A TRUST MODEL FOR CLOUD COMPUTING ENVIRONMENT

Teófilo Teixeira Branco Júnior (Universidade do Minho, Guimarães, Portugal) - teofilotb@hotmail.com
Henrique Manuel Dinis dos Santos (Universidade do Minho, Guimarães, Portugal) - hsantos@dsi.uminho.pt

This paper presents a proposal for a management model containing requirements concerning reliability in Cloud Computing (CC). The proposal was based on a literature review focused on the problems, challenges and underway studies related to the safety and reliability of applications and Information Systems (IS) in this technological environment. This literature review examines the existing obstacles and challenges from the point of view of respected authors on the subject. The main issues are addressed and structured as a model, called "Trust Model for Cloud Computing environment". This is a proactive proposal that aims to organize and discuss management solutions for the CC environment aiming improved reliability of the IS applications operation, both for providers and their customers.

Keywords: Cloud Computing, Information Systems, Information Security, Trust Model, Cloud Security.

UM MODELO DE CONFIANÇA PARA O AMBIENTE DE COMPUTAÇÃO EM NUVEM.

Este artigo apresenta uma proposta de um modelo de gestão contendo requisitos relacionados com a confiabilidade dos sistemas no ambiente de Computação em Nuvem (CN). A proposta teve como base uma revisão da literatura sobre os problemas, desafios e estudos que estão em curso relacionados com a segurança e confiabilidade de aplicações e Sistemas de Informações (SI) neste ambiente tecnológico. Nesta revisão bibliográfica são abordados os entraves e desafios atualmente existentes na visão de conceituados autores sobre o tema. Estas questões foram abordadas e estruturadas na forma de um modelo, denominado de "Modelo de Confiança para o ambiente de Computação em Nuvem". Trata-se de uma proposta proativa que tem por objetivo organizar e discutir soluções de gestão para o ambiente de CN com uma maior confiabilidade para a operacionalização das aplicações de SI, tanto por parte dos provedores como também dos seus clientes.

Palavras-Chave: Computação em Nuvem, Sistemas de Informação, Segurança da Informação, Modelo de Confiança, Segurança na Nuvem.

1. Introdução

O objetivo deste trabalho, como parte integrante de projeto de investigação do autor, é o de organizar, através de uma revisão da literatura, pontos polêmicos e de discussão sobre os entraves existentes para a plena utilização dos sistemas de informações em ambiente de Computação em Nuvem, sob a ótica da confiabilidade.

A nova tecnologia de Computação em Nuvem (CN) causa dúvidas e desconfianças sobre a conveniência da adoção desta tecnologia, principalmente no tocante a segurança da

informação. Embora promissora, esta tecnologia necessita ainda resolver diversos pontos de vulnerabilidade (Grobauer, Walloschek, and Stocker 2011).

A partir da percepção das incertezas que pairam sobre o ambiente de CN acerca da segurança na operacionalização de aplicações e guarda de dados, o autor vislumbrou a oportunidade do tratamento destas questões, partindo inicialmente por uma revisão da literatura para elucidar os principais pontos polêmicos e em discussão no momento.

A partir desta revisão da literatura, é proposto um modelo de gestão do ambiente de CN que visa organizar e verificar os requisitos necessários para que os Sistemas de Informações operem com confiabilidade e segurança no ambiente de CN, fatores estes essenciais para que esta tecnologia produza bons resultados para a operação de sistemas de informação, tanto do ponto de vista da racionalização dos recursos, como do seu efetivo uso e guarda de dados.

Este trabalho tem por finalidade colaborar com os provedores de ambiente de CN, desenvolvedores de aplicações para CN e clientes usuários no sentido de orientar como é possível tornar confiável o ambiente de Nuvem a ser utilizado pelas organizações para a guarda de seus dados. O desenvolvimento e o aprofundamento deste estudo abrem perspectivas para trabalhos futuros, como por exemplo, o do desenvolvimento de um framework para apuração do nível de reputação dos provedores de serviços e de desenvolvedores de aplicações no ambiente de CN.

1.1 Estrutura do artigo

Com o intuito de explorar a temática proposta, este artigo está organizado em cinco Seções: Na primeira Seção são abordadas a introdução, definição dos objetivos, estrutura e a metodologia do presente estudo.

A Seção 2 trata da metodologia de pesquisa que norteou os fundamentos teóricos da proposta deste artigo. No caso em estudo foi realizada uma revisão da literatura.

Na Seção 3 é feita uma contextualização do ambiente de Computação em Nuvem envolvendo os principais conceitos relacionados, as camadas de arquitetura, os modelos de implementação e vantagens do uso deste ambiente para os usuários.

A Seção 4 versa sobre os desafios relacionados a confiabilidade e a segurança do uso de Sistemas de Informação no ambiente de Computação em Nuvem. São abordados os principais pontos de vista convergentes dos autores pesquisados e as propostas sugeridas.

Na Seção 5 é apresentada uma proposta de gestão operacional para o ambiente de Computação em Nuvem através da proposição do "Modelo de Confiança".

Finalmente, na Seção 6 são apresentadas as conclusões sobre os estudos desenvolvidos, os benefícios esperados e as possibilidades de aprimoramento da gestão operacional dos sistemas de informação no ambiente de CN, complementando-as com as recomendações e perspectivas de trabalhos futuros a serem desenvolvidos.

2. Revisão da Literatura

Uma boa revisão de literatura cria uma base sólida para o avanço do conhecimento. Deste modo, facilita o desenvolvimento da teoria, fecha as áreas onde existe uma infinidade de pesquisas e descobre áreas onde é necessária a investigação e proporciona uma contribuição importante no estabelecimento de orientações para o futuro da investigação que são fundamentais para o fortalecimento na área em estudo (Webster, Jane; Watson 2002).

Primeiramente, procurou-se identificar os principais riscos envolvidos na tecnologia da Computação em Nuvem, notadamente relacionados a operacionalização de Sistemas de Informação e seus respectivos dados. Nesse sentido, uma pesquisa da literatura foi realizada no sentido de:

i. Caracterizar os trabalhos apresentados sobre a problemática tratada, identificando os pontos relevantes, carências apontadas e os pontos de vista apresentados;
ii. Fazer uma catalogação das questões envolvidas de forma crítica em relação as opiniões dos autores pesquisados, a fim de definir os pontos de interesse do autor;
iii. Ressaltar as premissas e os requisitos necessários para o uso e disponibilização de aplicações de SI no ambiente de Computação em Nuvem.

O objetivo da pesquisa da literatura foi a de encontrar trabalhos que tratasse das seguintes questões de partida:

i. Quais são as vulnerabilidades e riscos envolvidos na operacionalização de sistemas o ambiente de Computação em Nuvem?
ii. Quais podem ser verificadas a prestação e a conformidade dos serviços de TI no ambiente de Computação em Nuvem?
iii. Quais são os aspectos que devem ser observados no processo de migração da TI tradicional para o ambiente de Computação em Nuvem?

Foram utilizadas as seguintes palavras-chave e termos utilizados para a pesquisa por título, nos idiomas Inglês e Português:

i. “Plataformas, Modelos e *Frameworks* de TI no ambiente em Computação em Nuvem”,
ii. “Segurança em Computação em Nuvem”,
iii. “Vulnerabilidades no ambiente de Computação em Nuvem”,
iv. “Migração de TI tradicional para Computação em Nuvem”.

Foram selecionadas as seguintes fontes de acordo com o seguinte critério de prioridade:

i. Publicações de artigos em revistas científicas;
ii. Teses e dissertações;
iii. Anais de conferências internacionais.

Na pesquisa das revistas científicas, foi realizada consulta no SCImago Journal & Country Rank (http://www.scimagojr.com) para verificação da visibilidade das revistas (SJR). Foi atribuída uma maior atenção aos aspectos qualitativos considerando o número de citações dos artigos, de forma a selecionar aqueles que tivessem maior impacto. Os seguintes

Journals foram selecionados com base no nome da revista, na descrição, área de estudo e categoria.

i. MIS Quarterly: Management Information Systems; Information Systems Research;
ii. ACM Transactions on Database Systems;
iii. Robotics and Computer-Integrated Manufacturing;
iv. Information Systems Journal;
v. Journal of the Association of Information Systems;
vi. International Journal of Project Management;
vii. IEEE Transactions on Engineering Management;
viii. Information Systems Management;
ix. Project Management Journal;
x. Enterprise Information Systems;
xi. Journal of Computer Information Systems;
xii. Information and Organization; Information Systems Management.

