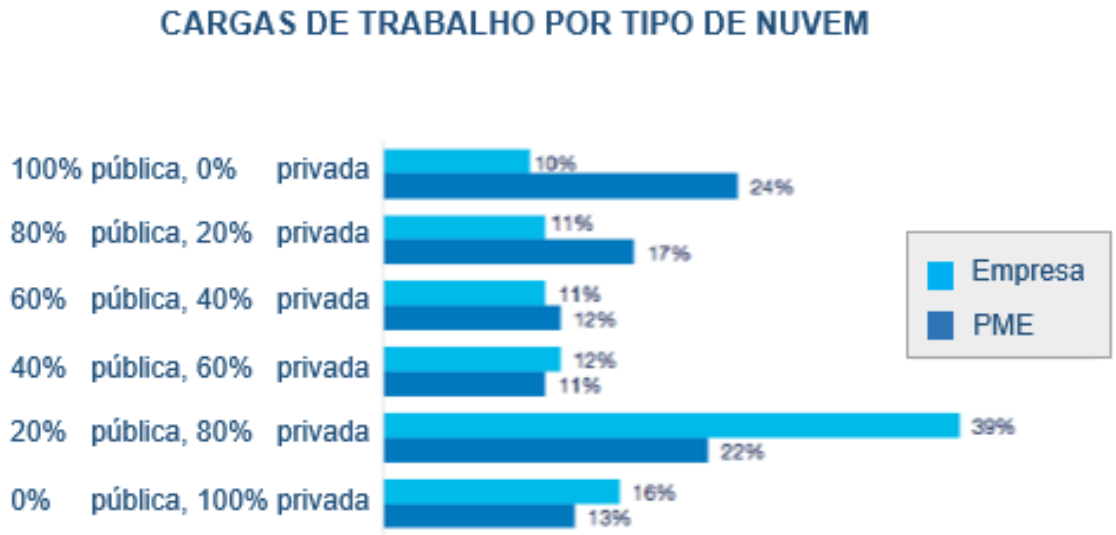

Figura 3: Uso da nuvem pública e privada em grandes e pequenas empresas [38]

SANS *Institute InfoSec Reading Room* [39], em 2015 realizou uma pesquisa com 485 profissionais que utilizavam uma variedade de provedores de nuvem e modelos de serviço. Em seu relatório apresentou o estado de uso dos modelos de serviço, identificando um maior uso de ofertas de *Software* como Serviço (SaaS) com um total de 59% das empresas estudadas, apesar disso a maior área de crescimento previsto é a Infraestrutura como Serviço (IaaS), onde 29% dos entrevistados planejam implantar um ambiente IaaS. Inúmeras são as razões para o deslocamento para PaaS e IaaS, como a velocidade e escalabilidade, juntamente com os serviços que o provedor pode proporcionar. A Figura 4 demonstra melhor a comparação do uso atual e o crescimento nos próximos 12 meses em cada modelo [39].

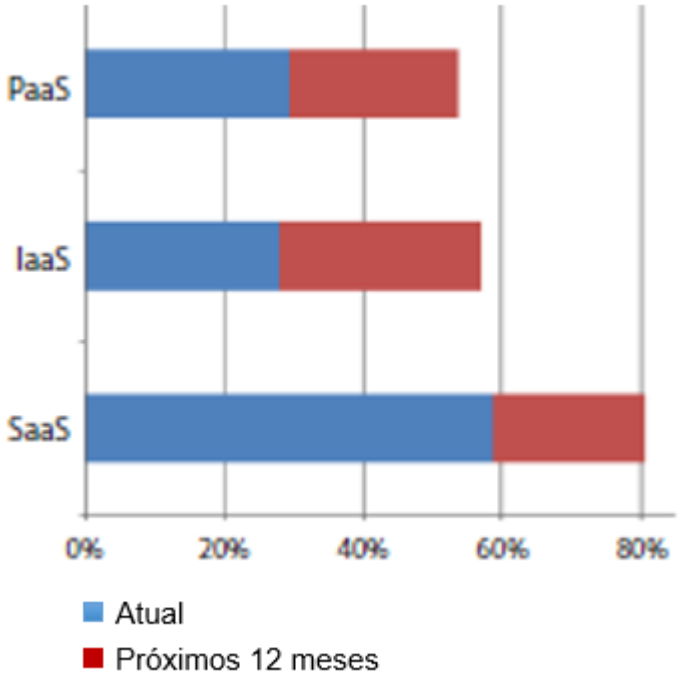

Figura 4: Uso atual e estimativa de crescimento da utilização dos modelos de serviço [39]

