ISSN: 2447-5580

COMPUTAÇÃO EM NUVEM: A SEGURANÇA DA INFORMAÇÃO EM AMBIENTES NA NUVEM E EM REDES FÍSICAS

CLOUD COMPUTING: INFORMATION SECURITY IN CLOUD ENVIRONMENTS AND PHYSICAL NETWORKS

Adan Lucio Pereira[1], Elton Wagner Machado da Penha[2], Nazur Amorim Gomes[3], Rodrigo Randow de Freitas[4]

1 Graduado em Engenharia de Computação. UFES, 2013. Centro Universitário Norte do Espírito Santo - CEUNES. São Mateus, ES. *E-mail:* adanlucio@gmail.com

2 Bacharel em Ciência da Computação. Faculdade Pitágoras, 2010. Unidade Teixeira de Freitas, BA – Brasil. *E-mail:* ewmachado@gmail.com

3 Graduando em Engenharia de Computação. UFES. Centro Universitário Norte do Espírito Santo - CEUNES. São Mateus, ES. *E-mail:* nazuragomes@hotmail.com

4 Doutor em Aquicultura, FURG, 2011. Centro Universitário Norte do Espírito Santo - CEUNES. São Mateus, ES. *E-mail:* rodrigo.r.freitas@ufes.br

Recebido em: 09-03-2016 - Aprovado em: 19-05-2016 - Disponibilizado em: 15-07-2016

RESUMO: O Artigo aborda o tema Cloud Computing, ou seja, Computação em Nuvem, cujo objetivo principal deste estudo é a Segurança da Informação em Ambientes na Nuvem em comparação às Redes Físicas. O modelo de computação analisado pode ser definido como um conjunto de recursos computacionais disponibilizados na rede que consiste na abstração da infraestrutura de Hardware e também na virtualização de software. As implementações de novas tecnologias e avanço da infraestrutura de rede trazem à tona muitos pontos a serem discutidos. De acordo com a literatura, à medida que os dados alocados na nuvem, muitas dúvidas entram em questão. Até que ponto as informações estão mais vulneráveis na Cloud que nas redes físicas? Até que ponto as corporações podem confiar em migrar dados para a nuvem? Quais dados poderão ser migrados? Quais pontos devem ser considerados antes de fazer a migração? Independentemente das questões levantadas concluímos que é importante que os critérios de acessos sejam estabelecidos e que as garantias do cumprimento dos princípios de segurança sejam respeitadas. Fato que os sistemas em nuvem estão crescendo consideravelmente a medida que as tecnologias se desenvolvem e com isso surgem novos desafios.
PALAVRAS-CHAVE: Tecnologia da informação, Computação em nuvem, segurança

ABSTRACT: The article talks about Cloud Computing, ie, Computação em Nuvem, which theme focuses on Information Security in Cloud Environments compared to Physical Networks. The analysis of this computing model can be defined as a set of computational resources available on the network that is the abstraction of the hardware infrastructure and also in the virtualization software. The implementation of new technologies and advancement of network infrastructure bring up many points to be discussed. According to the literature, as many important data are allocated in the cloud, many doubts come into question. To what extent the information is more vulnerable in the Cloud that the physical networks? The extent to which corporations can trust migrate data to the cloud? What data can be migrated? What points should be considered before making the migration? Regardless of the issues raised, we conclude that it is important that the access criteria are established and that the guarantees of compliance with the safety principles are respected. Fact that cloud systems are considerably growing as technologies develop and thus new challenges come up with.
KEYWORDS: Information technology, Cloud computing, Security

PEREIRA, A.L; PENHA, E.W.M; GOMES, N.A & FREITAS, R.R. (2016). Computação em nuvem: a segurança da informação em ambientes na nuvem e em redes físicas. **Brazilian Journal of Production Engineering** (BJPE). 2 (1): 12-27. ISSN : 2447-5580.

1 INTRODUÇÃO

O aumento do volume de informações e o surgimento de novos tipos de dados provocou a necessidade do desenvolvimento de novas tecnologias com maior capacidade de processamento, maior capacidade de armazenamento, menor custo e menores dimensões físicas. Com a expansão e aperfeiçoamentos dessas tecnologias durante o tempo, esses sistemas computacionais passaram a fazer parte da vida das pessoas e das empresas mudando significativamente a forma de se trabalhar e se comunicar (PEREIRA e APPEL, 2013).

Como consequência desse desenvolvimento tecnológico contínuo, nasceu o termo denominado Tecnologia da Informação e Comunicação (TIC), definida que pode ser definida como o conjunto de técnicas e recursos tecnológicos que, em conjunto, desempenham atividades na indústria, comércio, setor de investimentos e na educação (ANDRADE, 2006).

Nesse novo ambiente, as organizações têm buscado um uso cada vez mais intenso e amplo da Tecnologia de Informação, vista como uma ferramenta diretamente ligada a estratégia competitiva e à sobrevivência das organizações. Assim, o aprimoramento de *hardwares* e *softwares* garante a operacionalização da comunicação e dos processos decorrentes em meios virtuais. É importante ressaltar que a popularização da *internet* teve grande influência na potencialização do uso das TICs em diversos campos (ALBERTIN, A. e ALBERTIN, R., 2008).

Inserindo-se nesse contexto, as organizações enxergaram o potencial da *internet* e então novos sistemas de comunicação e informação foram criados, formando uma verdadeira rede de comunicação em massa. Novas tecnologias como *Active Server Pages* (ASP), *Java Server Pages (*JSP), *Personal Home PageTools* (PHP) e *Servlets* facilitaram a criação de *Websites* mais dinâmicos e de *e-commerce*. Consequentemente, em 2004, com o surgimento das redes de relacionamento e com o compartilhamento de informações onde a interatividade se tornava o ingrediente principal, iniciava-se a *Web 2.0* (CARMONA e HEXSEL, 2005; ALMANN *et al*., 2009).

A *Web 2.0* unificou todas as ferramentas já existentes para mudar a forma como se era utilizada usa a *Web*. A ideia principal consistia em fazer com que os usuários da grande rede interagissem diretamente com a tecnologia ajudando a melhorá-la e fazendo com que gradualmente ela satisfaça às expectativas do usuário (ARGOLLO *et. al.,* 2010*).*

Assim, a *web* passou a ser vista como uma plataforma provedora de serviços e sistemas. Como exemplos, existem softwares e ferramentas disponibilizadas na *Web* em que não há necessidade de uma instalação da ferramenta no computador. Vale ressaltar que não é uma nova tecnologia, mas sim um modelo que reutiliza as tecnologias já existentes para dar um novo foco à *Web* mudando a sua forma de utilização e o comportamento do usuário, como aconteceu com as redes de relacionamentos (CALHEIROS, 2009).

Essa constante evolução, trouxe consigo novas áreas de pesquisa e novas tecnologias, como a Computação em nuvens por exemplo. O conceito da computação em nuvens começou a ser discutido com o desenvolvimento virtualização e dos sistemas distribuídos. Entretanto, o conceito de Computação em Nuvem gera grande confusão, já que este não se trata de uma nova tecnologia, mas sim da evolução natural e convergência de várias tecnologias e conceitos. Entre eles o *Utility Computing* (comercializar sistemas computacionais como serviços), o *Grid Computing*, o *Web 2.0*, o *Services Oriented Architecture* (SOA) e o

modelo de *software* como serviço (*Software as a Services*) (LOPES, 2011; SOUSA *et al.,* 2009; TAURION, 2009; ZHANG *et al.*, 2010; HASHEM *et al.*, 2015).