Considerando o escopo da pesquisa, os artigos foram preferencialmente pesquisados nas seguintes bases de dados levando-se em conta o vasto conjunto de artigos publicados relacionados com o assunto em estudo:

i. Elsevier Science Direct (http://www.sciencedirect.com);
ii. IEEE Xplore (http://ieeexplore.ieee.org/);
iii. ACM Digital Library (http://www.portal.acm.org/dl.cfm);
iv. Springer Link (https://www.link.springer.com);

Foram também realizadas consultas na Web of Science (http://workinfo.com), Scopus (http://www.scopus.com) e J. Stor (http://www.jstor.org). Salientamos que os artigos foram selecionados a partir do título, resumo e palavras-chave. Destas fontes, foi dada prioridade a referências com menos de cinco anos. Foram selecionados os trabalhos levando-se em conta critérios como adequação ao tema do presente trabalho, relevância das publicações, produção acadêmica dos autores e citações de seus trabalhos.

A partir do material pesquisado, foi realizada uma leitura preliminar nos resumos dos artigos, no sentido de selecionar aqueles que se encontram dentro do objetivo da pesquisa. Assim, a revisão da literatura foi realizada numa primeira fase, em função do título, do resumo e nas palavras-chave, mas, em alguns casos, devido à inadequação do conteúdo do artigo com a temática em investigação, não foi integrada na bibliografia. Como resultado da pesquisa da temática em investigação, foi elaborada uma matriz de conceitos-chave por referências bibliográficas (Webster, Jane; Watson 2002) , conforme relacionado na Tabela 1.

Os resultados desta pesquisa serviram para embasar a proposta do "Modelo de confiança" que versa sobre a proposição de um modelo de gestão operacional do ambiente de CN estruturando os requisitos de confiabilidade necessários para tal.

Referências	**Conceitos Chave**			
	Plataformas/ Modelos Frameworks	**Segurança**	**Vulnerabilidades**	**Migração**

B. Grobauer et al, 2011			●	
P. Mell and T. Grance, 2011	●			
R. Buyya et al, 2011	●			
C. Weinhardt et al, 2009	●		●	
A. Lenk et al, 2009	●			
R. Buyya et al, 2009	●			
S. P. Mirashe and N. V Kalyankar,2010	●			
J. Che et al, 2011	●	●		
Y. Chen et al, 2010		●	●	
G. Dhillon and J. Backhouse, 2000	●			
M. Armbrust et al, 2009	●		●	
M Kanchana et al, 2013		●		
M. Jensen et al, 2009		●	●	
A. Khajeh-Hosseini et al, 2010				●
H. Mouratidis et al, 2013	●	●		●
S. Mansfield-Devine, 2008			●	●

Tabela 1 – Matriz de autores x conceitos-chave

3. O ambiente de Computação em Nuvem

Esta seção descreve os conceitos necessários ao entendimento desta tecnologia. Na Seção 3.1 são discutidos os conceitos relacionados a Computação em Nuvem e os modelos de sua implementação. Na Seção 3.2 são abordadas as vantagens da sua adoção para usuários, empresas e organizações.

3.1 A Computação em Nuvem

Computação em Nuvem são depósitos de recursos virtualizados de TI facilmente utilizáveis e acessíveis, nos quais o fornecedor oferece garantias de utilização e de qualidade do uso desses serviços e o usuário é tarifado somente pelo que utilizar (Mell and Grance 2011).

O provedor de serviços supre os recursos computacionais a cliente oferecendo acesso aos recursos de TI a baixo, uma vez que este último não se preocupa com a aquisição e manutenção da infraestrutura de TI (Mell and Grance 2011).

O ambiente de Computação em Nuvem é acessado através da Internet, sendo fundamental o seu acesso para que o usuário possa desfrutar do serviço ofertado. A infraestrutura de comunicação é composta por um conjunto de hardwares, softwares, redes de telecomunicação e interfaces que permitem a entrega da computação como serviço. Para viabilizar este modelo, torna-se necessário reunir todas as aplicações e dados dos usuários em grandes centros de armazenamento, denominados de "datacenter"(Rajkumar Buyya, Broberg, and Goscinski 2011).

Computação em Nuvem representa um modelo de serviço onde a premissa é a do fornecimento de todo o tipo de processamento de sistemas de informação e de aplicações tecnológicas, através da disponibilização da infraestrutura e armazenamento de dados através da internet, pautado sobretudo na necessidade de consumo do usuário (Rajkumar Buyya, Broberg, and Goscinski 2011).

De acordo com os recursos providos e o modelo de serviço ofertado pelo provedor do ambiente de computação em Nuvem, os serviços podem ser categorizados em três camadas: Infraestrutura como Serviço (IaaS); Plataforma como Serviço (PaaS); e Software como Serviço (SaaS), conforme ilustrado na Figura 1 (Weinhardt et al. 2009).

i. Infraestrutura como Serviço (IaaS). Nesta camada são oferecidos os serviços de infraestrutura sob demanda, isto é, oferece recursos "de hardware" virtualizados como computação, armazenamento e comunicação. Este tipo de serviço prove servidores capazes de executar softwares customizados e operar em diferentes sistemas operacionais. Possui uma aplicação que funciona como uma interface única para a administração da infraestrutura, promovendo a comunicação com hosts, switches, roteadores e o suporte para a inclusão de novos equipamentos. É responsável por prover a infraestrutura necessária para as outras classes intermediária e superior.
ii. Plataforma como Serviço (PaaS). É oferecido como serviço um ambiente no qual o desenvolvedor pode criar e implementar aplicações sem ter que se preocupar com a infraestrutura de hardware que irá necessitar. Esta classe fornece uma infraestrutura com nível de integração compatível com diversos sistemas operacionais, linguagens de programação e ambientes de desenvolvimento.
iii. Software como Serviço (SaaS). Essa camada disponibiliza aplicações completas ao usuário final. Este acesso é provido pelos prestadores de serviço através de portais web, permitindo a execução de aplicações que são executadas na nuvem a partir de uma máquina local. Para oferecer esta transparência, o SaaS utiliza-se das outras duas camadas inferiores, o PaaS e o IaaS.

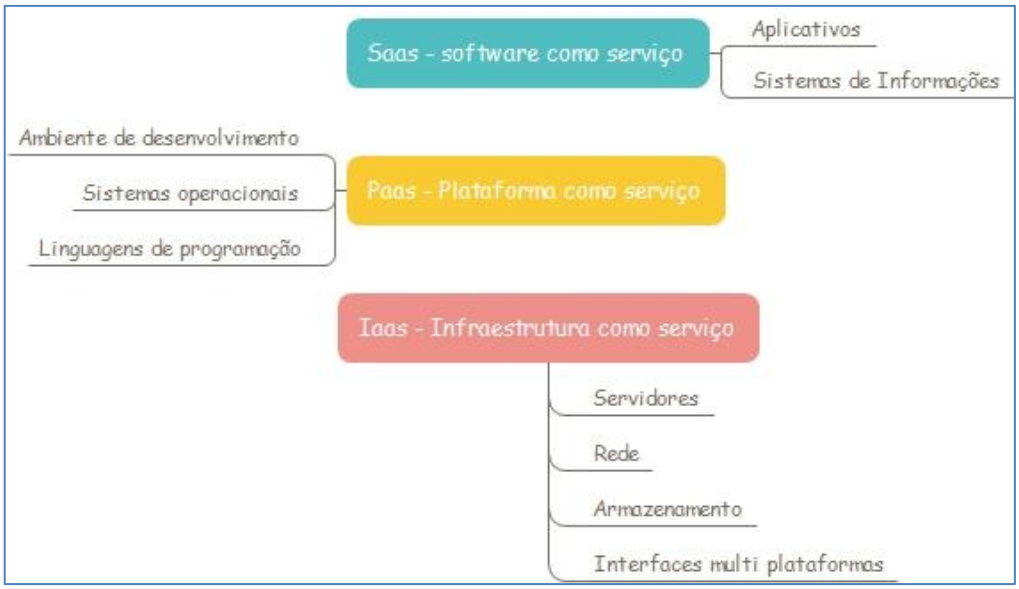

Figura 1. Camadas de arquitetura de Nuvem.

