

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DIRETORIA DE PESQUISA E PÓS GRADUAÇÃO
ESPECIALIZAÇÃO EM GESTÃO DE SERVIÇOS DE TELECOMUNICAÇÕES

JOÃO MATHEUS AMPESSAN SCHIAVO

CLOUD COMPUTING: UMA QUESTÃO DE SEGURANÇA

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA

2015

JOÃO MATHEUS AMPESSAN SCHIAVO

CLOUD COMPUTING: UMA QUESTÃO DE SEGURANÇA

Monografia apresentada ao Programa de Pós-Graduação em Gestão de Serviços de Telecomunicações da Universidade Tecnológica Federal do Paraná - *Campus* Curitiba.

Orientador: Prof.*MSc.* Alexandre Miziara

CURITIBA

2015

Dedico esta monografia aos meus pais Moacir e Solange, que sempre me ajudaram na concretização de meus objetivos, pelo amor, carinho e, por todos os ensinamentos ao longo da vida e pelo apoio recebido durante a minha especialização.

AGRADECIMENTOS

Agradeço a Deus por ter me dado à oportunidade de estar no mundo.

Aos meus pais, Moacir João Schiavo e Solange Terezinha Ampessan Schiavo, e à minha família, agradeço todo o amor, carinho, compreensão e respeito.

Agradeço também ao meu orientador Prof.MSc. Alexandre Miziara pela dedicação na orientação e ajuda na elaboração deste trabalho.

Agradeço aos meus colegas de curso que, ao final desta longa caminhada, tornaram se bons amigos, proporcionando momentos memoráveis que eu me lembrarei com carinho para sempre.

“Apesar dos nossos defeitos, precisamos enxergar que somos pérolas únicas no teatro da vida e entender que não existem pessoas de sucesso e pessoas fracassadas. O que existem são pessoas que lutam pelos seus sonhos ou desistem deles.”

AUGUSTO CURY

RESUMO

SCHIAVO, João Matheus Ampessan. *Cloud Computing: uma questão de segurança*. 2015. Monografia (Especialização em Gestão de Serviços de Telecomunicações) – Programa de MGA, Centro Federal de Educação Tecnológica do Paraná. Curitiba, 2015.

A computação em nuvem ou *Cloud Computing* surge da necessidade de construir infraestruturas de TI complexas, onde os usuários não têm que realizar instalação, configuração e atualização de *softwares* sendo um novo modelo de computação emergente que move todos os dados e as aplicações dos usuários para grandes centros de armazenamento, os chamados *data centers*. Desta forma, as aplicações e os sistemas de *hardware* são distribuídos na forma de serviços virtuais baseados na Internet. Baseada em conceitos já estudados e estabelecidos previamente, como a virtualização e o modelo *pay-per-use*, a computação em nuvem possui uma série de vantagens no mercado atual, como a possibilidade de ampliar os recursos utilizados sempre que necessário. Porém, por ser um modelo relativamente recente, ainda existem grandes desafios pela frente a serem solucionados, como a segurança e a interoperabilidade. A adesão a serviços de segurança obrigará às equipes de segurança de TI das companhias a estabelecer maiores controles para os serviços baseados na Nuvem. A grande quantidade de pesquisas na área permitirá que o tema ainda seja amplamente debatido por muito tempo e difundido pelas empresas de todo o mundo.

Palavras-chave: *Cloud Computing*. Computação em nuvem. Segurança em redes. Redes de computadores. Tecnologia.

ABSTRACT

SCHIAVO, João Matheus Ampessan. *Cloud Computing: a security issue*. 2015. Monograph (Specialization in Telco Services Management) - MBA Program, Federal Center of Technological Education of Paraná. Curitiba, 2015.

Cloud Computing comes the need to build complex IT infrastructure, where users do not have to perform installation, configuration and software upgrades in a new model emerging computing that moves all data and user applications for large storage centers, called Data Center. Thus, applications and hardware systems are distributed as Internet-based virtual services. Based on concepts already studied and previously established, such as virtualization and model pay-per-use, Cloud computing has several advantages in the current market, such as possibility of expanding the resources used whenever necessary. However, because it is a relatively recent model, there are still major challenges ahead to be solved, such as security and interoperability. Adherence the security services will force teams to IT security companies to establish greater controls for Cloud-based services. The great amount of research in the area will allow the subject still be widely long debated and publicized by companies around the world.

Keywords: Cloud Computing. Cloud. Network security. Computer networks. Technology.

LISTA DE FIGURAS

Figura 1 – Modelo de <i>Cloud Computing</i>	15
Figura 2 – Plataforma do Chrome OS	16
Figura 3 – Modelo de <i>Cloud Computing</i>	28
Figura 4 – Crescimento do tráfego total de Internet (WAN) no Google	29

LISTA DE SIGLAS E ABREVIATURAS

CEO	Chief Executive Officer
CSA	Cloud Security Alliance
LAN	Local Area Network
IBM	International Business Machines
ISACA	Information Systems Audit and Control Association
NIST	National Institute of Standards and Technology
OS	Operational System
PC	Personal Computer
SLA	Service Level Agreement
SOA	Service-oriented Architecture
TI	Tecnologia da Informação
VoIP	Voz sobre IP
WAN	World Area Network

SUMÁRIO

1 INTRODUÇÃO	10
2 JUSTIFICATIVA	11
3 OBJETIVOS	12
3.1 OBJETIVO GERAL	12
3.2 OBJETIVOS ESPECÍFICOS	12
4 FUNDAMENTAÇÃO TEÓRICA	13
4.1 CLOUD COMPUTING	13
4.2 CLASSIFICAÇÃO DE SERVIÇOS NA CLOUD COMPUTING	16
4.2.1 Software como Serviço (SaaS)	17
4.2.2 Plataforma como Serviço (PaaS)	17
4.2.3 Infraestrutura como Serviço (IaaS).....	18
4.2.4 O modelo Multi-Inquilino.....	19
4.3 MODELOS DE IMPLANTAÇÃO PARA COMPUTAÇÃO EM NUVEM	20
4.3.1 Nuvem Privada (Private Cloud)	20
4.3.2 Nuvem Pública (Public Cloud)	21
4.3.3 Nuvem Comunitária (Community Cloud)	21
4.3.4 Nuvem Híbrida (Hybrid Cloud)	22
4.4 CARACTERÍSTICAS DA CLOUD COMPUTING	22
4.5 A REALIDADE BRASILEIRA.....	23
5 UMA QUESTÃO DE SEGURANÇA	25
5.1 GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO NA NUVEM	27
5.2 DESAFIOS PARA AS REDES DE COMPUTADORES.....	27
CONSIDERAÇÕES FINAIS	31
REFERÊNCIAS BIBLIOGRÁFICAS	32

1 INTRODUÇÃO

Segundo especialistas na área de tecnologia, importantes mudanças tecnológicas surgem a cada 20 anos, e uma delas é a *Cloud Computing* ou Computação em Nuvem. Cada vez mais dominante no mundo de Tecnologia da Informação (TI), esta nova tecnologia vem para desafiar o setor de telecomunicações e surge em meio a um mantra formado pelas organizações da área que visam principalmente à redução de custos.