A Intel *Security* [40], divulgou um relatório em 2016 que também afirma que a maioria das organizações estão planejando investir em todos os modelos de serviços em nuvem, mas a maior porcentagem é para Infraestrutura como Serviço, seguido de Segurança como Serviço (SecaaS) e Plataforma como Serviço. Por último se encontra o *Software* como Serviço (SaaS) apesar de ser o mais utilizado. A Figura 5 demonstra o resultado comparativo entre os investimentos que as organizações desejam realizar em cada modelo de serviço.

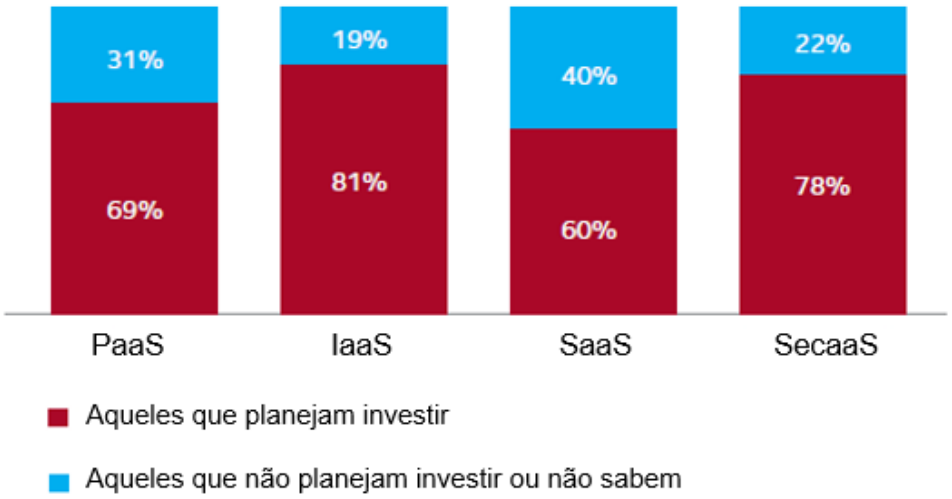

Figura 5: Comparações entre os investimentos em cada modelo de serviço [40]

A adoção da nuvem está crescendo juntamente com os benefícios oferecidos por ela, com maiores ganhos na velocidade da infraestrutura, à medida que as melhores práticas de nuvem se tornam mais estabelecidas e os provedores melhoram suas ofertas. Com o aumento da maturidade dos usuários e provedores, as preocupações com a segurança têm sofrido uma redução. O desafio passa a ser pessoal de TI especializado em Computação em Nuvem, para que o crescimento da adoção da nuvem seja ainda maior.

5.2 ADOÇÃO DA NUVEM NO BRASIL

Um estudo divulgado em 2016, realizado pela BSA - *The Software Alliance* [41] com 24 países que correspondem a 80% do mercado de TI mundial, cujo objetivo é avaliar políticas relacionadas à Computação em Nuvem baseado na performance em sete áreas, classificou o Brasil como 22º colocado, ficando na frente somente da China e Vietnã. Já o Japão, Estados Unidos e Alemanha ocupam as primeiras posições.

De acordo com o levantamento, o Brasil progrediu aproximadamente 4 pontos, apesar de ter permanecido na mesma colocação, se comparado com o último estudo

realizado em 2013. Avançando principalmente nas áreas de segurança, infraestrutura e liberdade na internet. Os pontos responsáveis para que o Brasil permaneça na mesma colocação, é a inexistência de uma legislação apropriada e balanceada para privacidade dos dados, lacunas na área de proteção à propriedade intelectual e a lentidão dos processos judiciais [41].