Entretanto, com a convergência de diversos conceitos em um único, a computação em nuvens traz inúmeros desafios quanto à segurança dos dados incorporados a esses sistemas. As informações trafegadas nas redes, principalmente corporativas, possuem algum tipo de valor e devem ser resguardadas, exigindo assim um nível de segurança eficiente nos sistemas que gerenciam a rede. Essas informações podem ser alvos de diversos problemas de infraestrutura física ou de ataques virtuais. De modo geral, a segurança de recursos de informação possui três componentes primordiais (COLOURIUS, 2007):

1- **Integridade de dados** - que significa proteger contra alteração indevida ou danos;
2- **Confidencialidade** - que significa proteger os dados contra a exposição a pessoas não autorizadas;
3- **Disponibilidade** - que significa proteger os dados contra a interferência com os meios de acesso aos recursos.

Inserindo-se neste contexto, fica evidente que a proteção desses dados é uma necessidade primordial, para que os recursos computacionais sejam utilizados de forma segura, protegendo as empresas e indivíduos que necessitam do auxílio computacional para a realização de suas atividades.

2 VIRTUALIZAÇÃO E SISTEMAS DISTRIBUÍDOS

A virtualização de um sistema de *hardware* consiste em rodar vários sistemas operacionais na mesma máquina. Isso é possível com o uso de aplicações muito específicas, que geram máquinas virtuais (*Virtual Machines*, ou *VMs).* As Maquinas virtuais emulam os componentes físicos de um PC, possibilitando que um sistema operacional diferente seja instalado em cada uma delas, em um único *hardware* (FOROUZAN, 2008; LI *et al*., 2015).

O processo de virtualização pode ser usado, por exemplo, para reduzir a dependência da máquina física no modelo cliente-servidor. A ideia principal desse ambiente virtualizado é armazenar em um servidor remoto e central todos os dados e aplicações necessárias ao usuário. Dessa forma, cada usuário pode acessar esses dados de qualquer terminal na rede como se os dados estivessem armazenados naquele computador e todos os processos e programas também são executados nesse servidor central (TIGRE e NORONHA, 2013; DA SILVA *et al.*, 2014).

Duas das principais características presentes nas máquinas virtuais, flexibilidade e portabilidade, também tornam interessante o uso da virtualização em *desktops.* Essas aplicações possibilitam o desenvolvimento de produtos de *software* destinados a vários sistemas operacionais, sem a obrigação do uso de uma plataforma física para desenvolver e testar cada um deles. Dessa forma, as máquinas virtuais em *desktops* podem ser utilizadas para finalidades experimentais sem qualquer comprometimento do sistema operacional atual, ou então, para compor plataformas distribuídas como *clusters* e grades computacionais (KUSIC *et al.,* 2008; NGUYEN VAN *et al.*, 2009).

É possível apontar a segmentação ou particionamento, agrupamento, aglomeração ou associação de recursos computacionais, simulação/emulação, isolamento, substituição ou inclusão, hibridismo, como as correntes técnicas de virtualização atuais (PEIXOTO, 2012).

Uma coleção de computadores independentes que se apresenta ao usuário como um sistema único e consistente é chamado de Sistema Distribuído. Porém, há uma necessidade de se manter tudo conectado onde a ideia principal é o compartilhamento de informações (TANENBAUM e WETHERALL, 2011).

Em paralelo, os sistemas distribuídos trabalham com trocas de mensagens na rede, onde há um servidor e um cliente. O cliente requisita uma operação através de um programa (processo) em qualquer computador da rede e o servidor recebe a requisição e o responde apropriadamente, aplicada as devidas restrições na rede. Para os usuários o maior benefício é o compartilhamento das informações como Bancos de Dados ou arquivos e documentos que precisam estar disponíveis a vários usuários da rede (TORRES, 2014).

3 COMPUTAÇÃO EM NUVEM

O termo Computação em nuvem pode ser definido como um conjunto de uma grande rede de servidores interligados, sejam eles virtuais ou físicos, ou ainda pode ser definido como sendo um conjunto de recursos computacionais disponibilizados na internet como um serviço (SOUSA *et al,* 2009). Empresas como a *Amazon, VMware, Microsoft e Google* já dispõe de serviços de computação em nuvem comumente utilizados, como o *Gmail* e o *Youtube*, além também do *Google docs,* que permite a edição de arquivos de texto, elaboração de slides e planilhas eletrônicas, permitindo assim a elaboração de documentos que podem ser acessados em qualquer lugar do mundo e a qualquer hora (TAURION, 2009).

Nas aplicações de sistemas de computação em nuvens, são implementados os avanços das tecnologias e da infraestrutura de rede com o intuito de prover diversos recursos computacionais ao cliente, (*hardwares*, plataformas de desenvolvimento e *softwares)* como serviços que são acessados através da internet e utilizam um modelo de tarifação denominado de *pay-per-use*, ou seja, o valor cobrado corresponde ao tempo e/ou recurso do serviço utilizado. Os clientes não necessitam de máquinas de grande desempenho para obter os resultados das aplicações, como ocorreria se a aplicação fosse executada localmente. Consequentemente, a finalidade da máquina utilizada pelo cliente passa a ser somente para a entrada dos dados e para a exibição dos resultados após as aplicações remotas (SINGH *et al., 2008;* VERNEKAR e GAME, 2012; TORRES, 2014; HASHEM *et al.,* 2015).

Os serviços implantados nesses sistemas são armazenados e processados em um ou mais servidores de *data centers*, acessados remotamente. Como esses serviços passam a ser executados nas máquinas dos *data centers*, a tarefa de manutenção do serviço é deslocada dos clientes, que estão pagando por esse serviço, para os gestores dos *data centers*, agora denominados provedores de serviços (PEIXOTO, 2012; ROSS e KUROSE, 2013). A Figura 1 apresenta um sistema em nuvens.

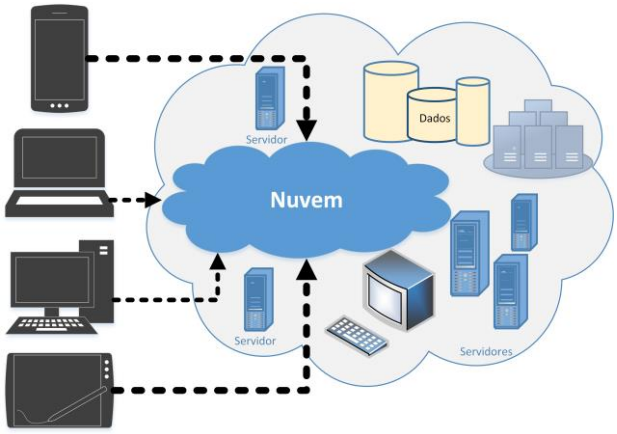

Figura 1 - Representação geral da computação em nuvem. (Figura elaborada pelos autores)

A arquitetura de um sistema em nuvens é baseada em duas camadas, a *front-end* e a *back-end*. A Camada *front-end* funciona como uma interface para o usuário final acessar os serviços, possibilitando a entrada de dados e posteriormente a conexão com a segunda camada, a *back-end*. Assim, a principal função da camada *back-end* consiste em processar os serviços provenientes da camada de interface (AMARANTE, 2013). Após a realização das tarefas na nuvem, o resultado é enviado para o *front-end*. Existe, ainda, uma interface de gerenciamento, que serve para controlar o acesso aos recursos disponíveis na nuvem, de modo que um cliente não cause interferência na requisição de

outro cliente e/ou acesso indevido de informações privadas (TORRES, 2014; BOTTA *et al.,* 2016).