Esta arquitetura em nuvem refere-se como um modelo no qual a computação (processamento, armazenamento e *softwares*) está em algum lugar da rede e é acessada remotamente, por exemplo: uma empresa ou pessoa não precisar ter mais nenhum *software* instalado em sua máquina, pois o acesso a todo e qualquer recurso será via internet (nuvem), num sistema operacional a partir de qualquer computador e em qualquer lugar, pode-se ter acesso a informações, arquivos e programas num sistema único, independente de plataforma.

Por esta constante evolução, a *Cloud Computing* nos obriga a estar constantemente em atenção à suas mudanças, ascensões e possíveis declínios, sejam os mesmos tecnológicos, ou apenas conceituais. No Brasil a tecnologia de computação em nuvem está fora da realidade na maioria das organizações, pois a infraestrutura de telecomunicações do país é deficiente.

A questão de segurança é de extrema importância para a *Cloud Computing* se tornar viável e é considerada prioridade na implementação deste serviço. Mas como esta virtualização permitirá que haja segurança em grande escala e significativa redução de custos para as organizações?

Este é o cenário da *Cloud Computing* e o seu crescimento será muito mais rápido e intenso que os analistas dizem e mesmo que muitos dos atores atuais da indústria de TI gostariam que fosse.

2 JUSTIFICATIVA

Abordar a *Cloud Computing* na visão de segurança é colocar em questão a essência desta tão recente tecnologia. O conceito, apesar de simples, tem provocado revoluções e se tornado cada vez mais conhecido devido à popularização da banda larga. Depois de uma era tecnológica caracterizada pela ascensão do computador pessoal (PC), estamos vendo o ressurgimento da centralização.

Esta centralização e virtualização de arquiteturas através de redes que antes eram acessadas localmente na própria empresa por seus usuários torna o quesito segurança como prioritário e fundamental para que a Computação em Nuvem continue sendo a plataforma do futuro pela qual empresas de todo o mundo possam aderir, deixando de lado seus servidores e sistemas, reduzindo custos e gastos com manutenção.

A empresa ou organização precisa confiar que seu trabalho e seus dados estarão tão seguros na nuvem quanto em seu próprio computador ou servidor, para isso este momento de auge em *Cloud Computing* é a melhor ocasião para se estudar e pôr em prática modelos de segurança robustos que atendam a necessidade e tragam mais confiança a estas organizações.

3 OBJETIVOS

3.1 OBJETIVO GERAL

Introduzir em âmbito de pesquisa a tecnologia de *Cloud Computing* e demonstrar a gestão de segurança, riscos e benefícios ao se utilizar desta plataforma por empresas e organizações.

3.2 OBJETIVOS ESPECÍFICOS

Promover o conhecimento sobre *Cloud Computing*, enfatizando a sua segurança tanto para o fornecedor da tecnologia quanto para as organizações e instituições que usufruem do serviço, de forma a relacionar os riscos que geram discussões e sustentar as ideias com modelos de gestão de segurança que tragam confiança e favoreçam o avanço desta tecnologia.

4 FUNDAMENTAÇÃO TEÓRICA

4.1 CLOUD COMPUTING

No ano de 1981 a IBM lançou nos Estados Unidos o seu primeiro computador pessoal. Mesmo possuindo configuração inúmeras vezes inferiores aos computadores domésticos atuais, o IBM PC 5150 iniciou a mudança do modelo computacional da época que era baseado em *mainframes*. Neste antigo modelo, um computador central trabalhava atendendo às solicitações de vários terminais, que tinham como finalidade efetuar a conexão entre dispositivos de entrada e saída do cliente e o servidor. Todo o processamento e armazenamento de dados era efetuado remotamente.

Os computadores pessoais iniciaram um novo modelo descentralizado, onde cada estação possui seu próprio poder computacional e trabalha de forma independente. A evolução no *hardware* e *software* dos computadores pessoais atingiu patamares quase inimagináveis há algumas décadas. Enquanto a versão inicial do IBM PC 5150 possuía um processador Intel 8088 de 4,77 MHz, 16 KB de memória RAM e utilizava fitas cassete como mídia de armazenamento, o *smartphone* Nexus S, anunciado pelo Google, possui processador de 1GHz, 512MB de memória RAM e 16GB de armazenamento interno, pesando apenas 129 gramas.

Com o crescimento da demanda, os preços dos microcomputadores caíram de maneira acentuada, permitindo o aumento da presença em micro e pequenas empresas e residências de diversas classes sociais. (ALECRIM, 2008)

A popularização do acesso à Internet começou a reconectar os computadores. A evolução constante da tecnologia computacional e das telecomunicações está fazendo com que o acesso à internet se torne cada vez mais amplo e cada vez mais rápido. Habitualmente, utilizamos aplicações instaladas em nossos próprios computadores, assim como armazenamos arquivos e dados dos mais variados tipos nos mesmos. No ambiente corporativo, este modelo é um pouco diferente, já que nele é muito mais fácil encontrar aplicações disponíveis em servidores e que podem ser acessadas por qualquer terminal com níveis de acesso através de uma rede.

Esse cenário cria a situação perfeita para a popularização da *Cloud Computing*, uma tecnologia recente que faz com que muitos aplicativos, assim como arquivos e outros dados relacionados, não precisam mais estar instalados ou armazenados no computador do usuário.

Em 2007, Eric Schmidt, então CEO do Google, utilizou pela primeira vez o termo *Cloud Computing* (computação em nuvem) para referenciar a maneira de como a empresa gerenciava seus *Data Centers*.

A palavra *cloud* (nuvem) pode ser definida como toda a estrutura de servidores presentes na Internet que não só armazenam, mas também processam informações e fornecem diversos serviços, como *backup* e até utilização de um servidor virtual.

