RAABY FRANCYS APOLINARIO DE PAULO

SEGURANÇA E PRIVACIDADE EM COMPUTAÇÃO EM NUVEM

LAVRAS – MG

2014

RAABY FRANCYS APOLINARIO DE PAULO

SEGURANÇA E PRIVACIDADE EM COMPUTAÇÃO EM NUVEM

Monografia de Graduação apresentada ao Departamento de Ciência da Computação para obtenção do título de Bacharel em Sistemas de Informação.

Orientador
Prof. Dr. Neumar Malheiros

LAVRAS – MG
2014

RAABY FRANCYS APOLINARIO DE PAULO

SEGURANÇA E PRIVACIDADE EM COMPUTAÇÃO EM NUVEM

Monografia de graduação apresentada ao Colegiado do Curso de Bacharelado em Sistemas de Informação, para obtenção do título de Bacharel.

APROVADA em 4 de julho de 2014.

Luiz Henrique Andrade Correia

Hermes Pimenta de Moraes Júnior

Neumar Costa Malheiros (Orientador)

LAVRAS-MG
2014

Dedico este trabalho aos meus pais, meus irmãos e a todos que de alguma forma contribuíram para o meu crescimento acadêmico e pessoal.

AGRADECIMENTOS

Agradeço primeiramente, a Deus pelas oportunidades que me concedeu, por estar sempre ao meu lado, iluminar meus pensamentos para a conclusão deste trabalho e principalmente por me dar forças para prosseguir nos momentos difíceis.

Aos meus pais, pelo apoio que sempre me deram, por serem responsáveis pela minha formação, por terem enfrentados dificuldades para que eu pudesse realizar meu sonho, entendendo minha ausência e sempre me incentivando, por cada oração para que eu superasse todos os desafios e por serem um exemplo de amor e dedicação.

Aos meus familiares, em especial meus irmãos, que sempre me apoiaram nessa busca pelo meu sonho. A minha avó querida, Benedita Cunha Apolinário, por cada oração e pelo seu imenso amor. Aos meus avós Alexandra Mariano de Paulo e Vicente de Paulo, que se foram antes de me ver concluir este sonho, mas que foram essenciais na minha formação.

Ao meu namorado Lucas por ter me incentivado a continuar e me ajudado nos momentos mais difíceis deste projeto. O qual é uma pessoa muito importante e especial na minha vida.

Ao meu orientador, prof. Neumar Malheiros, pela oportunidade, paciência, incentivo, auxílio e apoio neste projeto.

A todos, que de alguma forma, contribuíram para meu crescimento acadêmico e por momentos inesquecíveis nestes anos, só posso dizer: Muito obrigada!

“A tarefa não é tanto ver aquilo que ninguém viu, mas pensar o que ninguém ainda pensou sobre aquilo que todo mundo vê.” (Arthur Schopenhauer)

RESUMO

O presente trabalho teve como objetivo estudar as questões que envolvem a segurança e privacidade dos dados das empresas que usam serviços de Computação em Nuvem. Como a utilização desses dados podem afetar as organizações ou até que ponto o uso desse novo paradigma pode ser benéfico, são questões que causam um certo receio na transição para este novo modelo de serviço. As empresas ainda temem que o sigilo de suas informações seja comprometido. Por isso, as empresas que fornecem serviços de Computação em Nuvem precisam ter boas práticas de segurança e garantia da privacidade dos dados dos usuários para minimizar esses riscos. Algumas soluções que fornecem serviços de Computação em Nuvem foram estudadas nesse trabalho, uma delas, o Windows Azure, foi analisada em um estudo de caso para verificar os mecanismos de segurança fornecidos.

Palavras-Chave: Computação em Nuvem; Segurança; Privacidade.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1 INTRODUÇÃO

A Computação em Nuvem (*Cloud Computing*) surgiu como um novo paradigma na área de computação, a partir da necessidade de se oferecer serviços de Tecnologia da Informação (TI) sob demanda com pagamento baseado no uso (VAQUERO *et al.*, 2008). Este paradigma permitiu a diminuição dos custos para empresas e usuários finais, uma vez que não é preciso um investimento tão grande em equipamentos e software.

A Computação em Nuvem é um modelo que possibilita acesso, de modo conveniente e sob demanda, a um conjunto de recursos computacionais configuráveis. Esses recursos podem ser rapidamente reservados, utilizados e liberados com mínimo esforço gerencial ou interação com o provedor de serviços (MELL; GRANCE, 2011).