A implementação da nuvem irá depender da aplicação a ser oferecida e do tipo de contrato de prestação de serviço. Atualmente os tipos de modelo de implementação são Público, Privado, Comunidade e Híbrido (Figura 2) (Weinhardt et al. 2009):

i. Privado - As nuvens privadas são construídas exclusivamente sobre um Data Center privado. Neste caso, a organização provém a estrutura completa da infraestrutura e dos serviços. Somente os seus órgãos e setores internos assumem o papel de clientes consumidores dos recursos.
ii. Público - As nuvens públicas são executadas por terceiros. As aplicações de diversos usuários ficam misturadas nos sistemas de armazenamento. Este é o tipo de uso mais comum disponibilizado aos consumidores pessoas físicas. Há um compartilhamento entre os recursos de infraestrutura compartilhados e o usuário não tem ideia de onde seus dados ficam armazenados.
iii. Comunidade - A infraestrutura de nuvem é compartilhada por diversas organizações que se unem para suportar e prover uma comunidade específica.
iv. Híbrido - Nas nuvens híbridas temos uma composição de mais de um modelo de Nuvem. Algumas aplicações podem ser públicas e outras privadas e os recursos de TI são escalonados a partir da necessidade de alocação dos recursos que podem ser integrados entre si.

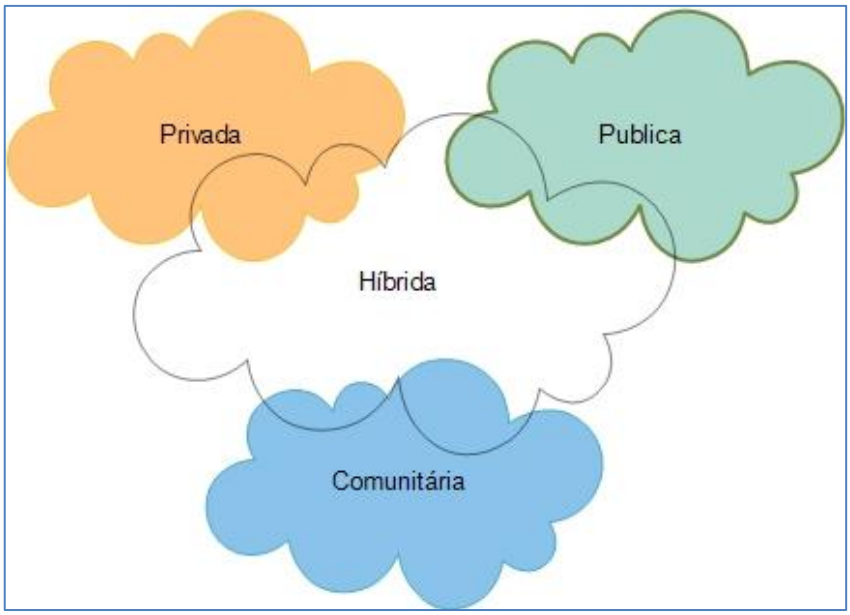

Figura 2. Modelos de implementação de nuvem

Em relação aos participantes da Nuvem (Figura 3), estes podem ser categorizados em três grupos: (Mell and Grance 2011)

i. Provedores de serviço. É quem disponibiliza, gerencia e monitora toda a infraestrutura do ambiente de Computação em Nuvem, garantindo o nível de serviço acordado e a segurança adequada para os dados e as aplicações dos usuários clientes;
ii. O desenvolvedor é o responsável por desenvolver e prover serviços de sistemas de informações e aplicações para uso pelo usuário, a partir da infraestrutura oferecida pelo provedor do serviço de infraestrutura;
iii. O usuário final é o consumidor que irá utilizar os recursos oferecidos pelo ambiente de Computação em Nuvem.

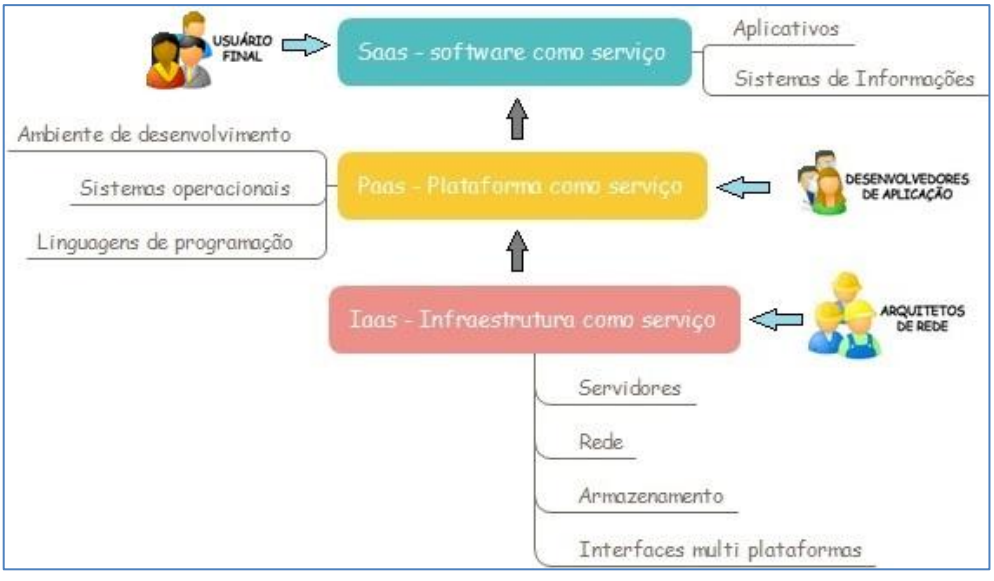

Figura 3 – Participantes no ambiente de Computação em Nuvem

3.2 As vantagens do uso da Computação em Nuvem

No ambiente de Computação em Nuvem, a convergência de tecnologias propicia à computação na nuvem prover serviços de forma transparente aos usuários consumidores desta tecnologia. Ressaltam-se as seguintes vantagens para os usuários (R. Buyya et al. 2009):

i. Elasticidade e escalonamento. A Computação na Nuvem propicia a sensação de recursos computacionais ilimitados disponíveis para uso. Neste sentido, usuários tem a expectativa de lhes sejam fornecidos recursos em qualquer quantidade e a qualquer momento;
ii. Espera-se que a provisão de recursos adicionais ocorra de forma automática, quando do aumento da demanda e retirados no caso da diminuição desta demanda;
iii. Auto atendimento. O consumidor de serviços da computação na nuvem espera adquirir recursos computacionais de acordo com sua necessidade e de forma instantânea. Para suportar este tipo de expectativa, as nuvens devem permitir que os usuários possam solicitar, personalizar, pagar e usar os serviços desejados sem intervenção humana;
iv. Faturamento e medição por consumo. O usuário tem a opção de requisitar e utilizar a quantidade de recursos e serviços que ele julgar necessários. Os serviços devem ser precificados com base em uma métrica de curta duração, como por exemplo, medido em horas de uso. Por esta razão, as nuvens devem implementar recursos que garantam um eficiente comércio de serviços, tais como tarifação adequada, contabilidade, faturamento, monitoramento e otimização do uso;
v. Amplo acesso ao ambiente de qualquer meio ou plataforma. Os recursos devem estar disponíveis através da rede para serem acessados através de mecanismos padrões que permitam a utilização destes por plataformas heterogêneas, como smartphones, notebooks e outros dispositivos.

Atualmente, a estrutura das nuvens tem se mostrado eficaz no tocante ao disponibilizar ao usuário uma boa qualidade e quantidade de aplicações e serviços. Torna-se importante, contudo, prover especial atenção em relação a segurança dos dados, padronização e modelos de negócios para que esta possa vir a se tornar um ambiente confiável e seguro do ponto de vista técnico e negocial para a satisfação de todos os participantes envolvidos. Em relação a gestão do ambiente de Computação em Nuvem, torna-se necessário construir modelos de gestão capazes de incorporar a dinâmica da evolução entre a tecnologia e a sua utilização (Rajkumar Buyya, Broberg, and Goscinski 2011).

4. Desafios relacionados com a confiabilidade no ambiente de Computação em Nuvem

Apesar das vantagens na perspectiva do negócio, a Computação em Nuvem ainda apresenta desafios, sobretudo em relação à desconfiança dos usuários em colocarem seus dados em computadores dos quais não possuem controle. A Internet se apresenta como um ambiente hostil e isso torna-se crítico quando se tem dados confidenciais trafegando entre os terminais e os servidores em Nuvem (Mirashe and Kalyankar 2010).

Tanto para os executivos quanto para os técnicos da área de Tecnologia da Informação, torna-se um desafio descobrir como a Computação em Nuvem pode ser confiável e prover

o nível de segurança necessária para a sua plena operação. Neste sentido, há uma preocupação cada vez maior com a segurança. O nível de preocupação varia desde conformidades com regulamentações até a questão da segurança no trato com os usuários finais (Che et al. 2011).