Como exemplo tem-se as aplicações *Onedrive* (2016) e o *Dropbox* (2016). A camada *front-end* dessas aplicações pode ser acessada através do navegador de *internet*, onde são mostrados todos os arquivos do cliente. O *back-end* trata do armazenamento desses arquivos em algum servidor e o processamento de requisições solicitadas pela camada *front-end*. A Figura 2 indica essas duas camadas inseridas no processo de acesso as nuvens.

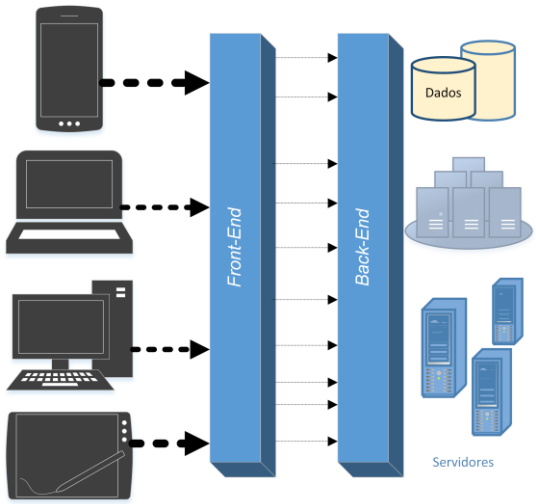

Figura 2 - Arquitetura de um sistema de computação em nuvem (Figura elaborada pelos autores)

3.1 SERVIÇOS NA COMPUTAÇÃO EM NUVEM

Os modelos baseados na implementação em nuvem são classificados de acordo com os recursos fornecidos ao usuário e como eles serão utilizados. Estes modelos são classificados como *Software-as-a-Service* (SaaS), *Infrastructure-as-a-Service* (IaaS), *Database-as-a-Service* (DaaS) e *Plataform-as-a-Service* (PaaS) (PEIXOTO, 2012; AMARANTE, 2013).

No modelo *Software* como Serviço (SaaS), ocorre o nível mais alto de abstração, ou seja, os usuários acessam o serviço (aplicação) através da internet, geralmente por navegadores de internet, não sabendo onde realmente o aplicativo está sendo executado. Como exemplo de um sistema SaaS pode-se citar o *Google Docs,* um pacote de aplicativos do Google que funciona totalmente *on-line* diretamente no browser (ESPADAS *et al.,* 2013; HAN *et al.,* 2015).

A Figura 3 apresenta um modelo SaaS, em que, um provedor de serviços fornece um aplicativo ou um pedaço de *software* para conjunto de máquinas.

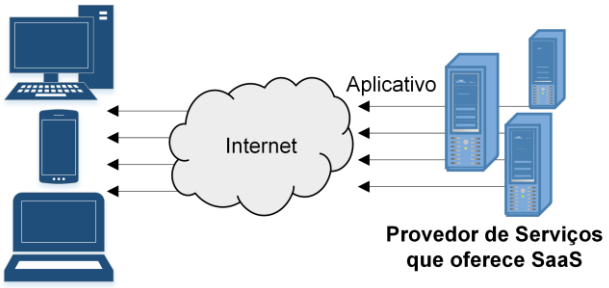

Figura 3 - Representação de um Serviço SaaS. (Figura elaborada pelos autores)

Já no modelo *Hardware* como um Serviço (IaaS), os recursos de *hardware* (capacidade de processamento, armazenamento e comunicação de dados) são disponibilizados como serviço para o cliente. Para isso, o fornecimento desses recursos é usualmente feito em termos de máquinas virtuais. Quem disponibiliza essas aplicações recebe o nome de provedor de IaaS (BIJON *et al.,* 2015). A *Amazon Web Services* (AWS) é um exemplo de plataforma que utiliza esse modelo. A Figura 4 apresenta um modelo IaaS.

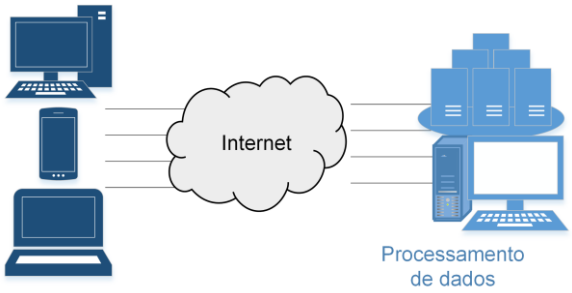

Figura 4 - Representação de um Serviço SaaS. (Figura elaborada pelos autores)

Quando o recurso se trata do gerenciamento de banco de dados o modelo que se torna prestador desse serviço é o *DaaS*. Vale ressaltar que cada Banco de Dado adicional colocado em operação aumenta o custo

final do serviço, uma vez que, o aumento da quantidade de bancos é diretamente proporcional ao aumento das atividades de Gestão, segurança, integração, desempenho e disponibilidade (SEIBOLD e KEMPER, 2012; HUSSEIN e KHALID, 2016). A Figura 5 apresenta um modelo DaaS.

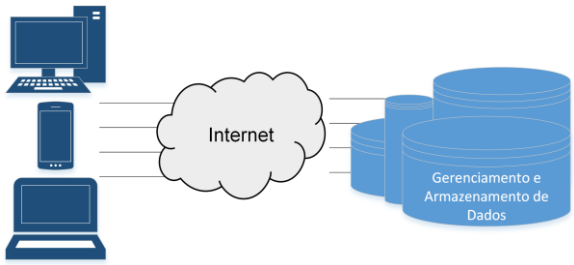

Figura 5 - Representação de um Serviço DaaS.
(Figura elaborada pelos autores)

Por fim, o quarto modelo, Plataforma como Serviço (PaaS), apresenta uma plataforma de desenvolvimento para os clientes finais. Nesse ambiente, o desenvolvedor não necessita se preocupar com o *hardware* sobre o qual está desenvolvendo e executando suas aplicações, terceirizando os serviços de desempenho necessários para rodar tais aplicações (LECHETA, 2015; CHARD *et al., 2016*). A Figura 6 apresenta um modelo PaaS, em que, um provedor de serviços permite que os clientes acessem uma plataforma computacional rodando sobre um sistema em nuvens.

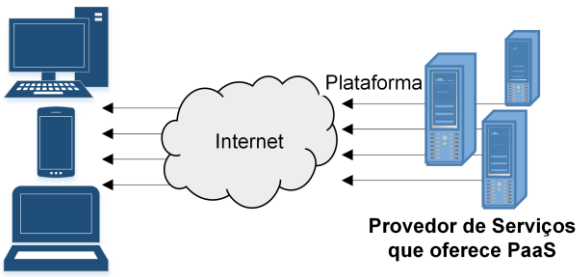

Figura 6 - Representação de um Serviço PaaS.
(Figura elaborada pelos autores)

O modelo IaaS é a base de todos os serviços de nuvem. Assim, o PaaS é construído com base na estrutura do IaaS e o SaaS construído com base no PaaS. Geralmente o SaaS é implementado em conjunto com o DaaS. Verifica-se que assim como as capacidades são herdadas, também são herdadas as questões de segurança da informação e risco (BIJON *et al.,* 2015). Um diagrama de referência, em forma de pilha, dos sistemas em nuvem, elaborado pela entidade *Cloud Security Alliance* (2010) é apresentado na Figura 7 e determina a relação entre esses modelos citados.