O ranking completo dos países envolvidos no estudo pode ser observado na Tabela 4.

Tabela 4: Ranking dos países [41]

Colocação	País	Pontuação
1	Japão	84.8
2	Estados Unidos	82.4
3	Alemanha	82.0
4	Canadá	80.9
5	França	80.7
6	Austrália	80.0
7	Singapura	79.5
8	Itália	79.3
9	Reino Unido	78.9
10	Polônia	76.7
11	Espanha	76.3
12	Coréia	75.5
13	Malásia	69.7
14	África do Sul	61.3
15	México	60.8
16	Argentina	58.0

17	Rússia	56.4
18	Índia	56.1
19	Turquia	54.4
20	Indonésia	49.4
21	Tailândia	48.8
22	**Brasil**	**48.5**
23	China	47.9
24	Vietnã	43.7

Pesquisas realizadas pela *Asia Cloud Computing Association* (ACCA) [42] sobre os países que possuem as melhores condições para oferta de Computação em Nuvem, o Brasil apareceu em 8º lugar, empatado com a Malásia, África do Sul e Emirados Árabes Unidos. Segundo ACCA, esta “é a primeira vez que a pesquisa sobre os 14 mercados da Asia-Pacífico inclui seis mercados não asiáticos para a comparação”.

Os parâmetros utilizados para elaboração do ranking, foi a conectividade internacional, qualidade da banda larga, disponibilidade e sustentabilidade de energia elétrica, risco a centro de dados, segurança, privacidade, ambiente regulatório, proteção à propriedade intelectual, sofisticação dos negócios e liberdade de informação. Os pontos que o Brasil se destacou positivamente foram relativos à energia, segurança e liberdade, já nos quesitos de conectividade internacional, risco a centro de dados e na proteção à propriedade intelectual o Brasil não teve uma boa pontuação [42].

Um relatório divulgado em abril de 2016, elaborado pela *Iternational Trade Administration* [2] para fornecer informações relacionadas ao mercado de Computação em Nuvem em outros países, para as empresas americanas que desejam entrar ou expandir os mercados internacionais, avaliou o Brasil como o maior mercado de serviços de computação da América Latina, o que tem atraído a atenção de fornecedores por todo o mundo. Apesar da oportunidade, os fornecedores deverão gerenciar questões como a preocupação com a segurança, deficiências de conectividade, altos custos e uma atual economia recessiva. A *DatacenterDynamics* também afirma que o

maior mercado tecnológico da América Latina é o Brasil, concentrando 45% dos centros de dados existentes nesta região [43].

O Brasil ainda precisa superar muitos desafios, como todos os que foram apresentados através das pesquisas que revelam o estado atual do Brasil em relação ao mundo. Ainda assim, é notório o crescimento da adoção da Computação em Nuvem no Brasil, pois cada vez mais empresários brasileiros têm sido atraídos pelos diversos benefícios dessa tecnologia.

Atualmente a grande busca por reduções de custos, favorece o crescimento do mercado em nuvem, pois grandes empresas brasileiras decidiram aderir esse modelo para resolver questões financeiras de forma ágil [44].

5.3 ADOÇÃO DA NUVEM NO GOVERNO BRASILEIRO

Tendo em vista o aumento da adoção da Computação em Nuvem por parte de órgão públicos e também como forma de incentivá-la, o Ministério do Planejamento, Orçamento e Gestão divulgou em maio de 2016, um manual intitulado de “Boas práticas, orientações e vedações para contratação de Serviços de Computação em Nuvem”.

Diretrizes importantes são abordadas no manual [45], tais como:

- Vedação de contratação de salas-cofre e salas seguras por órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), visando a redução dos gastos.
- Dados e informações de órgãos públicos devem ser hospedados em centros de dados localizados fisicamente no Brasil, a fim de resguardar o governo em eventuais questões legais.
- Recomenda-se a utilização de modelos híbridos, possibilitando a contratação de serviços privados, sem comprometer a segurança nacional.