As principais abordagens na área de Segurança da Informação não fazem distinção do ambiente a que estão aplicadas, o que equivale a deduzirmos que as preocupações e normas de segurança que se aplicam aos sistemas tradicionais também devem ser adotadas para o ambiente de Computação em Nuvem. Neste sentido, as abordagens tradicionais relativas a Segurança da Informação são regidas por certificações que tem como objetivo aprofundar o estudo das normas que regem cada um dos assuntos-foco relacionados. Tal premissa implica em considerar que o ambiente de Computação em Nuvem, além das normas de segurança tradicionais, deve ainda adotar medidas de segurança para o próprio ambiente em si (Chen, Paxson, and Katz 2010).

Para adequação dos padrões de Segurança da Informação no ambiente de Nuvem, ressaltamos a atuação da Instituição Cloud Security Alliance (CSA) (https://cloudsecurityalliance.org/) e do National Institute of Standards and Technology (NIST) (http://www.nist.gov).

A CSA é uma organização que tem por objetivo a promoção da utilização de melhores práticas para a prestação de garantia de segurança dentro do ambiente de Computação em Nuvem. O Conselho Internacional de Normalização (ISC) foi designado para coordenar os trabalhos em todos os aspectos de normalização na CSA. Os esforços são executados em conjunto pela CSA Global, que desenvolvem padrões para o provimento da segurança (Mell and Grance 2011).

O NIST é uma agência governamental não regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos, cuja uma das missões é promover a inovação e a competitividade industrial dos Estados Unidos através do estabelecimento de padrões tecnológicos. Uma das atribuições do NIST é o desenvolvimento de normas e orientações, incluindo os requisitos mínimos, para proporcionar a segurança da informação (Mell and Grance 2011).

Atualmente, diversas entidades trabalham no desenvolvimento de padrões de segurança específicos para Computação em Nuvem, levando essas pesquisas para um grande número de áreas, incluindo auditoria, aplicativos, criptografia, governança, segurança de rede, gerenciamento de risco, armazenamento e virtualização. Mesmo tendo sido estabelecido quem assumirá a responsabilidade pela custódia das informações, os proprietários destas continuam sendo as organizações contratantes. Há então, a necessidade de que os provedores provem que estão habilitados a manter os dados seguros, bem como disponibilizar meios para que a administração do ambiente computacional ofertado possa ser verificada, a qualquer momento, pelo contratante (Dhillon and Backhouse 2000).

A seguir, abordamos os principais pontos de vista dos autores pesquisados em relação as três questões de pesquisa elencadas no início deste artigo.

4.1 As vulnerabilidades no ambiente de Computação em Nuvem (CN)

Vulnerabilidades podem ser considerados erros relacionados com a segurança que provocam enfraquecimento ou a remoção de uma resistência ao ambiente. Invasores podem explorar vulnerabilidades, utilizando técnicas de acordo com sua capacidade. O ambiente de Computação em Nuvem possui vulnerabilidades intrínsecas a tecnologia que podem ser consideradas relevantes, como as listadas a seguir (Grobauer, Walloschek, and Stocker 2011):

i. A utilização de VPNs (*Virtual Private Network* - Rede Privada Virtual). Apesar do isolamento proporcionado pela virtualização, diversas questões ainda permanecem abertas a fim de compor uma lista de requisitos desejados aos sistemas de Computação em Nuvem;
ii. Uma criptografia segura por si só pode resolver uma série de problemas de segurança. Entretanto, a preocupação reside exatamente na utilização de uma criptografia ruim, passível de ser quebrada. O uso de uma criptografia obsoleta ou a não atualização desta, pode se tornar um grande risco;
iii. Problemas de seção no protocolo HTTP. Tecnologias de aplicação Web requerem o estado de sessão. Muitas técnicas implementam manipulação de sessão e, caso estas implementações sejam falhas, ela podem comprometer todo o ambiente.

Em relação a característica própria do ambiente de CN, algumas vulnerabilidades são decorrentes dos serviços que são disponibilizados (auto atendimento sob demanda, acesso a rede de qualquer plataforma de TI, partilha de recursos, elasticidade rápida e medição do serviço) (Grobauer, Walloschek, and Stocker 2011) :

i. O acesso não autorizado a interface de gerenciamento. O acesso não autorizado à interface de gestão é, portanto, uma vulnerabilidade especialmente relevante para os sistemas de nuvem: a probabilidade de que o acesso não autorizado pode ocorrer é muito maior do que para os sistemas tradicionais, onde a funcionalidade de gerenciamento é acessível apenas para alguns administradores;
ii. Vulnerabilidades no protocolo da Internet. A nuvem característica de acesso à rede onipresente significa que os serviços em nuvem são acessados via rede utilizando protocolos padrão. Na maioria dos casos, esta rede é a Internet, que deve ser considerada não confiável;
i. Vulnerabilidade de recuperação de dados. A característica da elasticidade na Nuvem implica em que os recursos alocados para um usuário serão realocados para um usuário diferente em um momento posterior. Para os recursos de memória ou de armazenamento, pode, portanto, ser possível recuperar os dados gravados por um usuário anterior;
ii. Medição e tarifação. A característica de medição na Nuvem significa que qualquer serviço de nuvem tem uma capacidade de medição em um nível de abstração apropriadas ao tipo de serviço (como a armazenagem, processamento, e contas de usuários ativos). Dados de medição são usados para otimizar a prestação de serviços, bem como de faturamento. Neste caso, as vulnerabilidades estão relacionadas a manipulação destes dados, onde os mesmos podem ser alterados e virem a não representarem mais a realidade.

Embora estejam em curso o desenvolvimento de técnicas e ferramentas tecnológicas que possam solucionar estas vulnerabilidades, percebe-se que os maiores problemas referem-se a falta de controle de gestão ou a má aplicação delas.

4.2 A verificação da prestação e da adequação dos serviços de TI em ambiente de Computação em Nuvem: A auditoria na gestão dos acordos de serviços

Um acordo de nível de serviço (Service Level Agreement -- SLA) é um contrato entre um fornecedor de serviços de TI e um cliente especificando, em geral e frequentemente em termos mensuráveis, quais serviços o fornecedor vai prestar. Níveis de serviço são definidos no início de qualquer relação de contratação de serviços de TI e são usados para mensurar e monitorar o desempenho de um fornecedor (Armbrust et al. 2009).

Em um ambiente de Computação em Nuvem, um dos desafios consiste no desenvolvimento de modelos de auditoria mútua para gestão dos acordos (SLAs), a fim de que possa ser estabelecida uma relação de confiança entre o contratante e o contratado, consolidando assim a utilização deste ambiente através de uma relação formal, envolvendo as responsabilidades legais pertinentes (Chen, Paxson, and Katz 2010).

Para estabelecer e controlar os requisitos contratuais adequados, torna-se necessário adotar tecnologias capazes de coletar os dados necessários para informar as decisões de risco, como o acesso de uso, controles de segurança, localização e outros referenciais relativos a utilização do serviço. Nesse processo, os prestadores de serviços de Nuvem e os próprios consumidores devem dispor de métricas e controles para auxiliar a gestão do uso da nuvem em cumprimento aos SLAs (Service Level Agreement - Acordo de Nível de Serviço) acordados entre as partes (Weinhardt et al. 2009).

Para proceder a verificação da conformidade do ambiente computacional, são realizadas auditorias. A auditoria foca sua atividade prioritariamente na avaliação dos processos de governança, gestão de riscos e controle e, de forma complementar, na avaliação das principais atividades, processos e produtos da organização, especialmente aqueles considerados vitais para atingir os objetivos estratégicos. Com esse foco, a auditoria visa proporcionar relativa segurança às partes interessadas. A auditoria de sistemas, portanto, envolve a avaliação dos sistemas de informação e dos recursos tecnológicos que englobam o processo de geração, guarda e disponibilização da informação. Neste sentido, a sua função é promover a adequação, revisão, avaliação e recomendações para o aprimoramento dos controles internos em qualquer um dos sistemas de informação da empresa, bem como avaliar a utilização dos recursos humanos, materiais e tecnológicos envolvidos no processamento destes (M Kanchana;Sk. Nazar Hussain;M. Kiran Kumar;C. Pr 2013).