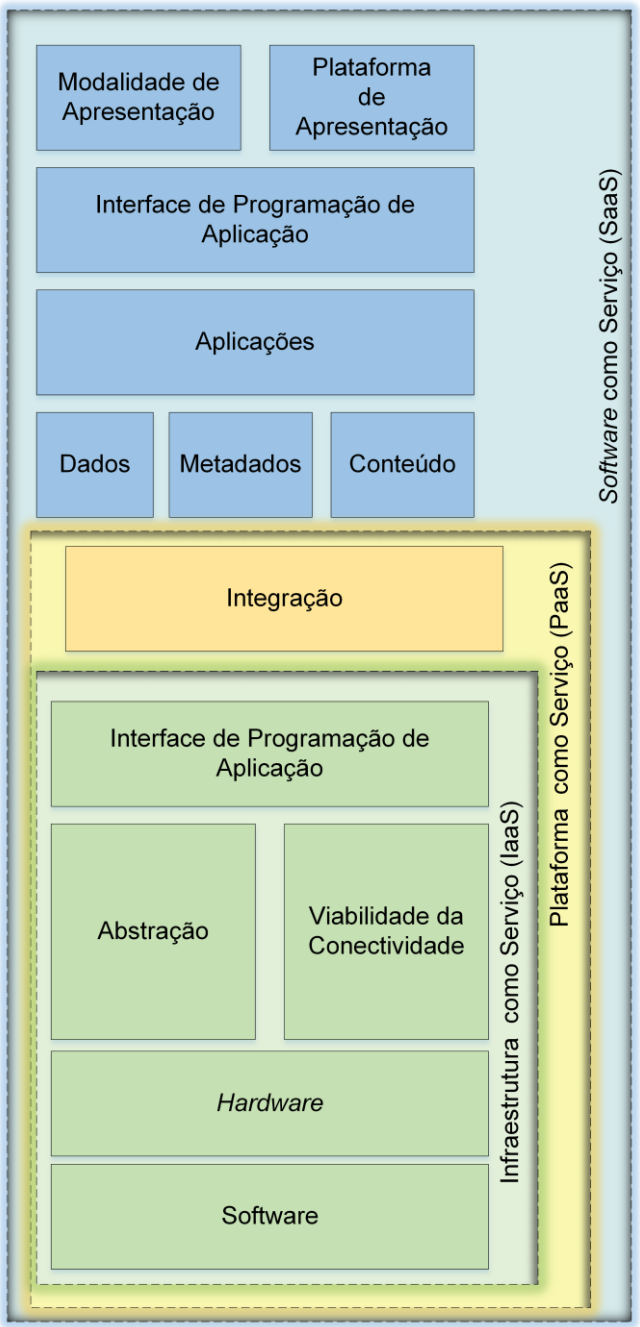

Figura 7 - Modelos de Sistemas em Nuvem
Fonte: Adaptado de (CSA, 2010)

É possível observar na Figura 7 que o modelo IaaS corresponde a todos os recursos da pilha de infraestrutura desde as instalações até as plataformas de *hardware* em conjunto com as aplicações do com o DaaS, dados, metadados e conteúdo. Essa camada, mais superior, inclui a capacidade de um sistema em abstrair (ou não) os recursos, bem como oferecer conectividade física e lógica às aplicações dos clientes. O serviço fornece ainda, uma Interface de Programação e Aplicação, do Inglês *Applications Programming Interface* - APIs, que permite a gestão e outras formas de interação com a infraestrutura por parte dos usuários (BIJON *et al.,* 2015).

Em seguida está a segunda camada da pilha, Plataforma como Serviço, que corresponde a integração dos sistemas com *frameworks* de desenvolvimento de aplicativos; recursos para mediação entre *software* e demais aplicações; funções para utilização de banco de dados; mensagens e filas. Tal modelo permite que o desenvolvedor crie aplicações para a plataforma cujas linguagens de programação e ferramentas são suportadas pela pilha (LECHETA, 2015).

Como terceira camada da pilha, o serviço SaaS por sua vez, representa a pilha mais externa do conjunto de modelos em nuvens. Essa camada fornece um ambiente operacional destinado ao cliente, com recursos do usuário, incluindo o conteúdo, a sua apresentação, as aplicações e as capacidades de gestão e gerenciamento das informações armazenadas no sistema (HAN *et al.,* 2015).

3.2 CRITÉRIOS DE ACESSO À NUVEM

Além do modo como são implantados, os sistemas em nuvens precisam ser classificados quanto aos critérios de acesso à nuvem. Para isso as nuvens podem ser classificadas como pública, privada, híbrida e comunitária (PEIXOTO, 2012).

Na nuvem pública, do inglês *Public Cloud*, os serviços estão disponíveis a todos os clientes finais, de acordo com o modelo *pay-per-use*. Esses serviços geralmente são oferecidos por companhias que possuem grande quantidade de recursos e juntas compartilham os serviços prestados, em troca de economia na implementação final. Para esse modelo, não podem ser aplicadas restrições de acesso quanto ao gerenciamento de redes ou, ainda, técnicas de autenticação e autorização. Consequentemente, as nuvens públicas possuem limites de customização relacionados justamente à segurança das informações e políticas de acesso aos dados armazenados em locais desconhecidos (VÁSQUEZ-RAMÍREZ *et al.,* 2016).

Outro modelo comumente utilizado é a nuvem privada, do inglês *Private Cloud*. Este modelo geralmente é implementado dentro do ambiente organizacional e faz o uso de tecnologias de autenticação e autorização para permitir o acesso ao gerenciamento das redes e as configurações dos provedores de serviços (CASTRO e SOUZA, 2011).

Para unificar os benefícios do modelo de nuvem pública com a privada, o conceito de nuvem híbrida, do inglês *Hybrid Cloud*, nasce para definir uma abordagem híbrida de dois ou mais modelos de nuvem. A Combinação desses conceitos pode aperfeiçoar a escalabilidade sob demanda. Além disso, este modelo é interessante pois quando uma Nuvem privada tem uma carga de trabalho alta, ela temporariamente compartilha o uso de recursos públicos para garantir o desempenho (AMARANTE, 2013).

Por fim, a infraestrutura de uma nuvem comunitária, do inglês *Community Cloud*, é destinada para o uso exclusivo de uma comunidade específica de clientes com objetivos semelhantes, podendo ser controlada, gerenciada e operada por uma ou mais organizações pertencentes a esse agrupamento de indivíduos (PEIXOTO, 2012).

4 SEGURANÇA DA INFORMAÇÃO EM AMBIENTES DE COMPUTAÇÃO EM NUVENS

O desenvolvimento e implementação de aplicações em nuvens trouxe consigo a necessidade do desenvolvimento de técnicas para o tratamento seguro da maciça quantidade de recursos provenientes dos serviços prestados pelos provedores, tais como, *e-mails*, desenvolvimento de aplicativos personalizados para os clientes, armazenamento de dados e gestão de infraestrutura (TAURION, 2009).

A definição de que a nuvem consiste em um conjunto de informações providas de um ou mais clientes, pode caracterizá-la como sendo um alvo propício a ataques por potenciais invasores. Essas ameaças podem afetar diretamente as exigências da segurança da informação (disponibilidade, confidencialidade e integridade), e consequentemente comprometer toda a nuvem (DIAS *et al.,* 2012).