“Embora possa parecer revolucionário, o conceito de Computação em Nuvem é um passo evolutivo na eterna busca pelo compartilhamento e conseqüentemente maior aproveitamento dos recursos computacionais”. (TAURION, 2009, p. 24)

Esta tecnologia pode ser vista por muitos como algo não tão complexo e com recursos semelhantes aos que já habitualmente são utilizados, como é o caso de alguns profissionais de TI que citam a *Cloud Computing* como uma simples arquitetura em nuvem repleta de servidores se comunicando entre si com o foco inicial em *hardware*. Porém, este modelo de virtualização vai muito além disso, e é disso que se refere o autor ao dizer que “a computação em nuvem sinaliza um novo paradigma computacional transformando toda a indústria de computação, como a energia elétrica transformou a nossa sociedade” (TAURION, 2009, p. 12).

Em alguns aspectos, o mercado de *Cloud Computing* ganhou corpo em 2008 quando empresas como a Amazon, IBM, Google, Microsoft e outras dezenas de grandes organizações tecnológicas lançaram produtos e serviços *on-demand*. Por outro lado, há quem veja esta tecnologia em nuvem como uma evolução natural da convergência de várias tecnologias e conceitos, como o próprio *Grid*, mais o conceito *Utility Computing* (que são serviços computacionais comercializados como os serviços utilitários, como energia elétrica), virtualização e *automatic computing*, que são sistemas capazes de auto gerenciar e corrigir problemas e falhas, acrescidos de tecnologias e tendências como Web 2.0, SOA e o modelo de *Software como Serviço* (SaaS). A Figura 1 mostra o conceito do modelo de *Cloud Computing* de acordo com as grandes empresas do ramo.

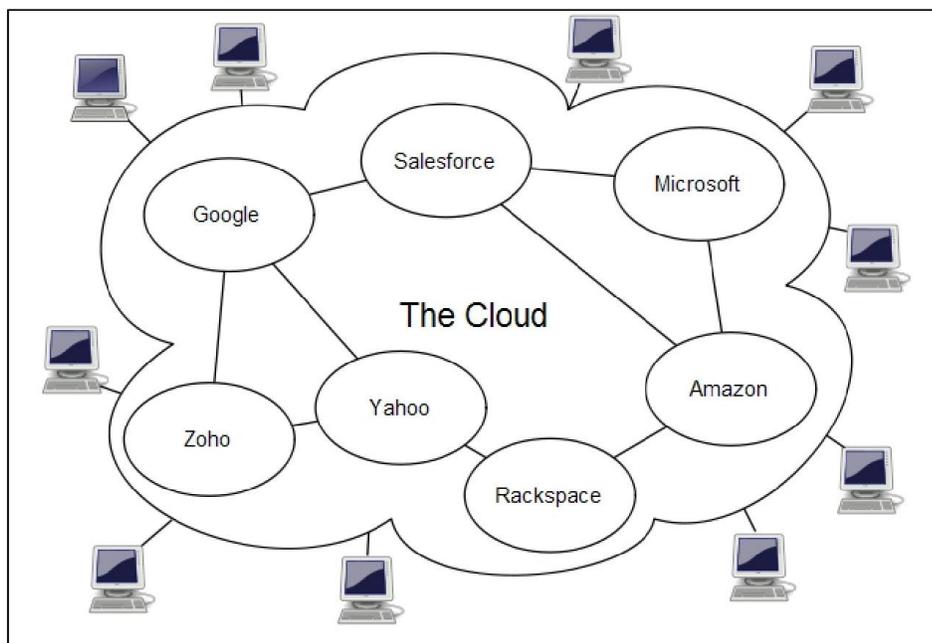


Figura 1 – Modelo de *Cloud Computing*
 Fonte: creativecommons.org, Sam Johnston

Segundo Laudon e Laudon (p.145, 1999), no atual Século XXI, os gigantes da comunicação estão envolvidos na maior competição empresarial de todos os tempos, onde o principal objetivo é construir e controlar com segurança a vasta teia de redes e serviços eletrônicos que fornecem informação, educação e serviços a empresas e residências de todo o mundo.

A empresa Google como exemplo vem, ao longo do tempo, se destacando no que diz respeito a plataformas de *Cloud Computing*. Uma arquitetura chamada “Google Docs”, permite que seus usuários possam criar planilhas, editar textos e elaborar apresentações de slides pela internet, sem necessidade de ter *softwares* instalados em seus computadores, as informações inseridas e alteradas ficam ali gravadas e distribuídas em inúmeros servidores da empresa. A praticidade é tanta que o acesso a plataforma se dá através de um navegador de internet qualquer onde basta o acesso do usuário a página do Google Docs para começar a trabalhar, não importando o computador utilizado nem o sistema operacional instalado. A plataforma vai muito além disso e a sua capacidade de integração com outros serviços e plataformas do próprio Google torna possível criar uma estrutura parruda e organizada de trabalhar com documentos tanto pessoais quanto corporativos. Outro desafio recente do Google, é o seu sistema operacional “nas nuvens” Chrome

OS. O compromisso da empresa é o de prover um sistema operacional completamente virtualizado e com o mínimo necessário de *hardware* para sua utilização. A figura 2 mostra a interface do sistema operacional desenvolvido pela Google.

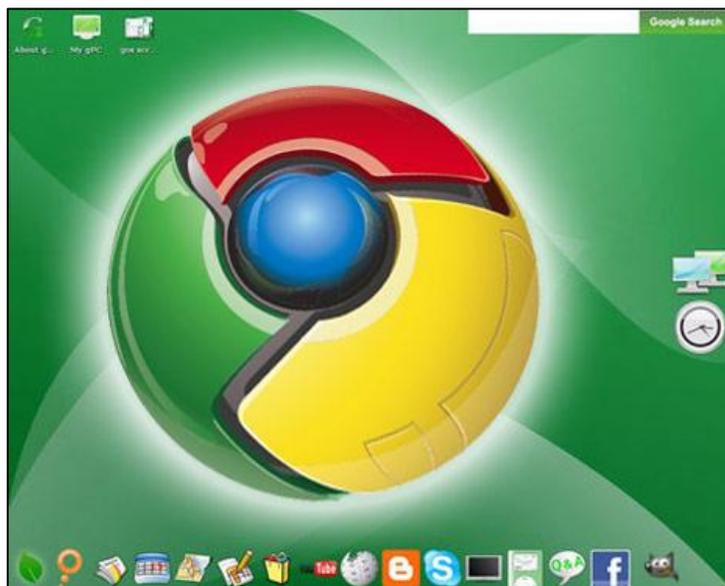


Figura 2 – Plataforma do Chrome OS
Fonte: google.com

Para Fontes (2008), a computação na nuvem não é nem uma solução para todos os problemas, nem uma solução de caos e pavor. É apenas mais uma opção de uso da tecnologia. Saber usar com inteligência pode ser a diferença de uma organização de mais sucesso daquela que ficou no nível normal.