A pioneira na criação de nuvem do governo federal é a SERPRO (Serviço Federal de Processamento de Dados), que lançou em 2013 uma nuvem computacional

projetada em *software* livre, voltada para as três modalidades básicas (infraestrutura, plataforma e *software*), e que abriga soluções para o programa “Cidades Digitais”.

5.4 PERSPECTIVAS FUTURAS

Mudanças em torno da nuvem, no cenário empresarial estão em ritmo acelerado. Há um grande crescimento em torno de ferramentas digitais, como a Internet das Coisas (IoT) e novos modelos de disponibilização da nuvem.

O uso dessa tecnologia está ampliando, e Gartner prevê que esse crescimento irá se tornar a maior parte dos novos gastos de TI. Para as empresas brasileiras os investimentos em 2017 podem chegar a 4,5 bilhões de dólares, e até 2020 atingirão 20 bilhões de dólares [46].

Gartner divulgou em maio de 2016 um documento chamado “*Market Insight: Cloud Computing’s Drive to Digital Business Creates Opportunities for Providers*” onde fez previsões da Computação em Nuvem para os anos seguintes. O estudo realizado afirma que, em 2020, uma política corporativa sem uso da nuvem (*no-cloud*) será tão rara quanto atualmente a existência de uma política sem uso da internet (no-internet) [47].

Conforme o estudo de Gartner relata, em 2019 mais de 30% dos investimentos em *softwares*, dos 100 maiores fornecedores desse segmento terão modificado sua estratégia “primeiro para nuvem” (*cloud-first*), para “exclusivamente para nuvem” (*cloud-only*). E em 2020, será vendido mais poder de computação através de provedores de nuvem IaaS e PaaS do está implantado em centro de dados corporativos [47].

6 PRINCIPAIS PROVEDORES DE COMPUTAÇÃO EM NUVEM

Uma pesquisa realizada em agosto de 2016 por Gartner, uma empresa de consultoria líder mundial em investigação de tecnologia de informação, sobre os principais provedores de serviços IaaS concluiu que o mercado de nuvem IaaS se consolidou significativamente em torno de dois principais provedores [48].

O Quadrante Mágico de Gartner [48], representado pela Figura 6, permite uma visão ampla das posições relativas dos concorrentes do mercado estudado. Sendo dividido em quatro tipos de provedores de tecnologia, os Líderes (executam bem sua visão atual e estão bem posicionados para o futuro), os Visionários (compreendem para onde o mercado está indo, mas ainda não executam bem), os Jogadores de nicho (focam com sucesso em um segmento pequeno, ou são desfocados e não inovam) e os Desafiadores (executam bem hoje ou dominam um grande segmento, mas não demonstram uma compreensão da direção do mercado).

Figura 6: Quadrante Mágico de Gartner [48]

Baseado nesse conceito os dois principais provedores consolidados como líderes no mercado de nuvem IaaS são a Amazon Web Service (AWS) e a Microsoft Azure, conforme observado na Figura 6.

6.1 COMPARAÇÃO ENTRE AMAZON AWS E MICROSOFT AZURE

O relatório *Magic Quadrant for Cloud Infrastructure as a Service, Worldwide,* divulgado por Gartner [48] apresenta informações importantes a respeito dos provedores, tais como suas ofertas, locais de atuação, pontos fortes e precauções. Baseado nessas informações, a Tabela 5 apresenta comparações entre os provedores de serviços IaaS líderes no mercado.