A garantia do cumprimento dos princípios de segurança está diretamente ligada com o modelo de implantação contratado pelo cliente do sistema em nuvem. O modelo de nuvem privada por exemplo, permite a restrição de acessos uma vez que se encontra atrás do *Firewall* do cliente local, mantendo, dessa forma, controle do nível de serviço e aderência às regras de segurança do cliente final, e não do sistema contratado (CASTRO e SOUZA, 2011).

Como este ambiente ainda está em processo de amadurecimento muitas organizações ainda têm receio sobre sua segurança. Tais especulações podem ser comprovadas com os resultados da pesquisa realizada pela revista *InformationWeek* em 2013, 2014 e 2015, que buscou saber dos profissionais de segurança e tecnologia da informação, quais são as preocupações sobre os sistemas baseados em computação em nuvem (DAVIS, 2014; COBB, 2015). A Figura 8 indica as principais respostas dessa pesquisa.

É possível notar, ao observar a Figura 8, que a maioria dos especialistas que responderam as pesquisas teme os riscos associados ao acesso não autorizado ou vazamento de informações, correspondendo a cerca 50% no ano de 2013, um aumento de 1% em 2014, e um decréscimo de 3% no ano de 2015. O segundo fator que mais preocupa os pesquisadores é a preocupação com os próprios defeitos de segurança dessa tecnologia com 49% em 2013, redução de 1% em 2014, chegando em 2015 com 43%.

Outro fator que merece destaque é que 7 das 8 respostas indicadas apresentam um percentual menor de risco no ano de 2015 quando observado em relação ao ano de 2013. Tal evolução pode estar diretamente ligada com o amplo desenvolvimento e atenção que os sistemas baseados em nuvens receberam nos últimos anos.

Assim, todo serviço oferecido em rede deve atender aos princípios que garantam a disponibilidade, integridade e confidencialidade de dados. Os riscos devem ser avaliados antes da implantação da nuvem e quem migrar para este sistema deve ficar atento as devidas orientações ao usar o produto final (KANDUKURI *et al.,* 2009).

É de suma importância que seja identificado e avaliado os ativos suportados pela nuvem antes de da efetiva migração para o sistema. Ao realizar a migração é necessário se atentar para os riscos ao manipular dados ou funções para a nuvem, e a organização deve estar precavida para as piores eventualidades, como a destruição ou má administração dos ativos (DAWOUD *et al.,* 2010).

Os controles de segurança na nuvem não diferem dos controles de segurança de qualquer ambiente de T.I. No entanto, a computação em nuvem envolve uma lenta perda de controle uma vez que os quesitos de segurança podem ficar a cargo do provedor. À medida que a organização vai amadurecendo, o sistema de segurança também é ajustado (CSA, 2010).

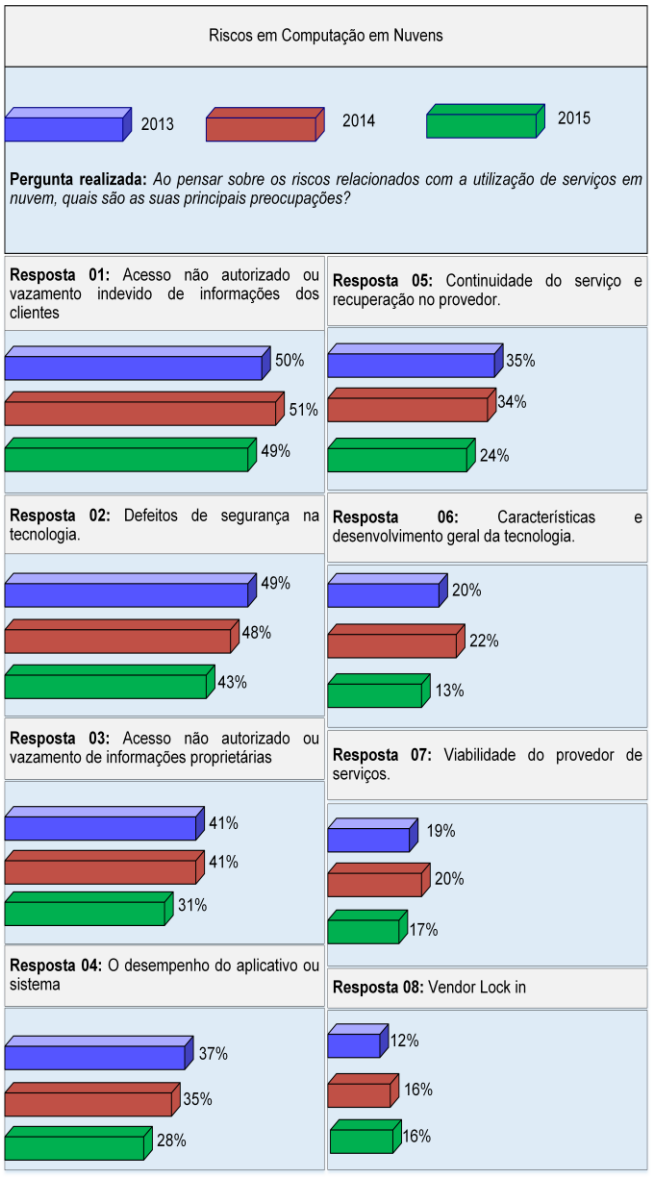

Figura 8 - Riscos em Computação em Nuvens. Fonte - Baseando em Davis (2014) e Cobb (2015)

Como a computação em nuvem tem a intenção de reduzir custos para as empresas, ela procura oferecer serviços flexíveis para atender a um determinado cliente e com isso a segurança fica mais comprometida, pois a responsabilidade dos riscos passa a ser maior para o consumidor. Esses requisitos podem ser observados quando é efetuada a escolha sobre qual modelo será implementado na nuvem. Por exemplo, no SaaS, nível mais alto indicado na pilha (Figura 7), o consumidor contrata a segurança, enquanto no IaaS, o consumidor implementa a segurança (TAURION, 2009; CASTRO e SOUZA, 2011; AMARANTE, 2013; TORRES, 2014).

4.1 Áreas de atenção crítica

Os riscos na área de Tecnologia da Informação estão presentes na nuvem e com isso padrões e estratégias podem ser traçadas para evitar ou combater esses problemas sob dois pontos de vista: dos Domínios de Governança ou sob os Domínios Operacionais (CSA, 2010).

Os Domínios de Governança estão classificados na literatura como (MUSSON, 2009; CSA; GUO e SONG; MIRASHE e KALYANKAR, 2010; ISACA, 2011; VAN GREMBERGEN, 2013; OROZCO *et al*., 2015):

- **Governança e Gestão de Riscos Corporativos -** Uma das áreas de foco mais críticas da governança de tecnologia da informação na computação em nuvem. Alguns riscos inerentes à computação em nuvem devem ser considerados em um processo decisório que visa à adoção desse novo paradigma. Corresponde, ainda, a capacidade de uma organização para governar e medir o risco empresarial introduzido pela computação em nuvem. Itens como a precedência legal em caso de violação de acordo, a capacidade de organizações usuárias para avaliar adequadamente o risco de um provedor de nuvem, a responsabilidade para proteger dados sensíveis quando o usuário e o provedor podem falhar e, como as fronteiras internacionais podem afetar estas questões, são alguns dos itens discutidos;
- **Aspectos Legais e *Electronic Discovery* -** Este domínio compreende aos problemas legais em potencial quando se utiliza computação em nuvem:requisitos de proteção da informação e de sistemas informáticos, leis de divulgação de violações de segurança, os requisitos regulatórios, requisitos de privacidade, as leis internacionais, entre outros;

- **Gestão do Ciclo de Vida da Informação -** Este domínio inclui o gerenciamento de dados que são colocados na nuvem, itens em torno da identificação e controle de dados, bem como controles compensatórios que podem ser usados para lidar com a perda de controle físico ao mover um dado;
- **Portabilidade e Interoperabilidade -** Este domínio compreende a habilidade de mover dados/serviços de um provedor para outro, sem problemas de identificação e/ou acesso aos mesmos.