Como descrito em (PETNEWS, 2012), a ideia da Computação em Nuvem já existia em 1960, com Joseph Licklider, que discutia sobre uma rede de computadores intergaláctica em que todos estariam conectados acessando programas e dados. Foi também na década de 1960, que John McCarthy, um dos pioneiros da inteligência artificial, propôs a ideia de que a computação deveria ser organizada na forma de um serviço de utilidade pública, assim como os serviços de água e energia, em que usuários pagam pelo que usam. Mas, somente em 1997, o termo Computação em Nuvem veio a ser mencionado em uma palestra acadêmica ministrada pelo professor Ramnath Chellappa. No entanto, a primeira empresa a disponibilizar serviços sob demanda na Internet foi desenvolvida com o surgimento da Salesforce.com só dois anos depois em 1999. A partir do sucesso desta, outras empresas grandes começaram a investir nessa área.

Existem três aspectos importantes para se definir um modelo padrão para os serviços de Computação em Nuvem. O primeiro deles, a virtualização, que proporciona a ilusão de disponibilizar recursos ilimitados. O segundo aspecto é a escalabilidade, ou seja, a empresa pode contratar um serviço modesto no começo

e expandir quando for necessário, sem que haja perda do que já existia e com gasto menor se comparado ao modelo de negócios padrão utilizando *hardware* próprio. O último aspecto é o "pague pelo que usar" (do inglês *pay-per-use*), que consiste basicamente em pagar apenas pelo serviços utilizados. O preço pago pelos serviços contratados pode aumentar ou diminuir, conforme a demanda de recursos exigida (VAQUERO *et al.*, 2008).

Com a popularização do acesso à Internet, principalmente com a expansão cada vez maior da conexão através de dispositivos móveis, a Computação em Nuvem vem se tornando cada vez mais presente e necessária, uma vez que existe a limitação de capacidade de armazenamento e processamento nesses aparelhos. Com isso, utilizar a nuvem vem sendo algo vantajoso tanto para os fabricantes que podem diminuir os custos na produção quanto para os usuários que podem ter seus dados sempre ao alcance em qualquer aparelho e sem o risco de perder tudo caso ocorra algum problema com os aparelhos. No Brasil, a Computação em Nuvem ainda não é amplamente utilizada devido às baixas taxas de velocidade da Internet no país, exceto em regiões metropolitanas, onde já existem serviços de acesso à Internet de qualidade. Consequentemente, nessas regiões, as pessoas utilizam mais os serviços de armazenamento e compartilhamento de dados na nuvem.

Além disso, outro fator que tem levado à crescente demanda pela Computação em Nuvem é o crescimento explosivo de bases de dados. Uma prova disso é a projeção realizada pela Century Link, na qual até 2015, o mundo testemunhará um aumento de quatro vezes na quantidade de informações criadas e replicadas por meio de recursos computacionais (DELL, 2013). Neste contexto, o armazenamento em Nuvem representa uma solução eficiente para guardar todos esses dados com segurança e facilidade de acesso aos usuários finais.

1.1 Definição do Problema

As vantagens da Computação em Nuvem são notórias. No entanto, existem alguns problemas que precisam ser resolvidos, como por exemplo questões de segurança e privacidade das informações armazenadas na Nuvem. Além disso, existem alguns desafios para que ocorra a transição para esse novo modelo de serviço por parte das empresas. Como a utilização desses dados podem afetar as organizações ou até que ponto o uso desse novo paradigma pode ser benéfico, são questões que causam um certo receio. As empresas ainda temem que o sigilo de suas informações seja comprometido, uma vez que os dados estão armazenados em infraestruturas de terceiros distribuídas pela Internet.

1.2 Objetivos

Já que a Computação em Nuvem vem sendo vista como uma tendência mundial, são necessário certos cuidados, principalmente no que diz respeito a segurança e privacidade. Neste contexto, o objetivo deste trabalho é estudar as questões que envolvem a segurança e a privacidade dos dados das empresas que usam serviços de Computação em Nuvem. Para isso, foi realizado um estudo de quais são os principais problemas e desafios de segurança e privacidade neste paradigma. Foi realizado também, um estudo de algumas das principais ferramentas que fornecem serviços de Computação em Nuvem. Após este estudo aprofundado, estas ferramentas foram avaliadas. A partir dessa avaliação, foi realizado um estudo de caso com a ferramenta Windows Azure para verificar se ela atende aos principais requisitos de segurança e privacidade.