O termo foi se tornando mais popular não só entre os gerentes de TI, mas também entre os investidores que foram seduzidos pelas ideias sobre redução do capital investido na infraestrutura computacional.

4.2 CLASSIFICAÇÃO DE SERVIÇOS NA CLOUD COMPUTING

As nuvens computacionais podem ser classificadas como públicas, privadas ou híbridas, de acordo com os seus inquilinos. As nuvens públicas são providas sob demanda a qualquer cliente, bastando que o mesmo contrate o serviço e o acesse usando a Internet.

Armbrust (2009) afirma que os serviços que definem as soluções e a arquitetura em ambientes de computação em nuvem podem ser compostos por três diferentes modelos: SaaS, PaaS e IaaS.

A empresa que contrata um modelo de serviço neste ambiente de computação em nuvem deve observar que os riscos e benefícios globais são diferentemente tratados, ou seja, dependem do modelo de serviço atribuído e o seu tipo de implantação para então definir os riscos que os acompanham.

4.2.1 Software como Serviço (SaaS)

O modelo de serviço internacionalmente conhecido como *Software as a Service* (SaaS) é o tipo mais conhecido e difundido de serviços de computação em nuvem. Fornece todas as funcionalidades de uma aplicação tradicional através do navegador de Internet, sem a necessidade de instalar aplicativos localmente.

SaaS elimina a preocupação com desenvolvimento e atualização das aplicações e dos seus servidores relacionados. Alguns exemplos comuns são serviços de *webmail*, como o Gmail da empresa americana Google, mensagem instantânea, como Yahoo!, serviços de VoIP, como Skype, e os aplicativos empresariais do Salesforce.com.

Este tipo de serviço de computação em nuvem modifica a forma de licenciamento de *software*. No modo tradicional, o cliente adquire uma licença do aplicativo, instala em seus computadores e cuida de tarefas de manutenção e atualização. O modelo de licenciamento tradicional permite a utilização do aplicativo por tempo indeterminado, já no modelo SaaS o cliente possui a permissão para usar o sistema enquanto estiver pagando pelo serviço. Desta forma, o tempo que a empresa dedicaria com a base de TI pode ser utilizado nas tarefas diretamente relacionadas à sua atividade de negócios.

4.2.2 Plataforma como Serviço (PaaS)

Diferentemente do modelo SaaS (*Software como Serviço*) a arquitetura de Plataforma como Serviço, do Inglês *Platform as a Service* (PaaS), fornece servidores

nos quais os usuários podem executar, administrar e gerenciar suas aplicações existentes ou desenvolver outras novas sem se preocupar com manutenção dos sistemas operacionais, *hardware* dos servidores ou capacidade computacional.

É um modelo que ainda está em desenvolvimento e apresenta algumas limitações, como restrição do tipo de aplicação, linguagem de programação e servidor de banco de dados utilizados. Google AppEngine, que antes utilizava somente a linguagem Python, passou também a suportar Java, já Force.com trabalha apenas com Apex. Essas peculiaridades dificultam o processo de migração das plataformas de desenvolvimento atuais para as baseadas no modelo de computação em nuvem.

4.2.3 Infraestrutura como Serviço (IaaS)

A solução de Infraestrutura como Serviço, do Inglês *Infrastructure as a Service* (IaaS), fornece estruturas de servidores virtualizados, em *cluster* ou em *grade*, além de armazenamento e sistemas projetados para melhorar ou substituir um *data center* completo, eliminando a presença dos servidores na empresa do cliente. O acesso à banda larga é essencial, pois o acesso a este servidor terceirizado ocorre através da Internet. O cliente pode aumentar ou diminuir dinamicamente a sua estrutura computacional. *Elastic Compute Cloud* (EC2) e *Simple Storage Service* são serviços da empresa virtual americana Amazon.com que permitem utilizar servidores virtuais e armazenamento remoto, respectivamente. O pagamento dos serviços da Amazon.com é baseado no volume de utilização, onde o cliente paga somente pelo utilizado.

No Brasil, RedeHost e LocaWeb são empresas que iniciaram na área de hospedagem de sites e atualmente também disponibilizam serviços de IaaS. O modelo mais comum entre as empresas brasileiras baseia-se em uma taxa mensal fixa de acordo com o serviço contratado.

4.2.4 O modelo Multi-Inquilino

A diminuição dos custos por parte dos provedores de serviços de computação em nuvem são baseados no compartilhamento de recursos computacionais por diferentes empresas clientes, chamadas de inquilinos. A arquitetura multi inquilinos permite que a estrutura física seja compartilhada ao mesmo tempo que exista uma separação lógica entre cada inquilino. Neste cenário, diversos inquilinos dividem um mesmo servidor do provedor, mas cada um só possui acesso às suas próprias informações.

A eficiência dos recursos computacionais é obtida através da alocação dinâmica de recursos, onde cada cliente os obtêm quando necessário e os liberam ao terminar a utilização, permitindo ao fornecedor de serviço possuir mais inquilinos por servidor.

Como cada empresa possui suas diferenças, o modelo multi-inquilino permite que haja uma personalização da aplicação de acordo com as necessidades do cliente. A customização depende do fornecedor do serviço, sendo este um grande atrativo para o cliente.

Em um modelo tradicional de estrutura cliente-servidor, cada inquilino utiliza servidores dedicados para a execução de suas aplicações, constituídos basicamente de um servidor de aplicação, responsável pelas regras de negócios e funcionamento do aplicativo, e de um servidor de banco de dados, que cuida do armazenamento de informações.