Tabela 5: Comparação entre AWS e Microsoft Azure [48]

	Amazon Web Service (AWS)	**Microsoft Azure**
Ano de Lançamento do Serviço	Empresa pioneira no mercado de nuvem, iniciada 2006.	Começou a disponibilizar serviços de IaaS em nuvem em 2013.
Ofertas	- Xen virtualizado *Multi-tenancy* e *compute-tenancy* única (*Elastic Compute Cloud* – EC2), com armazenamento *Multi-tenancy.* - Inúmeras capacidades adicionais de IaaS e PaaS, incluindo armazenamento de objetos com um sistema integrado CDN (*Amazon Simple Storage Service* – S3 e *CloudFront*). - Serviço de contentores *Docker* (EC2 *Container service* – ECS), orientação a eventos “sem servidor de computação” (Lambda), e uma experiência do desenvolvedor semelhante a aPaaS (*Elastic Beanstalk*).	- *Compute-Hyper-V* virtualizado *Multi-tenancy* (máquinas virtuais), com armazenamento *Multi-tenancy.* - Muitas capacidades IaaS e PaaS adicionais, incluindo o armazenamento de objeto (*Blob Storage*) e um CDN. - Azure *Marketplace* oferece *softwares* e serviços de terceiros. - Necessidades de colocação atendidas através de intercâmbios de parceiros (Azure *ExpressRoute*).

	- AWS *Marketplace*, possui uma extensa seleção de *softwares* e serviços de terceiros. - Necessidades de colocação atendidas através de intercâmbios de parceiros (AWS *Direct Connect*).	
Locais dos centros de dados	- Divide-se em regiões (cada uma com pelo menos duas zonas de centro de dados) - Costas Leste e Oeste dos Estados Unidos, Alemanha, Irlanda, Austrália, Índia, Japão, Cingapura, Coréia do Sul, Brasil e na China (previsão). - Uma região dedicada ao Governo Federal dos EUA.	- Divide-se em regiões - Várias regiões no Estados Unidos, Canadá, Austrália, Índia, Japão, Irlanda, Holanda, Hong Kong, Cingapura e Brasil. - Duas regiões dedicadas ao Governo Federal dos EUA. - Região da China é operado pelo 21Vianet Group, um serviço separado.
Relação com o Mercado		

	- Sua capacidade computacional sendo utilizada por clientes, é muitas vezes superior ao tamanho agregado de todos os outros provedores no mercado. - Mais de mil parceiros tecnológicos licenciaram seus *softwares* para serem executados na AWS, integrando-os aos recursos da AWS ou forneceram serviços complementares. - Uma quantidade elevada de parceiros de variados níveis e competências fornecem experiência em desenvolvimento de aplicativos, serviços gerenciados e serviços profissionais em nuvem. - Possui programas de treinamento e certificação da AWS, a fim de facilitar a adoção e operação da nuvem AWS.	- A Microsoft é uma marca consolidada no mercado. As relações existentes com os clientes, a história da execução de propriedades de Internet de consumidor de nível global, investimentos em engenharia e roteiro inovador facilitaram para que atingisse o status de provedor de nuvem estratégico IaaS. - Influencia seus clientes para a adoção da Azure lhes oferecendo descontos e mantendo os preços IaaS comparáveis a AWS para o público em geral. - A Microsoft está se tornando mais aberta e menos dependente do Windows, sistema operacional de sua autoria, criando o suporte também para o sistema operacinal Linux e outras tecnologias de código aberto.

		- A rede de parceiros para o apoio de resoluções de desafios de implementação complexos ainda está em construção, o que pode comprometer a qualidade das soluções oferecidas aos seus clientes. - Com poucos especialistas fora da Microsoft, poucas opções para o treinamento da Azure são fornecidas.
Inovação	- Líder em pensamento ágil e inovador com extensa variedade de mercados de TI, expandindo de maneira rápida suas ofertas de serviços e oferecendo soluções de alto nível.	- A Microsoft conta com altos níveis de investimento em engenharia e inovação. - Vem desenvolvendo rapidamente novos recursos e serviços, principalmente os que possibilitam interoperabilidade com a infraestrutura local.

Uso Recomendado	- Todos os serviços que se adaptam bem a um ambiente virtualizado. - Os serviços que possuem desafios para virtualizar ou executar em ambiente *Multi-tenancy*, como serviços com elevada segurança ou complexidade, requerem uma atenção especial.	- Aplicações empresariais de maneira geral e as que utilizam tecnologias Microsoft. - Aplicativos nativos da nuvem (incluindo Internet das Coisas).