1.3 Organização do Texto

Este trabalho está organizado da forma a seguir. No Capítulo 2, é apresentado o referencial teórico, onde é realizado um estudo com os conceitos básicos sobre segurança da informação, privacidade, virtualização, Computação em Nuvem e riscos de segurança e privacidade. No Capítulo 3, é apresentada a metodologia, no qual são descritas as atividades envolvidas. No Capítulo 4, são descritas diversas ferramentas que fornecem serviços de Nuvem e as melhores práticas de segurança e garantia da privacidade que foram identificadas. No Capítulo 5, é apresentado um estudo de caso. No estudo de caso, são avaliados os mecanismos de segurança e privacidade em uma das ferramentas estudadas, o Windows Azure. E por fim, no Capítulo 6, é apresentada a conclusão e a discussão de alguns trabalhos futuros.

2 REFERENCIAL TEÓRICO

Para que a Computação em Nuvem seja entendida de forma clara e objetiva, é preciso entender algumas questões relacionadas ao acesso remoto a dados através de redes de comunicação. Para tanto, será apresentado um breve estudo sobre segurança da informação, privacidade, virtualização e por fim, fundamentos do paradigma de Computação em Nuvem.

2.1 Segurança da Informação

Com os avanços da tecnologia, vem acontecendo um crescimento explosivo das bases de dados das organizações tornando a informação um bem vital. Junto a isso, é crescente também o número de problemas relacionados à segurança da informação, visto que boa parte das empresas utilizam a Internet como um meio de transmissão de dados confidenciais que muitas vezes não estão devidamente protegidos. Desse modo, estão suscetíveis a ataques, o que coloca em risco as organizações e as pessoas. A violação do sigilo e integridade das informações pode trazer prejuízos financeiros de grandes proporções. Os prejuízos causados pela perda de informações importantes não é feito apenas por roubos destas. Desastres naturais, bem como incidentes casuais podem trazer riscos, perdas, vazamento e até mesmo indisponibilidade da informação.

A segurança da informação torna-se essencial neste caso, pois ela tem como objetivo a proteção das informações de clientes e empresas, controlando o risco de revelação ou alteração dos dados por pessoas não autorizadas (CARNEIRO; RAMOS, 2010).

A segurança da informação se baseia em quatro propriedades básicas: a confidencialidade, integridade, disponibilidade e autenticidade. A confidencialidade garante que os dados se tornem acessíveis apenas para pessoas autorizadas. A integridade garante que as características originais da informação sejam man-

tidas. A disponibilidade assegura que pessoas autorizadas tenham acesso à informação sempre que for necessário. A autenticidade garante a confiabilidade de que os dados provêm de fato da fonte primária.

As principais técnicas de segurança da informação baseiam-se em ferramentas que permitem garantir que as informações não serão violadas. Entre as principais ferramentas de segurança, pode-se destacar: criptografia, *firewall* e IDS (*Intrusion Detection System*) (OLIVEIRA, 2003). A criptografia é uma técnica que permite que as informações sejam transformadas de forma a ficarem ilegíveis, podendo ser decifrada apenas por seu destinatário. O *firewall* é um sistema de controle de acesso. Com uso de tal sistema, é possível negar a usuários não autorizados o acesso a determinados recursos disponíveis na rede. Assim, ele funciona como um barreira de proteção. IDS (Sistemas de Detecção de Intruso) são sistemas inteligentes, que são capazes não só de detectar um tentativa de invasão em tempo real, mas também capazes de tomar decisões necessárias afim de evitar o sucesso do ataque.

Mesmo com todas essas ferramentas, a informação pode ser violada. Para muitos o valor da informação só é percebido quando esta é violada, por isso o investimento em segurança da informação é algo indispensável seja qual forem os dados transmitidos.

2.2 Privacidade

A violação de informações, não envolve somente uma questão de segurança, mas também uma questão de privacidade. Pois, a privacidade é o direito que todas as pessoas tem de resguardar suas informações pessoais.