Já os Domínios Operacionais estão classificados na literatura como (MUSSON, 2009; CSA, 2010; ISACA, 2011; VAN GREMBERGEN, 2013; OROZCO *et al*., 2015):

- **Segurança Tradicional, Continuidade de negócios e Recuperação de desastres -** Domínio capaz de determinar como a computação em nuvem afeta os processos e procedimentos operacionais atualmente usados para programar a segurança, continuidade de negócios e recuperação de desastres. O foco nesse domínio é discutir e analisar os possíveis riscos da computação em nuvem, na esperança de aumentar o diálogo e debate sobre a grande procura de melhores modelos de gestão de riscos corporativos;
- **Operação do Data-center -** Domínio que avalia a arquitetura e a operação de um fornecedor de *datacenter*;
- **Resposta a incidentes, notificação e correção -** A correta e adequada detecção de incidentes, a resposta, notificação e correção. Nesse sentido, para domínio, se faz necessário identificar os itens e/ou recursos que devem estar presentes tanto no nível dos prestadores e dos usuários para permitir bom tratamento de incidentes e forenses computacionais;
- **Segurança de Aplicação -** Domínio criado para proteger o *software* ou aplicação que está sendo executada ou sendo desenvolvida na nuvem. Isto inclui itens tais como, a necessidade de migrar ou projetar um aplicativo para ser executado na nuvem, e em caso afirmativo, selecionar a plataforma em nuvem mais adequada (SaaS, PaaS ou IaaS);
- **Gestão de criptografia e de chaves -** Domínio para identificar o uso de criptografia e gestão das chaves de acesso. Esse domínio permite analisar quais são as questões que surgem na utilização, tanto para proteger o acesso aos recursos, bem como para proteger os dados;
- **Virtualização -** Dada a inviabilidade de hospedar cada serviço/aplicação em um servidor dedicado, ocasionado tanto pelo custo de manutenção e subutilização da infraestrutura, como pela necessidade de atender a característica de elasticidade oferecida pelo paradigma de computação nas nuvens, foi adotado um modelo baseado na tecnologia de virtualização. Assim, este domínio foca nas questões da segurança em torno do sistema / *hardware* de virtualização.

Segundo Castro e Souza (2011), os sistemas em nuvens, independente do domínio de análise envolvido, devem apresentar um modelo de gestão de risco que realize:

1) Identificação e a avaliação dos ativos relacionados à implementação dos sistemas em nuvens;
2) Descrição das ameaças e vulnerabilidades do impacto potencial nos ativos (risco e cenários de incidente) para cada tecnologia implantada;
3) Determinação das possíveis ocorrências inesperadas quanto à implantação da nuvem;
4) Desenvolvimento e implementação de Planos de Tratamentos de Riscos com múltiplas opções (controle, evitar, transferir, aceitar), determinando as medidas que devem ser tomadas em situações de contingência.

5 PRINCIPAIS AMEAÇAS E ATAQUES EM REDES DE COMPUTADORES

O conceito de Rede de computadores pode ser definido como um grupo de computadores que estão conectados entre si e que possuem o objetivo de compartilhar informações e hardware através de um meio de transmissão em comum. Uma rede é composta de no mínimo, dois computadores. Adicionalmente, essas redes são ligadas por um sistema de comunicação que se constitui de um arranjo topológico interligando vários módulos através de enlaces físicos, que são os meios de transmissão, e de um conjunto de regras a fim de organizar a comunicação, que são os protocolos (FOROUZAN, 2008; TANENBAUM e WETHERALL, 2011).

Nas redes de computadores, a segurança da informação é fundamental para manter as informações íntegras e confidenciais. As redes não podem ser simplesmente classificadas como seguras ou não seguras porque o termo não é absoluto quando o assunto são as ameaças nas redes de computadores (COMER, 2007).

As ameaças podem ser acidentais, quando não há intenção humana de violação, ou intencionais quando ocorre uma ação maliciosa por parte do usuário. Algumas ameaças não resultam em perdas de informação (passivas) e outras alteram as informações do sistema (ativa) de forma intencional por meio de Personificação, *Replays*, Modificação, Cavalos de Troia, dentre outras (ROSS e KUROSE, 2013).

O trabalho realizado por Davis (2014) e replicado por Cobb (2015) apresenta uma pesquisa com 1029 profissionais de segurança e tecnologia do negócio em março de 2013, 536 em abril de 2014 e 435 em abril de 2015 relacionando os maiores desafios desses profissionais com a segurança de redes e informações. Após analisar o trabalho de Cobb e Davis as seguintes indicações representam os maiores desafios de segurança de TI:

- Gerenciamento do sistema de segurança das redes;
- Aplicação de políticas de segurança;
- Avaliação de riscos presentes nos sistemas de computação;
- Obtendo do preço adequado para os sistemas;
- Prevenção contra a violação de dados de invasores externos;
- Conscientização do usuário quanto à utilização do sistema;
- Controle de acesso do usuário aos sistemas e dados;
- Regulamentação e padronização dos requisitos do sistema;
- Obtenção de recursos e experiência profissional;
- Impedir o roubo de dados.

Adicionalmente, o trabalho realizado por Cobb (2015), permite constatar que 58% dos especialistas em Tecnologia da informação consideram o uso de dispositivos infectados na rede da corporação como uma situação preocupante, seguido por 49% com a preocupação dos usuários sendo vítimas de *phishing* ou outros *scams* (são fraudes na *Internet* que visa adquirir credenciais de um usuário por engano), e por último com a perda de dispositivos que portam informações sigilosas.

Alguns setores estarão sempre mais vulneráveis que os outros. As organizações do Governo, por exemplo, são as que menos quantificaram as perdas resultantes das falhas de segurança. As indústrias apontam seus próprios funcionários como um dos principais responsáveis e o setor de comércio sofre com vazamento de dados e acessos remotos indevidos (DAVIS, 2014; COBB, 2015).

Contudo, pode se aplicar alguns mecanismos para reverter essa realidade. É possível, por exemplo, proteger uma rede de computador através de Criptografias, Controle de Acesso, Integridade de

Dados, Segurança Física e Pessoal, e por fim contar com um *Hardware/Software* de segurança.

6 Discussão

Ao estudar a literatura inerente à segurança em computação em nuvens, em comparação com as estruturas de rede tradicionais, é possível perceber que são muito semelhantes. O que irá diferir será a responsabilidade da segurança da informação que será passada para o provedor.

Nas redes físicas existe um controle total da informação por parte do prestador que a implementa, exigindo a adoção de políticas de segurança e uso de técnicas e ferramentas tradicionais na rede física. Na nuvem quem realiza o controle total da informação é o provedor ou há uma divisão das responsabilidades, onde o provedor e o contratante se responsabilizam pela segurança da informação. Assim, provedor também utiliza de políticas de segurança dentro de seu datacenter, a diferença é que essas políticas são aplicadas pelo provedor e não pelo cliente. No entanto, o contratante deve manter as boas práticas de segurança dentro de sua organização.