Muitas organizações têm substituído ou complementado gradualmente seus centros de dados tradicionais por nuvem IaaS. E a avaliação para a adoção de uma nuvem IaaS não é mais simplesmente calcular a capacidade de armazenamento distribuído sob demanda, mas sim de uma maneira ampla onde a plataforma de infraestrutura contemple tanto a eficiência e agilidade, combinado com escalabilidade sem precedentes e presença global. A direção do mercado tem favorecido os dois provedores líderes, a AWS e Microsoft Azure que são responsáveis por quase todo o consumo de infraestrutura relacionada com nuvem IaaS [48].

Gartner afirma que “A próxima fase do mercado ainda não emergiu”. A próxima fase a qual ele se refere é a provável maior integração das capacidades IaaS e PaaS, incluindo uma maior utilização de tecnologias de contentores e gestão de operações automatizadas. Espera-se que as mudanças sejam de forma gradual e não de maneira súbita. E a previsão é que até 2018 o ambiente competitivo não irá mudar significativamente, logo os novos operadores no mercado terão um impacto pequeno antes desse tempo [48].

7 CONCLUSÕES E TRABALHOS FUTUROS

A Computação em Nuvem é um modelo que vem sendo amplamente utilizado no campo da TI e a cada dia possui mais usuários, sejam eles indivíduos ou organizações, com o desejo de usufruir as vantagens que por ela são oferecidas. O estudo realizado evidencia como o modelo apresentado pode trazer benefícios para as organizações que vierem adotá-la, mas também explicita os potenciais riscos que devem ser levados em consideração durante o processo de avaliação à viabilidade de adoção da nuvem.

Os usuários devem estar cientes das ameaças de segurança provindas do seu uso e aplicar cautelosamente medidas para mitigação dos riscos. Como este modelo utiliza tecnologias específicas, possui questões únicas relacionadas à segurança, questões essas que são adicionais às preocupações dos sistemas convencionais, pois apesar de abordar vulnerabilidades reconhecidas, as suas características dinâmicas são capazes de impedir a eficácia das medidas tradicionais.

Esta pesquisa analisou questões de segurança provindas da natureza compartilhada, virtualizada e pública da nuvem, apresentando formas para auxiliar na avaliação e na redução dos riscos. Os principais pontos abordados foram em relação a segurança da rede, dos dados e das aplicações, de forma a garantir a integridade, confidencialidade e disponibilidade das informações e comunicações.

A Computação em Nuvem possui grande potencial em se tornar líder em solução de TI segura e economicamente viável para as organizações. Conforme os benefícios têm ultrapassado as suas deficiências, mais organizações estão migrando ou iniciando seus negócios na Nuvem. Uma projeção realizada pelo Pat Gelsinger, CEO da VMware, afirma que a partir de 2021 será o modelo que irá superar os ambientes tradicionais e que até 2030, estará abrigando 52% das cargas totais de TI em Nuvem Pública, 29% em Nuvem Privada e apenas 19% mantidas no conceito tradicional [49].

7.1 TRABALHOS FUTUROS

Diante do exposto e da expansão em que o mercado se encontra, um tema que poderia ser abordado e explorado é a Internet das Coisas. Esta tecnologia possibilita a conexão de dispositivos não convencionais, que estão ao nosso redor executando funções específicas e se comunicando através de programas centralizados na nuvem. Com a grande quantidade de informações digitais disponíveis, será importante abordar aspectos relevantes voltados a segurança e privacidades desses dados.

8 REFERÊNCIAS

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg e I. Brandic, “Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility,” *Future Generation Computer Systems,* 2009.

[2] International Trade Administration, “2016 Top Markets Report Cloud Computing,” Abril 2016.

[3] Q. Zhang, L. Cheng e R. Boutaba, “Cloud Computing: State-of-the-Art And Research Challenges,” *Journal of Internet Services and Applications,* 2010.

[4] F. R. C. Sousa, L. O. Moreira e J. C. Machado, “Computação em Nuvem: Conceitos, Tecnologias, Aplicações e Desafios,” *Tópicos em Sistemas Colaborativos, Interativos, Multimídia, Web e Bancos de Dados, Sociedade Brasileira de Computação,* pp. 101-130, 2010.