O risco da privacidade ser violada aumentou com o surgimento de redes sociais, sites de compartilhamento e espionagem digital. A era digital trouxe dois lados: de um lado as facilidades de se obter e publicar informações, de outro a facilidade de que estas informações sejam expostas à todos.

A violação da privacidade tem sido um problema que pode atingir desde uma pessoa comum até casos de espionagem diplomática. A exposição de informações em redes sociais vem se tornando um problema cada vez mais comum, prejudicando a imagem de muitas pessoas, comprometendo sua privacidade e até mesmo trazendo problemas psicológicos. Já no meio político, a espionagem diplomática tem mostrado a vulnerabilidade dos meios de comunicação utilizados por serviços secretos, líderes e organizações de vários países.

Com tudo isso, a troca e disponibilização de informações na rede é posta sob suspeita. Até que ponto é seguro usar esses meios tecnológicos? Tendo em vista que com a globalização a tecnologia se tornou algo indispensável, essa questão vendo sendo cada vez mais abordada. Empresas do ramo de segurança e privacidade da informação vem sendo desafiadas todos os dias a superarem essas dificuldades para garantir a proteção das informações dos usuários.

2.3 Virtualização

A virtualização permite a simulação de uma máquina real dentro de outra máquina real. Com a virtualização é possível ter várias máquinas virtuais operando juntas em uma mesma máquina real, abrindo inúmeras possibilidades de configurações e tarefas a serem executadas por essas máquinas.

Quanto aos modelos de virtualização, existem três tipos mais comuns:

VMM (Monitor de Máquina Virtual) Nativo

Nessa arquitetura, o VMM (*Virtual Machine Monitor*) é utilizado diretamente no *hardware* da máquina real como visto na Figura 2.1. Mais utilizado em servidores, os monitores mais comuns desse tipo de arquitetura é o XEN (XEN, 2013) e o VMWARE ESX SERVER (VMWARE, 2013). Assim o monitor tem maior controle sobre o acesso ao *hardware* disponível, po-

dendo controlar as requisições feitas pelos sistemas convidados, simulando diferentes máquinas físicas de maneira isolada sobre o mesmo *hardware*.

Figura 2.1: Monitor de Máquina Virtual Nativo

VMM (Monitor de Máquina Virtual) *Hosted*

No modo *hosted*, o monitor é implementado em um sistema operacional hospedeiro como ilustrado na Figura 2.2. Toda a comunicação com o *hardware* é feita através desse sistema hospedeiro. Dessa forma, apenas o sistema hospedeiro tem controle sobre o *hardware* da máquina real. Nesse caso, o monitor é um processo no sistema hospedeiro. Esse tipo de arquitetura é bastante utilizado por usuários finais através do VIRTUALBOX (VIRTUALBOX, 2013) e VMWARE SERVER (VMWARE, 2013). Uma forma possível de otimizar o desempenho é configurar o sistema convidado para acessar diretamente o sistema hospedeiro. Um exemplo é o VMWARE, onde o sistema convidado pode utilizar o sistema de arquivos do sistema hospedeiro.

VMM (Monitor de Máquina Virtual) Híbrida

Esse tipo de arquitetura é a junção das características do monitor do modo nativo e do monitor do modo *hosted*. Essa maneira híbrida tem como função principal otimizar os dois sistemas, agregando as características de ambos os modelos de virtualização. A Figura 2.3, ilustra a arquitetura híbrida.