A arquitetura multi inquilino é classificada em três tipos de acordo com o nível de isolamento dos dados:

- Banco de dados separados: A execução das aplicações e os recursos computacionais são geralmente compartilhados entre todos os inquilinos, mas cada um possui a sua própria estrutura de banco de dados, garantindo a isolamento de dados entre eles.
- Banco de dados compartilhados com esquemas separados: Diferentes inquilinos utilizam os recursos de um mesmo banco de dados e a separação lógica dos dados ocorre por cada um possuir o seu conjunto de tabelas agrupadas em um esquema criado e restrito especificamente para ele.

- Banco de dados e esquemas compartilhados: Vários inquilinos compartilham o banco de dados e seu conjunto de tabelas. Cada entrada no banco de dados compartilhado possui uma identificação que o associa com o inquilino, garantindo a separação lógica dos dados entre os diferentes clientes.

Segurança e otimização de recursos são fatores que influenciam na escolha do nível de isolamento de dados da arquitetura multi-inquilino. Quanto mais isolados, mais seguros estarão os dados, impedindo que um inquilino acesse acidental ou propositalmente os dados do seu vizinho. Em uma forma mais compartilhada, mais inquilinos podem ser mantidos utilizando menos recursos computacionais, consequentemente diminuindo os custos de operação. Entretanto, é necessário um esforço maior na etapa de desenvolvimento para garantir um funcionamento seguro do sistema.

4.3 MODELOS DE IMPLANTAÇÃO PARA COMPUTAÇÃO EM NUVEM

A computação em nuvem dispõe de quatro modelos básicos para sua implantação. A escolha de um modelo que melhor se adapte às particularidades de cada empresa, depende do tipo de informação, do processo de negócios e do nível de visão e segurança desejado. O NIST (*National Institute of Standards and Technology*) (NIST, 2009), divide os modelos de implantação de computação em nuvem em: privado, público, comunitário e híbrido.

4.3.1 Nuvem Privada (*Private Cloud*)

Uma nuvem privada é, em geral, construída sobre um *data center* privado. Este modelo de implantação permite que esta seja administrada pela própria organização ou por terceiros através de políticas de acesso aos serviços. Segundo o NIST (2009), as ferramentas utilizadas para prover tais características podem ser em

nível de gerenciamento de redes, configurações dos provedores de serviços e a utilização de tecnologias de autenticação e autorização.

Diferentemente dos outros modelos de implantação de nuvem em detrimento de sua natureza privada, esse é o que prove um menor risco. Em termos de automação de tarefas como atualizações, torna-se engessado pelo fato de estar diretamente atrelado aos processos corporativos. Além disso, por exigir um gerenciamento interno, e embora traga algumas facilidades por estar no ambiente da empresa, este diminui a economia de recursos.

4.3.2 Nuvem Pública (*Public Cloud*)

De acordo com o NIST (2009), este modelo de implantação a infraestrutura de nuvens é disponibilizada para o público em geral ou para grupos de indústrias, sendo acessado por qualquer usuário que conheça a localização do serviço. As aplicações de diversos usuários ficam misturadas nos sistemas de armazenamento, o que pode parecer ineficiente a princípio, porém se adotadas as políticas de segurança e uma estrutura organizada, a existência de outras aplicações na mesma nuvem permanece transparente para os usuários.

Em termos de economia e compartilhamento de recursos, o conceito de nuvens públicas proporciona um maior desempenho, por outro lado, uma vez que os dados podem ser armazenados em locais desconhecidos e não podem ser facilmente recuperados, o modelo possui certas limitações de customização relacionadas justamente à segurança das informações, SLAs (Service Level Agreement) e políticas de acesso.

4.3.3 Nuvem Comunitária (*Community Cloud*)

No modelo de implantação de nuvem comunitária ocorre o compartilhamento por diversas empresas de uma nuvem localmente ou remotamente, sendo esta suportada por uma comunidade específica que partilha de interesses semelhantes, tais como a missão, os requisitos de segurança, política e considerações sobre flexibilidade.

O NIST (2009) cita que este tipo de modelo de implantação pode existir localmente ou remotamente e pode ser administrado por alguma empresa da comunidade ou por terceiros, semelhante ao modelo de Nuvem Privada em relação à definição de políticas de acesso e a utilização de tecnologias de autenticação e autorização. Outro fator importante é o fato dos dados e informações poderem ser armazenados com os dados de outros concorrentes pertencente à mesma comunidade.

4.3.4 Nuvem Híbrida (*Hybrid Cloud*)

De acordo com ISACA (2009), este modelo é composto de dois ou mais modelos de implantação de nuvem (nuvem pública ou comunidade privada) que permanecem como entidades únicas, sendo relacionadas por uma tecnologia padronizada ou proprietária que permite a portabilidade de dados e de aplicações (por exemplo, nuvem de ruptura para balanceamento de carga entre nuvens).

Para garantir que os dados sejam atribuídos ao tipo de nuvem correto, a escolha deste modelo exige uma minuciosa classificação e rotulagem dos dados. A conexão entre as nuvens pública e privada pode ser usada até mesmo em tarefas periódicas que são mais facilmente implementadas nas nuvens públicas, por exemplo. Como fator negativo do modelo é o alto risco, uma vez que funde diferentes formas de implantação.

4.4 CARACTERÍSTICAS DA CLOUD COMPUTING

Conforme já destacado, a Computação em Nuvem possibilita a utilização de aplicações e recursos diretamente da internet e o acesso se dá remotamente. Entretanto, existem outras significantes vantagens em utilizar este modelo de arquitetura em nuvem e que seguem descritas abaixo.

- a) o usuário não precisa se atentar com a estrutura em que a aplicação está rodando. *Hardware*, procedimentos de *backup*, controle de segurança, manutenção, entre outros, são de inteira responsabilidade do fornecedor do serviço;

- b) o compartilhamento de dados e informações bem como trabalhos colaborativos se tornam mais fáceis, uma vez que todos os usuários fazem parte de um mesmo lugar e acessam as mesmas aplicações e dados na rede;
- c) a redundância do serviço se torna possível, dependendo do fornecedor, podendo o usuário contar com alta disponibilidade, já que, se for o caso, um servidor parar de funcionar e os demais que fazem parte da estrutura continuam a oferecer o serviço;
- d) o usuário pode obter redução de custos, uma vez que, muitas aplicações em *Cloud Computing* são gratuitas e quando outras são cobradas, o usuário só pagará em relação aos recursos utilizados ou ao tempo de utilização.