[5] L. M. Vaquero, L. Rodero-Merino, J. Caceres e M. Lindner, “A Break in the Clouds: Towards a Cloud Definition,” *ACM SIGCOMM Computer Communication Review,* vol. 39, nº 1, pp. 50-55, 2008.

[6] S. R. M. Amarante, Artist, *Utilizando o Problema de Múltiplas Mochilas Para Modelar o Problema de Alocação de Máquinas Virtuais em Computação Nas Nuvens.* [Art]. Universidade Estadual do Ceará, 2013.

[7] M. Hogan, F. Liu, A. Sokol e J. Tong, “NIST Cloud Computing Standards Roadmap,” *NIST Special Publication 500-291,* 2011.

[8] CSA, Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing - Version 3.0,” *Cloud Security Alliance,* 2011.

[9] M. Veras, Cloud Computing: Nova Arquitetura da TI, Brasport, 2012.

[10] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica e M. Zaharia, Artists, *Above the Clouds: A Berkeley View of Cloud Computing.* [Art]. University of California at Berkeley, 2009.

[11] ISACA, Information Systems Audit and Control Association, “Princípios Norteadores de Adoção e Uso da Computação em Nuvem,” *Um Documento ISACA da série Visão sobre Computação em Nuvem,* 2012.

[12] S. Chaves, Artist, *A Questão dos Riscos em Ambientes de Computação em Nuvem. Dissertação de mestrado.* [Art]. Univerdide de São Paulo, 2011.

[13] ISACA, Information Systems Audit and Control Association, “Computação em Nuvem: Benefícios Para o Negócio com Perspectivas de Segurança, Governança e Qualidade,” *Documento Técnico da ISACA sobre Tecnologias Emergentes,* 2009.

[14] COSO, Committee of Sponsoring Organizations of the Treadway Commission, “Gerenciamento de Riscos Corporativos - Estrutura Integrada,” 2007.

[15] CSA, Cloud Security Alliance, “The Treacherous 12 Cloud Computing Top Threats in 2016,” *Top Threats Working Group,* Fevereiro 2016.

[16] M. Ali, S. U. Khan e A. V. Vasilakos, “Security in Cloud Computing: Opportunities and Challenges,” *Information Sciences,* vol. 305, pp. 357-383, 2015.

[17] CSCC, Cloud Standards Customer Council, “Cloud Security Standards: What to Expect & What to Negotiate - Version 2.0,” Agosto 2016.

[18] D. Zissis e D. Lekkas, “Addressing Cloud Computing Security Issues,” *Future Generation Computer Systems,* vol. 28, pp. 583-592, 2012.

[19] R. d. C. C. d. Castro e V. L. P. d. Sousa, “Segurança em Cloud Computing: Governança e Gerenciamento de Riscos de Segurança,” em *III Congresso Tecnológico de TI e Telecom InfoBrasil 2010, Anais Eletrônicos*, Fortaleza, CE, 2011.

[20] A. d. S. Netto e M. A. P. d. Silveira, “Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas,” *JISTEM-Journal of Information Systems and Technology Management,* vol. 4, nº 3, pp. 375-397, 2007.

[21] M. Sêmola, Gestão da Segurança da Informação, Rio de Janeiro, 2003.

[22] R. A. d. Jesus e J. S. d. Fonseca, “Aspectos da Segurança da Computação em Nuvens”.

[23] W. Jansen e T. Grance, “Guidelines on Security and Privacy in Public Cloud Computing,” *NIST Special Publication 800-144,* Dezembro 2011.

[24] ISACA, Information Systems Audit and Control Association, “Governança da Nuvem: Perguntas que os Conselhos Diretores Precisam Fazer,” *Um Informe Cloud Vision Series da ISACA,* 2013.

[25] S. Liu, “Securing the Clouds: Methodologies and Practices,” em *Encyclopedia of Cloud Computing*, Wiley, 2016.

[26] V. (. Winkler, Securing the Cloud, Elsevier, 2011.