Pelo fato dos auditores ainda não estarem familiarizados com a o nível de complexidade da Computação em Nuvem e sobre o que auditarem, é necessário levar em consideração os seguintes aspectos: (i) a aplicabilidade regulatória para uso da nuvem em questão; (ii) a divisão das responsabilidades entre o provedor do serviço e o cliente de nuvem acordado nos SLAs (Jensen et al. 2009). Neste sentido, torna-se relevante a busca de meios para viabilizar a auditoria mútua, completa e bilateral, adequando-os a cada nível de serviço contratado (Chen, Paxson, and Katz 2010).

4.3 Do processo de migração para o ambiente de Computação em Nuvem

Para que as empresas migrem sua estrutura de TI para o ambiente de Computação em Nuvem, devem ser considerados os benefícios, riscos e os efeitos nas organizações (Khajeh-Hosseini, Greenwood, and Sommerville 2010).

Com base em alguns estudos de caso , Khajeh-Hosseini, Greenwood, and Sommerville (2010) concluíram que a migração para a nuvem traz benefícios em relação ao desenvolvimento dos negócios da empresa e que em relação a gestão de projetos e gerenciamento de suporte, não houveram mudanças significativas. Entretanto, estes autores ressaltam que a maior fonte de riscos está relacionada a deterioração do atendimento ao cliente e qualidade de serviço prestado pelo provedor, além da dependência que se cria em relação a este.

Um outro fator a ser considerado em uma migração de ambiente está relacionado aos custos envolvidos na transferência dos dados, que devem ser levantados e planejados, pois a falta de previsão neste item pode ensejar esforços financeiros que se não disponíveis, podem colocar em risco todo o projeto de migração (Khajeh-Hosseini, Greenwood, and Sommerville 2010).

Outra consideração relevante é a perda de competências do pessoal de TI a nível interno da organização, o que pode resultar em dificuldades no caso se ter que trazer o sistema de volta, caso o provedor da Nuvem não prestar serviços inadequados ou o ambiente não atender as necessidades. Por isso, um fator essencial a ser considerado é a escolha do provedor (Khajeh-Hosseini, Greenwood, and Sommerville 2010).

No decorrer do processo de migração é importante que o provedor da Nuvem forneça os detalhes operacionais de como os dados do cliente será tratado, quais os requisitos de segurança se aplicam à infraestrutura da Nuvem e os planos de contingências previstos para o caso do sistema ficar comprometido (Mouratidis et al. 2013).

Os clientes não devem confiar cegamente nas alegações do provedor sobre a robustez e segurança de seu ambiente de Nuvem, devendo serem esclarecidos todos os detalhes das políticas adotadas referentes as tecnologias empregadas. O provedor deve ser investigado pela organização, sendo a ele solicitado todos os pontos importantes e relevantes a serem considerados no ambiente de Computação em Nuvem (Mouratidis et al. 2013).

Fator importante no processo de migração também é a realização de testes do ambiente do provedor. Antes de migrar o ambiente de TI, testes de consistência, de operacionalização e de segurança devem ser exaustivamente realizados para testar a confiabilidade do ambiente do provedor no processo de migração e regularmente para verificar se as aplicações críticas atendem aos requisitos de segurança. De preferência, estes testes devem ser realizados por empresas terceiras (Mansfield-Devine 2008).

5. Um “Modelo de Confiança” para a gestão da confiabilidade no uso do ambiente de Computação em Nuvem

O estabelecimento de um modelo contendo as premissas relacionadas com os princípios da Segurança da Informação, alinhado com os principais desafios apontados pelos

especialistas nesta área, poderá vir a ser útil como instrumento norteador de uma proposta de confiabilidade de utilização do ambiente de nuvem, caso este possa ser de fácil compreensão e reúna condições de ser adotado pelos provedores de serviços de TI em ambiente de Computação em Nuvem.

Um modelo de gestão orientando os processos necessários para adequação de tecnologias, bem como indicações de normas e certificações adequadas para segurança de cada modalidade de contrato, poderá se constituir em um instrumento que poderá permitir a verificação das condições diferenciadas na prestação de serviços em Computação em Nuvem. Tal modelo poderá conferir aos provedores de ambiente de TI e aos desenvolvedores de aplicações para Nuvem, a oportunidade de obterem uma qualificação melhor para determinação de um nível de confiança que conferem aos seus clientes usuários dos produtos de TI na Nuvem.

O referido modelo de gestão, denominado "modelo de confiança" é composto das áreas de interesse, conforme elencados na Figura 5.

A seguir, são descritos resumidamente os componentes que compõem cada uma das áreas de interesse do Modelo de Gestão operacional, denominado "Modelo de Confiança".

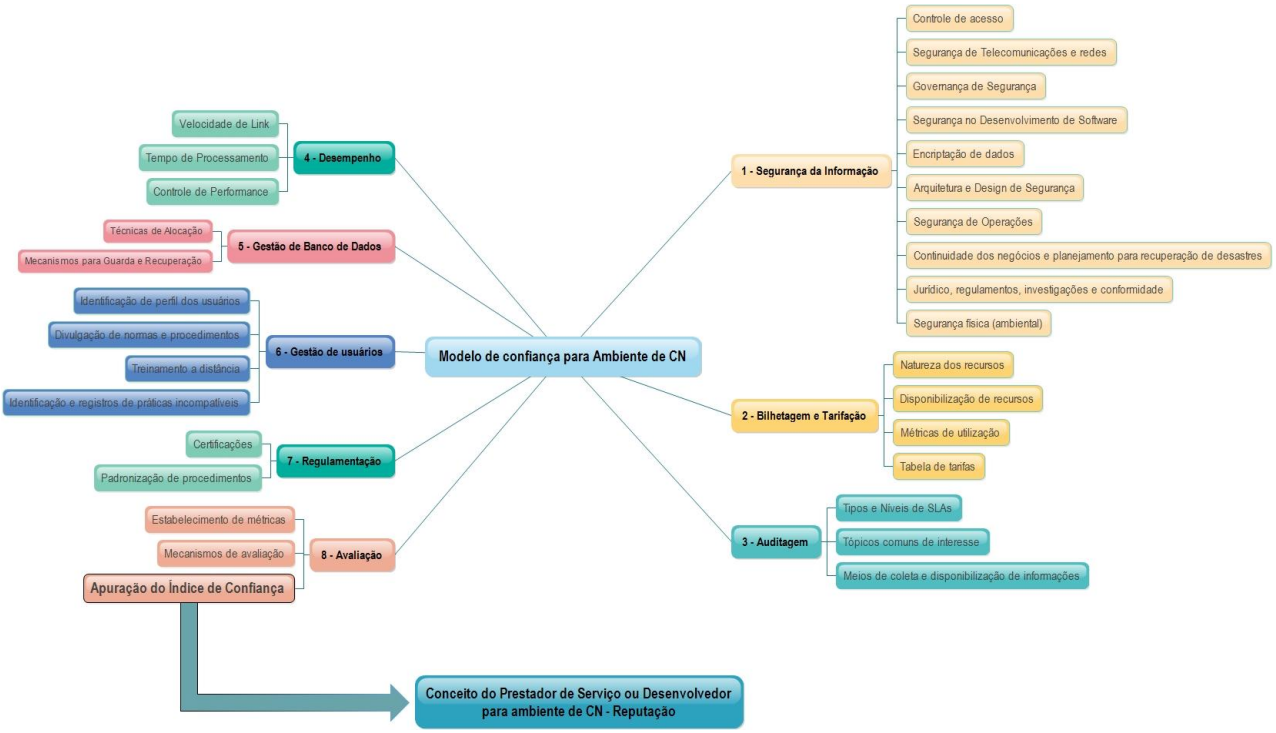

Figura 5 – Dimensões do "Modelo de Confiança" para Ambiente de Computação em Nuvem

5.1 Segurança da Informação (Confidencialidade, Integridade e Disponibilidade)

A Segurança da Informação trata dos princípios da confidencialidade, integridade e disponibilidade que os sistemas devem preservar. Os Sistemas de Informação no Ambiente de Computação em Nuvem seguem as mesmas normas e certificações independentemente do tipo e topologia das suas aplicações.

De acordo com a norma ISO/IEC 17.024, que versa sobre as abordagens na área de Segurança da Informação, há dez domínios a serem considerados em ambientes de TI a serem trabalhados que devem ser considerados em um modelo de gestão para o ambiente de Computação em Nuvem, conforme destacado na Figura 6.