Para Alecrim (2008), “independente da aplicação, com a *Cloud Computing* o usuário não necessita conhecer toda a estrutura que há por trás, ou seja, ele não precisa saber quantos servidores executam determinada ferramenta, quais as configurações de *hardware* utilizadas, como o escalonamento é feito, onde está a localização física do *datacenter*, enfim”.

4.5 A REALIDADE BRASILEIRA

A *Cloud Computing* no Brasil é vista ainda como fora da realidade para as grandes empresas que investem em tecnologia. Os primeiros testes deste modelo foram implementados em 2007, sendo que somente em 2008 começou a ser oferecido e comercializado. O grande problema enfrentado atualmente refere-se no que diz respeito a como este serviço é oferecido e distribuído.

Hoje, a computação em nuvem brasileira muito é tratada apenas como hospedagem, ou seja, você paga uma mensalidade por um pacote que às vezes pode ser personalizado, porém com funcionalidades ainda restritas e um valor um pouco excessivo.

Para Corrêa (2010), diferentemente da visão brasileira, o modelo estrangeiro de *Cloud Computing* tem desempenho dinâmico, ou seja, se você por acaso tiver uma demanda inesperada na sua aplicação, em 10 minutos você terá quantos

servidores quiser à disposição e funcionando para suportar a nova demanda. No modelo brasileiro, você abre um chamado e aguarda pacientemente ou liga na central de atendimento reclamando virtualmente com o primeiro atendente e implorando por uma solução mais rápida.

A realidade é que o Brasil é um país com uma imensa capacidade tecnológica, basta organização e desenvolvimento para que possa sair desta estaca inicial e assim comercializar a verdadeira *Cloud Computing*.

5 UMA QUESTÃO DE SEGURANÇA

Entender os riscos de segurança em *Cloud Computing* é exercer o papel fundamental para que esta tecnologia seja realmente procurada e confiada pelas empresas que demonstram interesse em adquirir este modelo em nuvem. De acordo com Taurion (2010), “o ritmo e disseminação da computação em nuvem está diretamente relacionado com o grau de confiança no modelo e nas tecnologias envolvidas”.

Questões relacionadas ao compartilhamento de tecnologias (*hardware* e *software*), Interfaces inseguras, perda de dados, uso indevido de *Cloud Computing* e sequestro de contas compõem a lista de riscos, não necessariamente na ordem de relevância.

Para que uma empresa utilize a computação em nuvem pode-se dizer que deve haver uma mudança severa em toda a sua tecnologia, desde *softwares* até *hardware*. Conforme Falsarella (2010), “esta mudança representa uma oportunidade para melhorar ainda mais a segurança, porém, ao mesmo tempo, representa a possibilidade de piorar as coisas, empurrando aplicações vulneráveis e dados para a web”.

Toda mudança tecnológica, por menor que seja, tem sempre riscos e, no caso da *Cloud Computing* à medida que mais e mais experiências práticas sejam obtidas, mais detalhes devem ser observados e relacionados. Ao definir como, por exemplo, controles de acesso para a computação em nuvem, as organizações devem considerar que os seus colaboradores estarão entrando na nuvem, bem como em sistemas internos, para usar os recursos. Além disso eles devem definir controles de uso, o acesso aos diretórios da nuvem interna ou permissões para copiar esses diretórios para fora da nuvem.

Nesta questão de controle de acesso quando relacionado à computação em nuvem, Falsarella (2010) afirma que utilizar apenas “Nome de usuário” e “Senha” não é a forma mais segura de acessar os dados corporativos, pois já estamos acostumados e diariamente vivenciamos ataques de “força bruta” contra grandes empresas de tecnologia como Google, Amazon e outros.

As ameaças a que nossos dados e serviços estão sujeitos quando estão nas nuvens são as mesmas a que estão sujeitos quando tradicionalmente armazenados nos nossos servidores, porém a responsabilidade de responder corretamente estas

ameaças parte do provedor de computação nas nuvens. Em uma análise mais detalhada sobre os riscos e ameaças, Carvalho (2009) aponta sete aspectos relacionados à segurança que devemos considerar ao selecionar um fornecedor de computação nas nuvens, sendo esses:

- a) Acesso privilegiado aos dados;
- b) Atendimento a normas e certificados;
- c) Localização física dos dados;
- d) Segregação dos dados;
- e) Recuperação de desastres;
- f) Suporte ao processo de investigação;
- g) Viabilidade a longo prazo.

A medida que este modelo vai ganhando forma aumenta o número de gestores de TI que estão confortáveis em relação ao nível de segurança de dados oferecido pelos provedores de *Cloud Computing*, que *Cloud Security* é tão boa ou melhor que muitos departamentos de TI poderiam oferecer internamente. Isso pode ser verdade, mas isso só será válido quando os argumentos ganharem exposição, ou seja, usuários finais, reguladores e outros grupos terão que ser convencidos de que a computação em nuvem é realmente segura.

Buscando preparar melhor o mercado futuro da computação em nuvem, a CSA (*Cloud Security Alliance*), entidade que promove as melhores práticas em *cloud computing*, criou uma certificação específica para profissionais especializados em segurança na nuvem. Através de um certificado batizado de *Certificate of Cloud Security Knowledge (CCSK)*, o grupo focaliza-se nos especialistas em segurança virtual das tecnologias da informação, reunindo especificações essenciais para que uma pessoa, ao fazer a certificação, possa ser realmente um profissional em computação em nuvem.

Fatores como latência¹, segurança, níveis de serviço e disponibilidade também são problemas que, com razão, atentam os profissionais de TI quando a conversa gira em torno de *Cloud Computing* e não devem ser deixados de levar em consideração. Nos próximos anos, os fornecedores terão de trabalhar muito para resolvê-los de modo a satisfazer os usuários.

¹ Em uma rede, latência é sinônimo de atraso, é uma expressão de quanto tempo leva para um pacote de dados ir de um ponto designado para o outro.

5.1 GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO NA NUVEM

Analisando o cenário atual para o gerenciamento de segurança da informação em ambientes de Computação em Nuvem, muitas literaturas apontam a necessidade e a importância de se adotar um modelo de Governança da Segurança da Informação com a finalidade de aliviar os riscos inerentes dos modelos de prestação de serviços em *cloud*.

Por se tratar de serviços de grande multiplicidade prestados pelos provedores de *Cloud Computing*, tais como e-mails, desenvolvimento de aplicativos personalizados, armazenamento de dados e gestão de infraestrutura, podemos considerar que esses são um aglomerado de recursos e dados.