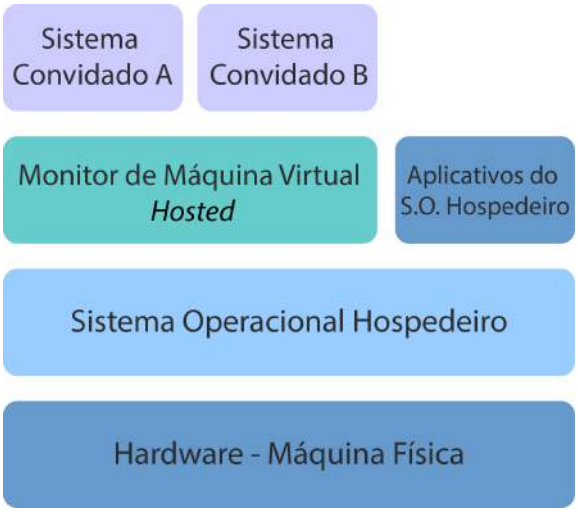


Figura 2.2: Monitor de Máquina Virtual Hosted

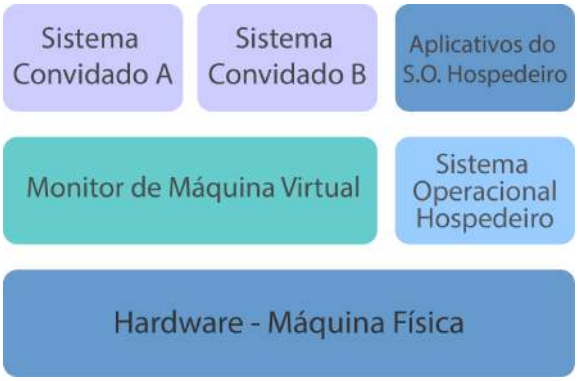


Figura 2.3: Monitor de Máquina Virtual Híbrida

O uso da virtualização diminui os custos referentes a *hardware*, espaço físico, facilidade de manutenção, entre outras vantagens. Muitas empresas estão migrando para a virtualização, visando essas vantagens e com isso reduzindo a complexidade do seu ambiente de TI.

O uso da virtualização na Computação em Nuvem é indispensável. O paradigma de Computação em Nuvem depende de ferramentas de virtualização para todas as soluções que ela disponibiliza.

2.4 Computação em Nuvem

Conforme apresentado em (BRIAN *et al.*, 2008), existem várias definições práticas para Computação em Nuvem. Qualquer aplicação Web já é chamada de serviço de Nuvem, muitas vezes puramente por razões de marketing. Entretanto, um serviço em Nuvem real possui características que vão além de meramente oferecer um serviço Web.

Segundo o NIST *(National Institute of Standards and Technology)* (NIST, 2014), Computação em Nuvem é um modelo que possibilita acesso, de modo conveniente e sob demanda, a um conjunto de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente reservados, utilizados e liberados com mínimo esforço gerencial ou interação com o provedor de serviços (MELL; GRANCE, 2011).

No entanto, Computação em Nuvem é um paradigma que está em constante evolução, ou seja, há muitas definições que poderão surgir com o decorrer do tempo, por meio de debates entre as partes envolvidas. Mas, pode-se dizer que a essência deste novo paradigma não mudará. Computação em Nuvem continuará fornecendo serviços de fácil acesso e de baixo custo e garantindo características tais como disponibilidade e escalabilidade.

De acordo com o que foi apresentado em (SOUSA; MOREIRA; MACHADO, 2009), o modelo de Computação em Nuvem visa fornecer basicamente três benefícios. O primeiro benefício é a redução do custo de aquisição e composição de toda infraestrutura de TI requerida para atender as necessidades da empresa. O segundo benefício é a flexibilidade oferecida por esse modelo quanto à adição e troca de recursos computacionais. Já o último benefício corresponde a abstrair e facilitar o acesso dos usuários aos serviços.

2.4.1 Características Essenciais

Para compor uma solução de Computação em Nuvem, são necessárias características essenciais, pois elas são consideradas vantagens que a Nuvem pode oferecer (SOUSA; MOREIRA; MACHADO, 2009). A seguir estão as cinco características essenciais e suas definições.

Self-service sob demanda

No *self-service* sob demanda, o usuário poderá reconfigurar o *hardware* e o *software* do serviço de nuvem contratado, podendo fazer instalação de *software*, aumentar o poder de processamento e armazenamento de acordo com a sua necessidade, sem que haja intervenção da empresa provedora do serviço.

Amplo acesso

Amplo acesso significa que o usuário tem acesso a todos os recursos através da rede por meio de mecanismos padronizados. Desse modo, o usuário não precisa modificar o sistema operacional e nem as linguagens de programação utilizadas por sua empresa.

Pooling de recursos

No *Pooling de recursos*, os recursos computacionais estão agrupados em conjuntos servindo múltiplos usuários, com diferentes recursos físicos e virtuais, que poderão ser disponibilizados de acordo com as suas necessidades. A localização física desses recursos são ocultas para o usuário, nesse caso é apenas especificada a localização em alto nível como país, estado e *data center*.

Elasticidade rápida

Na elasticidade rápida, quando há necessidade de um aumento rápido na quantidade de recursos alocados, o sistema poder realizar isso de forma au-

tomática de acordo com a necessidade do momento, e do mesmo modo diminuir quando não houver necessidade dessa demanda.