Também, nas redes físicas, existe o risco de um funcionário violar a informação. Esse risco também está presente nos sistemas em nuvens, com o agravante de que não se conhece quem administra os dados. Já o risco de ataques externos, tanto na nuvem quanto nas redes físicas são os mesmos.

Ainda considerando o setor de Tecnologia da Informação, nas redes físicas, ele pode não receber a devida atenção pelo fato de não ser o foco da organização e isso implica vulnerabilidade. Já os provedores de nuvem trabalham exclusivamente com isso e possui todo aparato necessário para administrar a segurança dos dados do cliente. Entretanto, já existem nas redes físicas políticas de segurança consolidadas, apesar da rede nunca estar totalmente segura. Fato diferente observado na nuvem, onde as políticas de segurança devem sofrer adaptações e há muito a se construir em cima do novo modelo.

Assim, a gestão de riscos, nas redes físicas é realizada pela organização em sua rede local e na nuvem devem-se estabelecer requisitos contratuais adequadas e adotar as tecnologias capazes de coletar os dados necessários para informar as decisões de informação de risco. Por exemplo, (uso da informação, acesso, controles de segurança, localização, dentre outros). Sendo que em redes físicas, as organizações não têm a Tecnologia da Informação como foco principal, isso implica em vulnerabilidade. Contudo, a computação em nuvem oferece, entre seus principais atrativos, uma redução de custos com infraestrutura e com mão de obra qualificada.

De maneira geral, assim como nas redes físicas, o processo de implementação, instalação e configuração do ambiente de nuvem deve seguir boas práticas de segurança, sendo que após essa fase o ambiente deve ser monitorado visando detectar mudanças ou atividades não autorizadas pelo cliente final.

7 Considerações Finais

O aumento do uso de sistemas distribuídos, em especial o modelo de computação em nuvens, tem motivado constantemente, pesquisas, trabalhos experimentais, desenvolvimento de novas tecnologias e metodologias de implantação de segurança em comunicação de dados de modo geral.

À medida que essas tecnologias vão se desenvolvendo os sistemas em nuvens vão se tornando uma necessidade cada vez maior. E com isso surgem novos desafios. Assim, o presente trabalho mostrou que esse novo paradigma de representação da comunicação e dados está cada vez mais inserido nas grandes empresas e nos dispositivos pessoais das pessoas.

Os sistemas em nuvens possuem potencial para reduzir as barreiras que a tecnologia da informação, impõe à inovação, o que pode ser visivelmente

observado quanto ao surgimento rápido de empresas de alta representatividade que utilizam essa tecnologia como *YouTube* e o *Facebook.*

Ao adotar o sistema em nuvens, os clientes finais podem aumentar ou reduzir o nível de utilização dos recursos computacionais de modo fácil e com flexibilidade, sem a necessidade da constante manutenção do sistema físico. E, ao tratar os possíveis riscos associados a esse sistema, a computação em nuvem torna possível novas classes de aplicações e disponibiliza serviços que antes não era possível com a utilização dos sistemas físicos e fixos provenientes da tecnologia da informação tradicional.

Além de tratar os riscos provenientes do modelo tradicional, esses novos sistemas devem garantir a segurança de uma nova infraestrutura. Apesar da necessidade do alto investimento na proteção dos dados, seja em ambientes físicos ou na nuvem, é imprescindível investir em consciência humana, pois são as pessoas que irão conduzir essas informações.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBERTIN, A. L.; ALBERTIN, R. M. M. *Benefícios do uso de tecnologia de informação para o desempenho empresarial.* Rev. Adm. Pública, vol.42, n.2, pp. 275-302, 2008.

ALMANN, A. L. *et al. Planeta web 2.0: inteligencia colectiva o medios fast food*. Rev. Caderno de Pesquisa vol.39, n.137, pp. 688-693, 2009.

AMARANTE, S. R. M. *Utilizando o Problema de Múltiplas Mochilas para Modelar o Problema de Alocação de Máquinas Virtuais em Computação nas Nuvens*. 2013. 82f. Dissertação (Mestrado em Ciência da Computação), Universidade Federal do Ceará, 2013.

ANDRADE, S. C. *Processo de inclusão digital em rede empresarial do segmento de Suprimentos industriais: utilização de tecnologias de informação e comunicação*. Ci. Inf., vol.35, no.1, pp.7-15, 2006, ISSN 0100-1965.

ARGOLLO, R. V. *et al.: Web 2.0 como estruturante dos processos de produção e difusão científica em um grupo de pesquisa: o TWIKI e o GEC*. Perspect. ciência inf., Belo Horizonte, v. 15, n. 1, p. 118-131, 2010, ISSN 0100-1574.

BIJON, K.; KRISHNAN, R.; SANDHU, R. Virtual resource orchestration constraints in cloud infrastructure as a service. In: *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy.* ACM, p. 183-194, 2015.

BOTTA, A.; DE DONATO, W.; PERSICO, V.; PESCAPÉ, A. Integration of cloud computing and internet of things: a survey. *Future Generation Computer Systems*, 56, 684-700, 2016.

CALHEIROS, D. S. Utilização das tecnologias da informação e comunicação, no contexto da web 2.0, na prática docente na educação superior. 2009. 167f. Dissertação (Mestrado em Educação). Universidade Federal de Alagoas. 2009

CARMONA, T.; HEXSEL, R. A. *Universidade Redes:* Torne-se um especialista em redes de computador. São Paulo: Digerati Books, 2005.

CASTRO, R. C. C.; SOUSA, V. L. P. *Segurança em Cloud Computing: Governança e Gerenciamento de Riscos de Segurança.* In: III Congresso Tecnológico de TI e Telecom InfoBrasil 2010, Anais Eletrônicos; Fortaleza, CE, 2011. Disponível em < http://www.infobrasil.inf.br/userfiles/26-05-S5-1-68740-Seguranca%20em%20Cloud.pdf> Acesso em janeiro de 2016.

CHARD, K *et al.* Globus Nexus: A Platform-as-a-Service provider of research identity, profile, and group management. *Future Generation Computer Systems*, 56, 571-583, 2016

COBB, M. *How Enterprises Are Attacking the IT Security Challenge*. Revista InformationWeek:

Connecting the Business Technology Community. 2015. Disponível em < https://pages.cloudpassage.com/rs/857-FXQ-213/images/how-enterprises-are-attacking-the-it-security-challenge.pdf> Acesso em Jan. 2016.

COLOURIUS, G. *Sistemas Distribuídos*: Conceitos e Projetos. 1a Ed. Cidade: Bookman, 2007.

COMER, D. E. *Redes de Computadores e Internet*. 4a ed. Porto Alegre: Bookman, 2007.

CSA (Cloud Security Alliance) - Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 *Prepared by the Cloud Security Alliance December* 2009.

DA SILVA, *et. al*. A Privacy Maturity Model for Cloud Storage Services. In: *2014 IEEE International Conference on Cloud Computing* (IEEE CLOUD), June 27 - July 2, 2014, Alaska, USA.

DAVIS, M. A. *Research: 2012 Strategic Security Survey.* Revista InformationWeek: Connecting the Business Technology Community. 2014. Disponível em < http://reports.informationweek.com/abstract/21/8815/security/research-2012-strategic-security-survey.html> Acesso em Jan. 2016.

DAWOUD, W.; POTSDAM, G.; TAKOUNA, I.; MEINEL, C. Infrastructure as a service security: Challenges and solutions. In: *7th International Conference on Informatics and Systems* (INFOS), 2010.