A percepção de que a nuvem é um conjunto de informações pode caracterizá-la como sendo um alvo propício a ataques por potenciais invasores. Ameaças como esta podem com certeza afetar diretamente os três pilares da segurança da informação: disponibilidade, confidencialidade e integridade, e consequentemente comprometer toda a nuvem.

Segundo Turion (2009), a garantia do cumprimento desses princípios relaciona-se diretamente com o modelo de implantação contratado pela empresa, por exemplo, o modelo de Nuvem Privada, que permite a restrição de acessos uma vez que se encontra atrás do *Firewall* da empresa, mantendo, dessa forma, controle do nível de serviço e aderência às regras de segurança da empresa.

5.2 DESAFIOS PARA AS REDES DE COMPUTADORES

Segundo Torres (2001, p.5), “As redes de computadores surgiram da necessidade da troca de informações, onde é possível ter acesso a um dado que está fisicamente localizado distante de você”.

O crescimento desta demanda implica no aumento da infraestrutura de Tecnologia da Informação e de Comunicação e neste cenário, a *Cloud Computing* traz um grande desafio para as redes de computadores e para as empresas de

Telecomunicações responsáveis pelo fornecimento de toda a infraestrutura necessária para alimentar com uma infinidade de *bytes* os produtos tecnológicos que cada vez mais estão presentes na vida da população mundial. Milhares de *data centers* estão conectados à Internet, provendo serviços como difusão de conteúdos áudio e vídeo, envio de e-mails, acesso às redes sociais e armazenamento de fotos e vídeos aos usuários em seus computadores e outros dispositivos portáteis em qualquer lugar do mundo. A Figura 3 mostra a evolução de hospedagem em Computação em Nuvem.

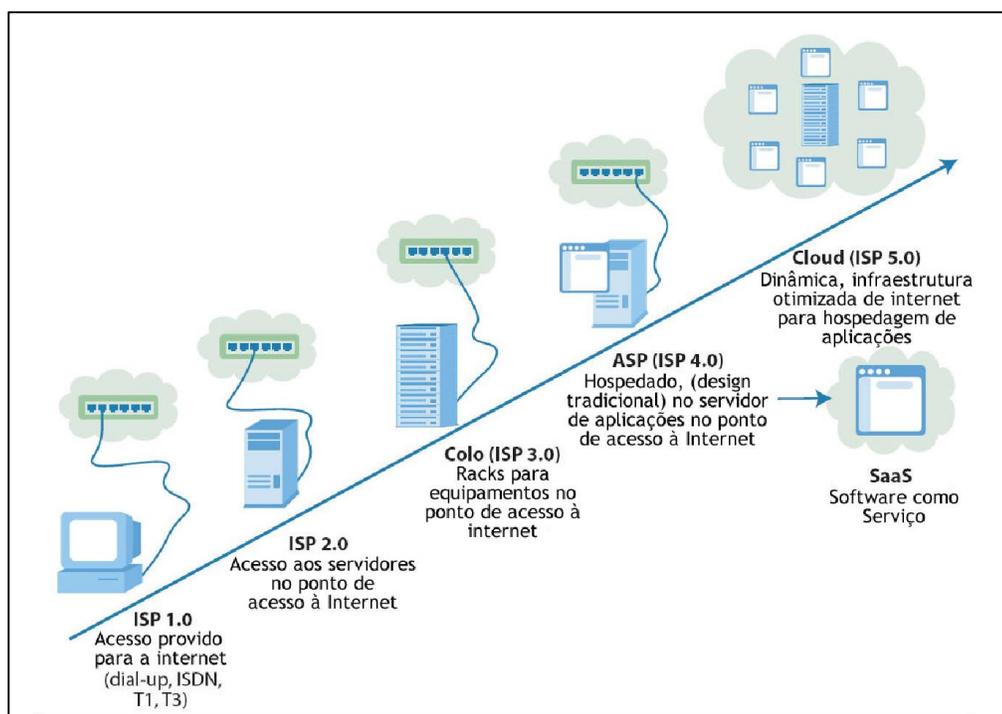


Figura 3 – Evolução da hospedagem em Cloud Computing
Fonte: Adaptado de Forrester Research Inc.

A medida que os serviços das empresas são migrados de servidores locais para *data centers* espalhados por todo o mundo, o tráfego de dados aumenta proporcionalmente isto porque o que antes era acessado em uma rede LAN (*Local Area Network*), passa a ser acessado através de uma rede WAN (*World Area Network*) o que gera demanda na ampliação da malha de redes de telecomunicações.

O principal problema nas redes de computação em nuvem é o desempenho a confiabilidade e a segurança das conexões com a infra-estrutura de nuvem. Essas

conexões WAN, devido ao aumento da complexidade e demandas de largura de banda dos aplicativos de *software*, vão se tornando mais e mais lotados ao longo do tempo. A tendência é de aumento de tráfego e congestionamento. Em uma infraestrutura de nuvem, em muitos casos, este congestionamento não pode ser facilmente previsto.

De acordo com Newman (2007), estima-se que 31% dos gastos das empresas com comunicação/transmissão são consumidos pelas WANs. *Cloud computing* pode facilmente aumentar o custo da comunicação se a otimização da WAN não é devidamente aplicada.

Sem as melhorias de desempenho, a latência e o tráfego inerentes de conexões WAN podem levar as conexões remotas para a nuvem e gerar um congestionamento. Quando os aplicativos remotos necessitam de alta-disponibilidade, otimizar conexões WAN de ponta a ponta é crucial para evitar que aplicações sejam interrompidas, corrompendo dados ou frustrando trabalhos em locais remotos.

Aplicações, tais como vídeos, aplicações de servidores virtualizados, e *software* como serviço (SaaS) rodando na nuvem exigem mais banda do que os tradicionais arquivos de dados baseados em texto e registros de banco de dados através de conexões WAN normais. A Figura 4 mostra um exemplo do crescimento do tráfego total da empresa Google que possui além de grande quantidade de dados baseados em texto, uma vasta armazenagem e *streaming* de vídeo.