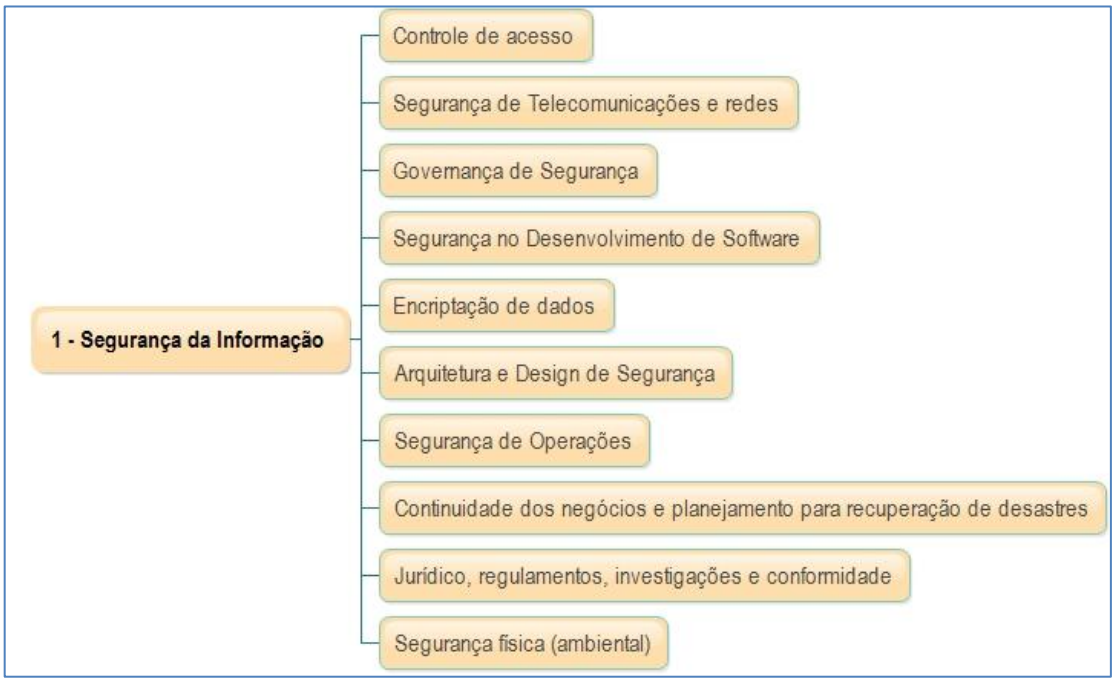

Figura 6 – Domínios do componente "Segurança da Informação"

i. Controle de acesso - Aborda sobre a tecnologia utilizada e a política de acesso ao ambiente de CN;
ii. Segurança de telecomunicações e redes - Descreve os padrões utilizados para a segurança da Infraestrutura do ambiente (IaaS), envolvendo tecnologias, equipamentos e configurações empregadas;
iii. Governança de Segurança da Informação - Envolve a definição dos planos de segurança, a forma de controle e de verificação dos procedimentos operacionais;
iv. Segurança no Desenvolvimento de Software - Detalha a metodologia de desenvolvimento das aplicações, camadas de desenvolvimento e regras de segurança a serem obedecidas pelos desenvolvedores;
v. Criptografia - Descreve as características referentes ao código em uso, versionamento e data de atualização;
vi. Arquitetura e Design de Segurança - Define a estrutura de aplicação da segurança distribuída pela tecnologia empregada;
vii. Segurança de Operações - Define os padrões e as ações a serem executados no ambiente operacional;
viii. Continuidade dos negócios e planejamento para recuperação de desastres - Contém o plano de contingenciamento das operações;
ix. Jurídico, regulamentos, investigações e conformidade - Embasamento jurídico relacionado a legislação em vigor, métodos de investigação e padrões de conformidade a serem seguidos;
x. Segurança física (ambiental) - Detalha os requisitos de segurança para o acesso as instalações do provedor e de seu parque tecnológico.

5.2 Bilhetagem e tarifação

Este componente aborda as modalidades e ferramentas da tarifação do serviço disponibilizado. Tais mecanismos de controle devem ser adequados para considerar a natureza dos recursos consumidos, a quantidade demandada destes recursos e o tempo de utilização. A bilhetagem deverá ser automática, bem como a solicitação de requisição destes recursos pelo usuário do ambiente. O ideal é que não haja intervenção humana neste processo. As formas de disponibilização desta tecnologia devem estar pautadas nos seguintes domínios, conforme representando na Figura 7:

Figura 7 – Domínios do componente "Bilhetagem e Tarifação"

i. Natureza dos recursos disponibilizados - Especifica como é controlado a disponibilização dos recursos tecnológicos utilizados pelos usuários-cliente em um espaço de tempo;
ii. Disponibilização dos recursos (quantidade) - Detalha as unidades empregadas na definição dos parâmetros quantitativos;
iii. Métricas de utilização - Especifica os cálculos utilizados para medição do consumo dos recursos;
iv. Tabela de tarifas - Compõe as regras adotadas para precificação.

5.3 Auditagem

Uma área fundamental no aspecto de segurança e verificação do cumprimento contratual acordado, refere-se a possibilidade de auditoria de TI mútua entre fornecedor e contratante. Na Computação em Nuvem, os provedores e usuários necessitam dispor de ferramentas de auditoria mútua, de forma transparente, para que o uso dos serviços possa ser atestado, estabelecendo assim a mútua confiança entre as partes (M Kanchana;Sk. Nazar Hussain;M. Kiran Kumar;C. Pr 2013).

A auditagem mútua deverá prover a capacidade ao usuário ou ao provedor de rastrear as ações executadas no ambiente, suas operações e intervenções em aplicações ou sistemas de informação. Um grande desafio é viabilizar estas ferramentas de controle sem que haja sem

perda de performance, pois o ambiente de Nuvem é provido por uma combinação de tecnologias complexas (Chen, Paxson, and Katz 2010).

Esta área de interesse é representada pelos seguintes domínios, representados na Figura 8:

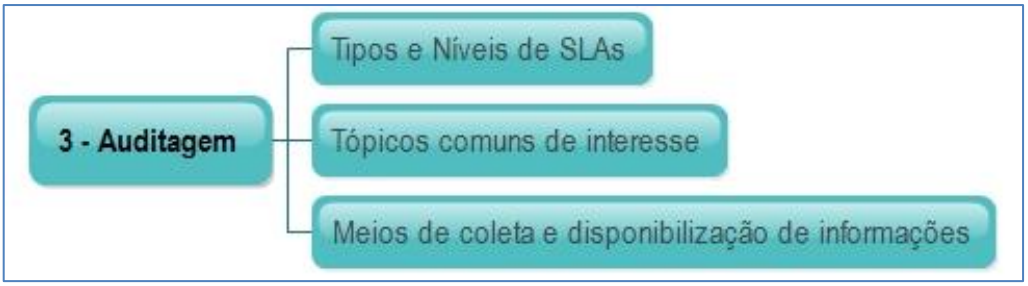

Figura 8 – Domínios do componente "Auditagem"

i. Tipos e Níveis de SLAs - Detalha os padrões de acordos estabelecidos para comercialização aos usuários;
ii. Tópicos comum de interesse - Define as operações de escopo e abrangência para realização de auditorias;
iii. Meios de coleta de disponibilização de informações - Define as fontes de coleta das informações para realização da auditagem.

Ressalta-se a possibilidade de integração através da adoção da auditagem de Computação em Nuvem com os modelos de gestão do serviço de Segurança (ScaaS), que bem estruturados, poderão vir a incrementar o próprio ambiente de segurança do cliente, em apoio aos planos de continuidade e de recuperação de desastres. Tais recursos permitirão também a detecção de riscos de confidencialidade dos dados com a provedora de Computação em Nuvem, proporcionando um compartilhamento destes riscos.