DIAS, J. M. F.; RODRIGUES, R; C. M. C.; PIRES, D. F. *A Segurança de Dados na Computação em Nuvens nas Pequenas e Médias Empresas.* Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica. Vol. 02, pg 56- 59, 2012

DROPBOX. *Dropbox*, Acesso em Janeiro 2016. Disponível em: <https://www.dropbox.com/>.

ESPADAS, J. *et al.* A tenant-based resource allocation model for scaling Software-as-a-Service applications over cloud computing infrastructures. *Future Generation Computer Systems*, 29(1), 273-286, 2013.

FOROUZAN, B. *A. Comunicação de Dados e Redes de Computadores*. Editora McGraw Hill, 4° Ed., p. 1168, 2008.

GUO, Z., SONG, M. A governance model for cloud computing. Management and Service Science (MASS). 2010 *International Conference on,* IEEE, p.1-6, August, 2010.

HAN, J.; CHUNG, K.; KIM, G. Policy on literature content based on software as service. *Multimedia Tools and Applications*, v. 74, n. 20, p. 9087-9096, 2015.

HASHEM, *et. al*. The rise of “big data” on cloud computing: Review and open research issues. *Information Systems*, v. 47, p. 98-115, 2015.

HUSSEIN, N. H.; KHALID, A. A survey of Cloud Computing Security challenges and solutions*. International Journal of Computer Science and Information Security*, v. 14, n. 1, p. 52, 2016.

ISACA. *IT control objectives for cloud computing: controls and assurance in the cloud*. Rolling Meadows: ISACA, 2011.

KANDUKURI, B. R.; RAMAKRISHNA, P.; RAKSHIT, A. Cloud Security Issues. *IEEE International Conference On Services Computing*, Pune, India, n., p.517-520, September 2009.

KUSIC, D.; KEPHART, J. O.; HANSON, J. E.; KANDASAMY, N.; JIANG, G. Power and performance management of virtualized computing environments via lookahead control. In: *Proceedings of the 2008 International Conference on Autonomic Computing, ICAC ’08*, Washington, DC, USA: IEEE Computer Society, 2008, p. 3–12 (ICAC ’08). Disponível em http://dx.doi.org/10.1109/ICAC.2008.31

LECHETA, R. R. *Web Services RESTful*: Aprenda a criar web services RESTful em Java na nuvem do Google. São Paulo: Novatec Editora, 432p, 2015

LI, W., ZHAO, Y., LU, S., E CHEN, D. Mechanisms and challenges on mobility-augmented service provisioning for mobile cloud computing. *Communications Magazine, IEEE*, v. 53, n. 3, p. 89-97, 2015.

LOPES, S. *Aspectos arquiteturais na adoção de cloud computing*. MundoJ, Curitiba, v. 8, n. 47, p. 20-23, maio 2011.

MIRASHE, S. P., KALYANKAR, N.V. Cloud computing. *Journal of Computing***,** v. 2, n. 3, p.78-82, March, 2010.

MUSSON, D. IT Governance: a critical review of the literature, *Information technology governance and service management*: frameworks and adaptations. Hershey, PA: IGI, 2009.

NGUYEN VAN, H.; DANG TRAN, F.; MENAUD, J.-M. Autonomic virtual resource management for service hosting platforms. In: *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*, CLOUD '09, Washington, DC, USA: IEEE Computer Society, 2009, p. 1–8 (CLOUD '09). Disponível em http://dx.doi.org/10.1109/CLOUD.2009.5071526

ONEDRIVE. *Onedrive*, Acesso em Janeiro 2016. Disponível em: <https://onedrive.live.com/>.

OROZCO, J.; TARHINI, A.; E TARHINI, T. A framework of IS/business alignment management practices to improve the design of IT Governance architectures. *International Journal of Business and Management*, *10*(4), 1, 2015.

PANCHOLI, V. R.; PATEL, B. P. Enhancement of Cloud Computing Security with Secure Data Storage using AES. *International Journal for Innovative Research in Science and Technology*, v. 2, n. 9, p. 18-21, 2016.

PEIXOTO, M. L. M. *Oferecimento de QoS para computação em nuvens por meio de metaescalonamento*. 2012. 179f. Tese (Doutorado em Ciências de Computação), Instituto de Ciências Matemática e de Computação, Universidade de São Paulo, 2012.

PEREIRA, A.L.; Appel, A.P.: Modeling and storing complex network with graph-tree. In: *New Trends in Databases and Information Systems*, Workshop Proceedings of the 16th East European Conference, ADBIS 2012, Pozna, Poland, September 17-21, pp. 305–315, (2013), DOI:10.1007/978-3-642-32518-2_29.

ROSS, K. W.; KUROSE, J. *Redes de Computadores e A Internet* - Uma abordagem *Top-Down*. São Paulo: Person Addison Wesley - 6ª Ed., 2013.

SEIBOLD, M.; KEMPER, A. *Database as a Service*. Datenbank-Spektrum, v. 12, n. 1, p. 59-62, 2012.

SINGH, A.; KORUPOLU, M.; MOHAPATRA, D. Server-storage virtualization: integration and load balancing in data centers. In: *Proceedings of the 2008 ACM/IEEE conference on Supercomputing*, SC '08, Piscataway, NJ, USA: IEEE Press, 2008, p. 53:1–53:12 (SC '08). Disponível em http://dl.acm.org/citation.cfm?id=1413370.1413424

SOUSA, F. R. C.; MOREIRA, L. O.; MACHADO, J. C. *Computação em nuvem*: conceitos, tecnologias, aplicações e desafios. Anais da II Escola Regional de Computação Ceará, Maranhão e Piauí (ERCEMAPI). 2009. Cap. 7, p. 150-175.

TANENBAUM, A. S.; J. WETHERALL, D. *Redes de computadores.* Rio de Janeiro: Editora Pearson Education - Br, 5. Ed. 620p, 2011.

TAURION, C. *Cloud computing*: computação em nuvem transformando o mundo da tecnologia da informação. São Paulo: Brasport, 2009. 228 p.

TIGRE, P. B.; NORONHA, V. B. *Do mainframe à nuvem*: inovações, estrutura industrial e modelos de negócios nas tecnologias da informação e da comunicação. Rev. Adm. (São Paulo), Mar 2013, vol.48, no.1, p.114-127, 2013.

TORRES, G. *Redes de Computadores*. Editora: Novaterra, 2° Ed, p. 1040, 2014

VAN GREMBERGEN, W. Introduction to the Minitrack" IT Governance and its Mechanisms"-HICSS 2013. In: *System Sciences* (HICSS), 2013 46th Hawaii International Conference on. IEEE, p. 4394-4394, 2013.

VÁSQUEZ-RAMÍREZ, *et. al*. An Open Cloud-Based Platform for Multi-device Educational Software Generation. In: *Trends and Applications in Software Engineering*. Springer International Publishing, p. 249-258, 2016.

VERNEKAR, S.; GAME, P. Component based resource allocation in cloud computing. In: *Proceedings of the International Conference on Information Systems Design and Intelligent Applications 2012* (INDIA 2012) held in Visakhapatnam, India, p. 907–914, Springer, 2012.

ZHANG, Q.; CHENG, L.; BOUTABA, R. Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications*, London, v. 1, p. 7-18, May 2010. Disponível em: <http://it341.blog.com/files/2012/12/Cloud-computing-state-of-the-art-and-research-challenges.pdf>. Acesso em jan. 2016.