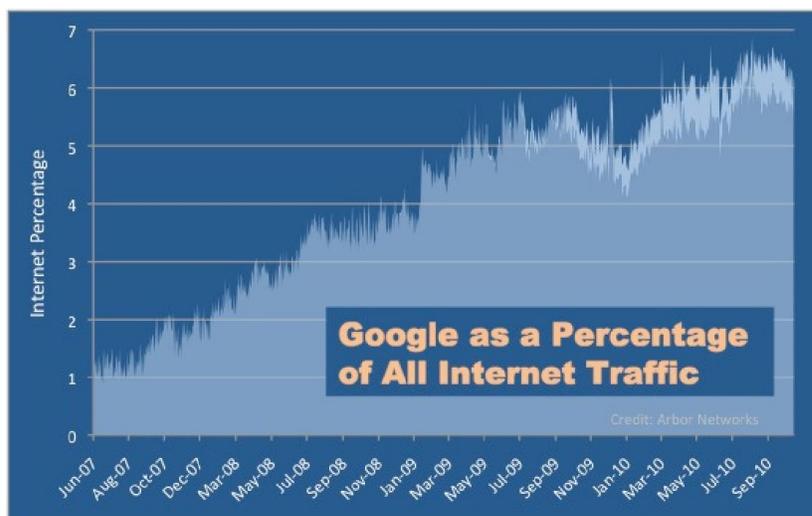


Figura 4 – Crescimento do tráfego total de Internet (WAN) no Google
 Fonte: <http://googlediscovery.com>

Segundo o UOL (2011), até 2015, o volume de tráfego de dados na internet deve crescer 26 vezes alcançando 6,3 exabytes por mês – ou uma taxa anual de 75 exabytes. Dois dos principais fatores para que esse aumento ocorra são o crescimento do uso de dispositivos móveis como tablets e smartphones, além do aumento do consumo de vídeos nesses aparelhos móveis.

Para que todo este cenário de crescimento no tráfego total da internet mundial não se torne um problema para a expansão da computação em nuvem é necessário que as empresas de telecomunicações se estruturam de modo a acompanhar este crescimento, podendo então através de medidas antecipadas, fornecer meios de transmissão seguros e de alta velocidade sem gerar resultados negativos para os seus usuários.

CONSIDERAÇÕES FINAIS

Citada por muitos como a computação do futuro, a Computação em nuvem ou *Cloud Computing* é um novo conceito que vem, aos poucos, ganhando espaço, não só na área organizacional e comercial, como também na área acadêmica. Nesse novo modelo, os dados e as aplicações dos usuários, que, originalmente, ficariam em seus computadores pessoais, deslocam-se para *data centers* distantes fisicamente, mas que podem ser acessados através da Internet. Chama-se de nuvem a camada conceitual que abstrai toda a infraestrutura da plataforma computacional, deixando os serviços transparentes aos usuários. Todo este novo modelo de infraestrutura está gerando indagações sobre a localização, segurança, disponibilidade, confiabilidade e portabilidade dos dados, uma vez que a “nuvem” poderá contar principalmente com serviços e dados de grandes empresas e órgãos do governo.

Para tanto, a segurança da nuvem requer uma abordagem estruturada e que seja ágil e elástica. Proteger e assegurar para os clientes que os serviços e dados são tratados de acordo com os níveis acordados de disponibilidade, integridade e confidencialidade é apenas o desafio inicial.

Este trabalho teve como principal propósito conceituar a computação em nuvem, abordando a segurança como fator fundamental para que esta nova plataforma seja vista ao longo do tempo como um modo evolutivo da tecnologia diminuindo a desconfiança gerada pelos profissionais da área e aplicando-a utilizando-se de todos os conceitos de segurança.

REFERÊNCIAS BIBLIOGRÁFICAS

ALECRIM, Emerson. O que é *Cloud Computing*? **InfoWester**, São Paulo, dez. 2008, Disponível em: <<http://www.infowester.com/cloudcomputing.php>>. Acesso em: 20 ago. 2015.

ARMBRUST, M, Fox, A., Griffith, R., Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. "Above the Clouds: A Berkeley View of Cloud Computing". **UC Berkeley Reliable Adaptive Distributed Systems Laboratory**. fev. 2009, Disponível em: <<http://radlab.cs.berkeley.edu/>>. Acesso em: 12 ago. 2015.

CARVALHO, Márcio B. de. Segurança nas Nuvens? **Fonte**, Minas Gerais, n. 9, dez. 2009.

CORREA, Willian. Qual o melhor *Cloud Computing* no Brasil? **iMasters**, Espírito Santo, mai. 2010, Disponível em: <http://imasters.uol.com.br/artigo/16923/cloud/qual_o_melhor_cloud_computing_no_brasil_nuvem_aqui_e_fumaca>. Acesso em: 19 jul. 2015.

FALSARELLA, Douglas. *Cloud Computing: a segurança pode ser melhor na nuvem?* **iMasters**, Espírito Santo, abr. 2010, Disponível em: <http://imasters.uol.com.br/artigo/16451/cloud/cloud_computing_a_seguranca_pode_ser_melhor_na_nuvem>. Acesso em: 10 ago. 2015.

FONTES, Edison. Segurança da Informação: A computação é na nuvem, mas os pés ficam no chão! **UOL Blog**, São Paulo, ago. 2008.

ISACA, Emerging Technology. Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives. **ISACA**. Illions, EUA. Out. 2009. Disponível em:<<http://www.isaca.org>> Acesso em: 15 set. 2015.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de Informação: com internet**. Rio de Janeiro, 4. ed. LTC, 1999.

NEWMAN, David. WAN acceleration offers huge payoff. **Network World**. ago. 2007.

NIST (National Institute of Standards and Technology). The NIST Definition of Cloud Computing, Version 15, **National Institute of Standards and Technology**,

Information Technology Laboratory. Gaithersburg, Maryland, EUA, 2009. Disponível em: <<http://www.nist.org>> Acesso em: 17 set. 2015.

TAURION, Cezar. Segurança em *Cloud Computing*. **WordPress**, São Paulo, mar. 2010. Disponível em: <<http://computingonclouds.wordpress.com/2010/03/04/seguranca-em-cloud-computing-3>>. Acesso em: 12 ago. 2015.

TAURION, Cezar. ***Cloud Computing: computação em nuvem***. Rio de Janeiro, ed. Brasport, 2009.

TORRES, Gabriel. **Redes de Computadores**. Rio de Janeiro. 1 ed. Axcel Books, 2001.

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ. **Normas para elaboração de trabalhos acadêmicos**. Curitiba: UTFPR, 2015.

UOL. Tráfego de dados mundial na internet triplicou em 2010, aponta pesquisa. **UOL Tecnologia**. Disponível em: <<http://tecnologia.uol.com.br>> Acesso em: 14 set. 2015.