[27] J. M. Myerson, “Craft a Cloud Service Security Policy,” *IBM Developer Works,* 23 Junho 2011.

[28] CSA, Cloud Security Alliance, “Security Guidance for Critical Areas os Focus in Cloud Computing - Version 2.1,” *Cloud Security Alliance,* 2009.

[29] B. R. Kandukuri, R. Paturi e A. Rakshit, “Cloud Security Issues,” em *2009 IEEE International Conference on Services Computing*, 2009.

[30] P. Samarati e S. D. C. d. Vimercati, “Cloud Security: Issues and Concerns,” em *Encyclopedia of Cloud Computing*, Wiley, 2016.

[31] L. V. d. Silva e M. E. Finkelstein, “A Necessidade de Regulação Legislativa Para Utilização do Serviço de Computação em Nuvem,” *Revista Estudos Legislativos,* pp. 81-102, 2014.

[32] B. Halpert, Auditing Cloud Computing, Wiley Corporate, 2011.

[33] The National IT and Telecom Agency, “Cloud Audit and Assurance,” Março 2011.

[34] CSA, Cloud Security Alliance, “Category 10 Network Security,” *SecaaS Implementation Guidance,* Setembro 2012.

[35] Open Web Application Security Project, “OWASP Top 10 - 2013,” 2013.

[36] Software Assure Forum for Excelence in Code e Cloud Security Alliance, “Practices for Secure Development of Cloud Applications,” 5 Dezembro 2013.

[37] CSA Global Enterprise Advisory Board, “State of Cloud Security 2016,” 2016.

[38] RightScale, “State of the Cloud Report,” 2016.

[39] D. Shackleford, “Orchestrating Security in the Cloud,” *A SANS Survey,* Setembro 2015.

[40] McAfee parte da Intel Security, “Blue Skies Ahead? The state of cloud adoption,” 2016.

[41] BSA The Software Alliance, “2016 BSA Global Cloud Computing Scorecard,” 2016.

[42] Asia Cloud Computing Association, “Cloud Readiness Index 2016,” 2016.

[43] DatacenterDynamics, “DatacenterDynamics,” 21 Junho 2016. [Online]. Available: http://www.datacenterdynamics.com.br/focus/archive/2016/06/novamente-s%C3%A3o-paulo-ser%C3%A1-palco-do-maior-evento-de-data-center-da-am%C3%A9rica-latin. [Acesso em 07 Novembro 2016].

[44] I. C. Gastim, “Estadão Economia e Negócios,” 21 Julho 2015. [Online]. Available: http://economia.estadao.com.br/noticias/governanca,empresas-investem-em-servicos-de-nuvem-para-cortar-custos,1728877. [Acesso em 16 Novembro 2016].

[45] Ministério do Planejamento, Orçamento e Gestão, “Boas Práticas, Orientações e Vedações Para Contratação de Serviços de Computação em Nuvem,” 12 Maio 2016.

[46] J. Mejías, “ComputerWorld,” 01 Novembro 2016. [Online]. Available: http://computerworld.com.br/tendencias-que-impactarao-o-mercado-de-cloud-computing-em-2017. [Acesso em 20 Novembro 2016].

[47] C. Stamford, “Gartner Says By 2020, a Corporate "No-Cloud" Policy Will Be as Rare as a "No-Internet" Policy Is Today,” Gartner, 22 Junho 2016. [Online]. Available: http://www.gartner.com/newsroom/id/3354117. [Acesso em 20 Novembro 2016].

[48] L. Leong, G. Petri, B. Gill e M. Dorosh, “Magic Quadrant for Cloud Infrastructure as a Service, Worldwide,” Gartner, 03 Agosto 2016. [Online]. Available: https://www.gartner.com/doc/reprints?id=1-2G45TQU&ct=150519. [Acesso em 23 Novembro 2016].

[49] F. Dreher, “ComputerWorld,” 04 Outubro 2016. [Online]. Available: http://computerworld.com.br/cloud-ira-superar-ti-tradicional-partir-de-2021. [Acesso em 06 Dezembro 2016].