5.4 Desempenho

O desempenho da utilização do serviço é um dos principais fatores para aceitação da tecnologia pelos usuários. Uma vez que o acesso a Internet é requisito para o acesso ao ambiente de Nuvem, torna-se importante a implantação de tecnologias que possam registrar os seguintes domínios determinantes de medição do desempenho, conforme ilustrado na Figura 9:

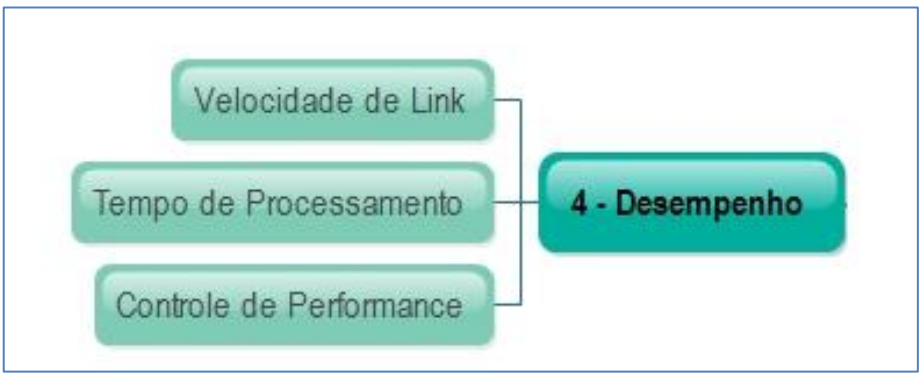

Figura 9 – Domínios do componente "Desempenho"

i. Velocidade do link - Requisitos de acesso ao ambiente, como velocidade mínima do link requerida e técnicas de medição empregadas para verificação;
ii. Tempo de processamento - Técnicas utilizadas para medição do desempenho do ambiente, como velocidade de processamento e tempo de resposta das aplicações;
iii. Controle de Performance - Equipamentos e softwares empregados para apuração.

5.5 Gestão do Banco de Dados

A implementação de técnicas de distribuição dos dados das aplicações de SI se constitui em importante preocupação dos especialistas quanto a integridade dos dados quanto a guarda e recuperação. O ambiente de Computação deve subsidiar todas as condições para que sejam atendidos os princípios inerentes a gestão dos Bancos de Dados, uma vez que eles constituem o bem mais precioso do usuário.

Neste sentido, são requeridos os seguintes domínios de estudo, conforme listados na Figura 10:

Figura 10 – Domínios do componente "Gestão de Banco de Dados"

i. Técnicas de alocação - Definição dos algoritmos e regras utilizadas para distribuição dos dados dos clientes nos Data Centers;
ii. Mecanismos para Guarda e Recuperação - Especifica a tecnologia e softwares utilizados para guarda dos dados, incluindo Backup, bem como a recuperação dos dados em consultas e outras operações relacionadas.

5.6 Gestão dos usuários

A importância da atuação das pessoas no âmbito da Segurança da Informação traz preocupação a esta área de estudo, a partir de comportamentos que podem ser considerados de risco para a manutenção da estabilidade dos sistemas de informação em ambientes de TI. Estando reconhecidamente como uma das preocupações na área da Segurança da Informação, ações que permitem a educação do usuário são importantes para que seja estabelecido um código de conduta entre o usuário e o provedor de serviços.

São os seguintes domínios tratados neste componente, conforme ilustrado na Figura 11:

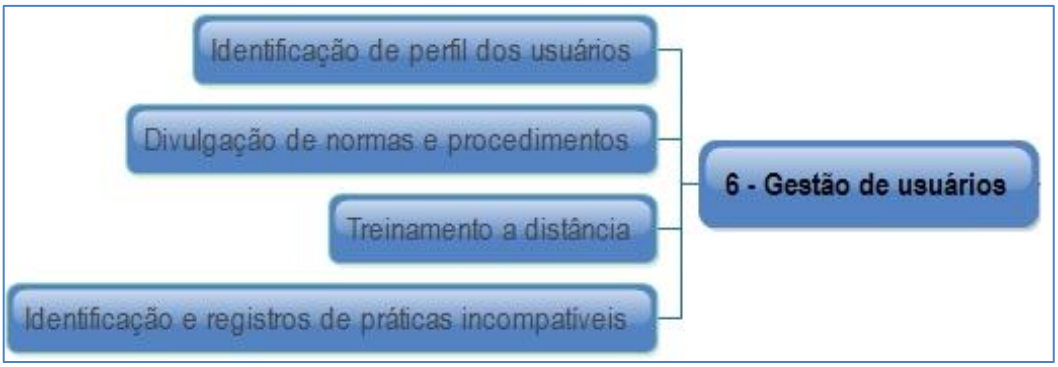

Figura 11 – Domínios do componente "Gestão de usuários"

i. Identificação do perfil dos usuários - Política e forma de registro no que tange a ações processadas no ambiente de CN;
ii. Divulgação de normas e procedimentos - Os meios utilizados para divulgação de normas e procedimentos operacionais a todos os usuários;
iii. Treinamento a distância - A disponibilização de treinamentos a distância utilizando o ambiente Web é um recurso importante na educação do usuário, devendo ser incentivado e estar disponível;
iv. Identificação e registros de práticas incompatíveis - Ferramentas que detectem ações não lícitas ou de risco provocado por pessoas devem permitir o registro destas ocorrências para tratamento específico. Ações de conduta discrepantes com o esperado devem ser detectadas e registradas em meios diferenciados.

5.7 Regulamentação

A regulamentação é importante para que haja uma padronização de procedimentos de cunho operacional e ético que tem como objetivo proteger a tecnologia e o serviço prestado por esta.

Não se justifica, por exemplo, que o estabelecimento de valores mais módicos para utilização do ambiente na Nuvem, exponha o usuário a ameaças de perda de invasão, exposição ou perda de seus dados. O serviço deve conter requisitos mínimos de segurança para que seja aceitável, dotando desta forma confiabilidade a tecnologia empregada.

São os principais domínios de estudo desta área, ilustrados na Figura 12:

Figura 12 – Domínios do componente "Regulamentação"

i. Certificações - Definição dos requisitos básicos de treinamento e as certificações necessárias a operacionalização do ambiente, definidas por tipo de usuário (Arquiteto de rede, desenvolvedor ou usuário final);
ii. Padronização de procedimentos - Envolve o código de ética a ser adotado na disponibilização, desenvolvimento de aplicações e uso do ambiente de CN.

5.8 Avaliação

A avaliação do modelo constitui passo importante para que as ações implementadas possam ser verificadas através de ferramentas tecnológicas que além de permitir a captação dos dados estatísticos relativos ao ambiente, possam estabelecer de forma facilitada à equipe de auditoria, dados de desempenho de cada uma das áreas de interesse do modelo da gestão operacional. Neste sentido, as áreas de domínio de estudo nesta área são assim definidas, como demonstrado na Figura 13:

Figura 13 – Domínios do componente "Avaliação"

i. Estabelecimento de métricas - Formulação e estabelecimento das métricas específicas relativas a aferição do uso do modelo de gestão do ambiente de CN;
ii. Mecanismos de avaliação - Estabelecimento dos mecanismos para apuração da aplicação do modelo e as formas de avaliação;
iii. Apuração do índice de confiança - Formulação de um "índice de confiança" que possa ser utilizado como referência para atribuir ao provedor de serviços de TI ou ao desenvolvedor de aplicações, uma "reputação" qualitativa dos serviços a que está habilitado a prestar.

6. Conclusões

Na busca de maior eficiência no controle dos recursos computacionais, bem como agilidade e redução de custos, a Computação em Nuvem pode proporcionar um melhor gerenciamento dos recursos de TI e da operacionalização dos Sistemas de Informação de maneira mais eficiente que a empregada tradicionalmente.

Torna-se, então oportuna a transição do ambiente operacional tradicional para o de Computação em Nuvem. Diante da evolução dos recursos computacionais e dos problemas decorrentes da dependência operacional cada vez maior da TI pelas organizações, novas tecnologias associadas a técnicas administrativas de gestão trazem uma abordagem mais

voltada para os resultados como eficiência operacional, competitividade e resposta rápida. Isso significa que a área de TI, em vez de produzir serviços de TI, passa a aperfeiçoar a produção e o consumo desses serviços de forma consistente sobretudo, com os requisitos de negócios.

Na revisão da literatura, verificou-se que embora diversos pesquisadores e empresas tratem de assuntos relacionados a problemática da segurança e fiabilidade no ambiente de Computação em Nuvem, diversas abordagens e estudos tornam-se necessários para tornar o ambiente tecnológico mais robusto.

A organização destes estudos, a divulgação deste ao mercado na forma de um modelo conceitual que possa estabelecer parâmetros para regulamentar uma relação de confiança entre provedor e usuário dos serviços de TI em ambiente de CN, constitui em um interessante instrumento no sentido de orientar provedores, desenvolvedores e utilizadores no sentido de disponibilizar serviços e aplicações seguras e confiáveis.

O estudo da revisão bibliográfica não se esgota neste estudo. Pelo contrário, a revisão bibliográfica relacionada ao tema deverá ser constantemente revista ao longo do processo de investigação, levando-se em conta o avanço da ciência e da tecnologia relativas a um tema vasto e inovador como o da Computação em Nuvem em constante evolução.

6.1 Benefícios esperados

Espera-se que o referido modelo de gestão operacional proposto propicie uma melhor gestão e melhor gerenciamento do ambiente de Computação em Nuvem, trazendo aos usuários, provedores e desenvolvedores os seguintes benefícios:

i. A possibilidade de verificação dos recursos disponibilizados pelo provedor de serviços, dada a natureza dinâmica dos ambientes regulatórios;
ii. A possibilidade de exercer o direito de auditar, particularmente quando se usa um provedor para um serviço no qual o cliente tenha que regulamentar o cumprimento das responsabilidades;
iii. Permitir a análise do escopo de conformidade, verificando se as regras de conformidade ao qual a organização está sujeita estão sendo impactados pelas práticas adotadas pelo provedor dos serviços de Computação em Nuvem para um dado conjunto de aplicações e dados;
iv. Permitir a análise sobre a segurança das aplicações e dos dados. Potenciais usuários finais dos serviços de Computação em Nuvem poderão ponderar quais aplicações e dados estão sendo considerados para serem movidos para serviços de Computação em Nuvem e em que medida eles estão sujeitos aos regulamentos de conformidade;
v. Avaliar a infraestrutura do provedor através de certificações que este possua em relação ao modelo regulatório. Alguns requisitos regulatórios especificam os controles que são possíveis ou difíceis de se atingir em certos tipos de serviços de nuvem;
vi. O atendimento ao escopo da norma ISO/IEC 27001/27002. As infraestruturas da Computação em Nuvem devem ser capazes de verificar se os dados estão sendo gerenciados de acordo com as regulamentações locais e internacionais aplicáveis, com controles apropriados, coleta de registros e emissão de relatórios;

vii. Subsidiar elementos para o desenvolvimento de um framework incorporando ferramentas e tecnologias para monitoramento do ambiente. Com a crescente necessidade de processamento e armazenamento de dados, torna-se cada vez mais desafiadora a gestão de datacenters, especialmente na nuvem (Kaufman 2009). Exigências como tempo de disponibilidade viram pré-requisitos cobrados por SLA, a fim de se assegurar o mínimo de qualidade dos serviços prestados;

viii. Ao propiciar confiabilidade, a Computação em Nuvem também poderá ser utilizada como uma forma de mitigar os riscos de continuidade do negócio de uma organização. Isso significa que a Computação em Nuvem poderá ser utilizada como meio para prevenir riscos de acidentes cataclísmicos e que envolvam a infraestrutura da organização em primeira instância, ou mesmo as instalações físicas, onde as perdas produtivas poderiam ser desastrosas.

6.2 Recomendações e trabalhos futuros

É recomendável a constante revisão do modelo de gestão proposto e a atualização tempestiva da revisão da literatura para atualização do conhecimento dos avanços tecnológicos da área de investigação em estudo. Torna-se necessário acompanhar e analisar as tecnologias que estão sendo desenvolvidas para viabilizar os controles necessário ao ambiente de Computação em Nuvem com vistas a dotá-lo de maiores recursos de confiabilidade para a operacionalização pelos usuários.

É também desejável o desenvolvimento e utilização de um *framework* para o monitoramento e gerenciamento das etapas do trabalho de investigação em curso para aprimoramento do modelo de gestão operacional proposto.

A montagem de um ambiente de CN para simulação e testes de avaliações das áreas de interesse elencadas no modelo de gestão referenciado neste artigo é essencial para avaliação das variáveis e diversas políticas previstas para a viabilização do modelo.

Um estudo complementar contemplando outros aspectos relacionados com a de viabilidade para montagem de um ambiente de estudos avançados em ambiente de Computação em Nuvem, com o aporte de recursos de ordem técnica e operacional, conjugada com fatores econômicos, de cronograma e outros, fornecerá um diagnóstico sobre a viabilidade do projeto de investigação em curso.

Referências

Armbrust, M et al. 2009. “Above the Clouds: A Berkeley View of Cloud Computing.” *University of California, Berkeley, Tech. Rep. UCB* : 07–013. http://scholar.google.com/scholar?q=intitle:Above+the+clouds:+A+Berkeley+view+of+cloud+computing#0.

Buyya, R. et al. 2009. “Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility.” *Future Generation computer systems* 25(6): 599–616. http://www.sciencedirect.com/science/article/pii/S0167739X08001957.

Buyya, Rajkumar, James Broberg, and Andrzej Goscinski. 2011. Cloud Computing: Principles and Paradigms *Cloud Computing: Principles and Paradigms*. John Wiley and Sons. http://books.google.pt/books?id=S1NvRRd77rQC&lpg=PT18&ots=HSi9o6Zo0g&dq=Cloud Computing: Principles and Paradigms&lr&hl=pt-BR&pg=PT23#v=onepage&q=Cloud Computing: Principles and Paradigms&f=false.

Che, Jianhua, Yamin Duan, Tao Zhang, and Jie Fan. 2011. "Study on the Security Models and Strategies of Cloud Computing." *Procedia Engineering* 23: 586–93. http://www.sciencedirect.com/science/article/pii/S187770581105394X (January 23, 2015).

Chen, Y, V Paxson, and RH Katz. 2010. … of California, Berkeley Report No. UCB/ … *What's New about Cloud Computing Security*. http://www.utdallas.edu/~muratk/courses/cloud13s_files/what-is-new-in-cloud-security.pdf (March 26, 2014).

Dhillon, Gurpreet, and James Backhouse. 2000. "Information System Security Management in the New Millennium." *Communications of the ACM* 43(7): 125–28.

Grobauer, Bernd, Tobias Walloschek, and Elmar Stocker. 2011. "Understanding Cloud Computing Vulnerabilities." *IEEE Security & Privacy Magazine* 9(2): 50–57. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5487489 (February 4, 2012).

Jensen, Meiko et al. 2009. Cloud: 2009 Ieee International Conference on Cloud Computing *On Technical Security Issues in Cloud Computing*. <Go to ISI>://WOS:000275314400015.

Kaufman, Lori M. 2009. "Data Security in the World of Cloud Computing." *Ieee Security & Privacy* 7: 61–64 ST – Data Security in the World of Cloud Co. <Go to ISI>://WOS:000268639100011.

Khajeh-Hosseini, Ali, David Greenwood, and Ian Sommerville. 2010. "Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS." In *2010 IEEE 3rd International Conference on Cloud Computing*, IEEE, 450–57. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5557962 (March 21, 2014).

Lenk, A et al. 2009. "What's inside the Cloud? An Architectural Map of the Cloud Landscape." *Software Engineering Challenges of Cloud Computing, 2009. CLOUD '09. ICSE Workshop on*: 23–31.

M Kanchana;Sk. Nazar Hussain;M. Kiran Kumar;C. Pr. 2013. "Preserving Audit of Secure Data Storage Services in Cloud Computing." *International Journal of Advanced Research in Computer Science* 4(5): 70–73. http://www.ijarcs.info/?wicket:interface=:3:::: (January 21, 2015).

Mansfield-Devine, Steve. 2008. "Danger in the Clouds." *Network Security* 2008(12): 9–11. http://www.sciencedirect.com/science/article/pii/S1353485808701405 (January 22, 2014).

Mell, Peter, and Timothy Grance. 2011. 145 National Institute of Standards and Technology, Information Technology Laboratory *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Mirashe, Shivaji P, and N V Kalyankar. 2010. "Cloud Computing" eds. Nick Antonopoulos and Lee Gillam. *Communications of the ACM* 51(7): 9. http://arxiv.org/abs/1003.4074.

Mouratidis, Haralambos, Shareeful Islam, Christos Kalloniatis, and Stefanos Gritzalis. 2013. "A Framework to Support Selection of Cloud Providers Based on Security and Privacy Requirements." *Journal of Systems and Software* 86(9): 2276–93. http://www.sciencedirect.com/science/article/pii/S0164121213000575 (December 25, 2014).

Webster, Jane; Watson, Richard. 2002. "Analyzing Teh Past to Prepare for the Future: Writing a Literature Review." *Management Information Systems Research Center, University of Minnesota*: 12. https://www.google.com.br/#q=writing+a+literature+review+webster+and+watson+2002 (January 23, 2015).

Weinhardt, Christof et al. 2009. "Cloud Computing – A Classification, Business Models, and Research Directions." *Business & Information Systems Engineering* 1(5): 391–99. http://www.springerlink.com/index/10.1007/s12599-009-0071-2 (July 5, 2011).