Para que pareça que o usuário tenha recursos infinitos a qualquer momento e em qualquer quantidade é necessária a virtualização, pois é através dela que várias instâncias de recursos requisitados podem ser criadas, utilizando um único recurso real.

Serviço Medido

Para controlar o aumento e a diminuição dos recursos, os sistemas em Nuvem utilizam medições para otimizar e controlar a demanda desses recursos. Esse controle pode ser monitorado tanto pelo usuário quanto pela empresa, de modo que ambas as partes tenham conhecimento de toda alteração realizada durante a utilização do serviço na Nuvem.

2.4.2 Modelos de Serviços

Para se definir um padrão para arquiteturas de soluções de Computação em Nuvem, são utilizados três modelos de serviços, que serão definidos na sequência. A Figura 2.4 mostra a estrutura desses modelos.

***Software* como Serviço (*Software as a Service* (SaaS))**

Em um nível mais alto na Nuvem estão localizados *softwares* que são disponibilizados aos usuários. Esses *softwares* estão instalados na Nuvem e são acessados remotamente pelos usuários.

Plataforma como Serviço (*Platform as a Service* (PaaS))

É uma plataforma de desenvolvimento para o SaaS. Nesse modelo o usuário também é considerado prestador de serviço, o PaaS é utilizado como facilitador no desenvolvimento de aplicações para o usuário. É utilizado para integração entre sistema operacional, um *middleware* e um ambiente

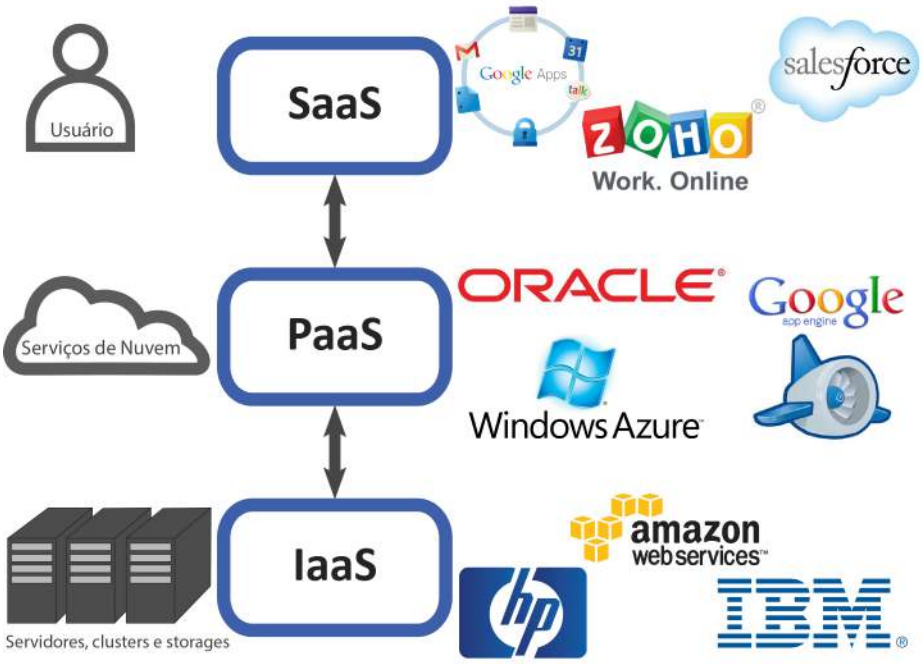


Figura 2.4: Modelos de Serviços

de desenvolvimento, fazendo a interação através de uma interface de programação de aplicativos. Dessa forma, torna-se mais simples e rápido o desenvolvimento de aplicações. No entanto, o desenvolvimento fica limitado à plataforma utilizada.

Infraestrutura como Serviço (*Infrastructure as a Service* (IaaS))

Envolve toda a infraestrutura de uma Nuvem, incluindo servidores, roteadores e sistemas de armazenamento disponibilizados na rede. Nesse modelo, apenas os prestadores de serviço têm acesso para prover aos usuários os serviços da Nuvem através da virtualização. O IaaS é amplamente utilizado em casos como o da computação de alto desempenho que necessita de um grande poder de processamento.

2.4.3 Modelos de Implantação

O modelo de implantação trata do fato de se ter ambientes separados de Computação em Nuvem para diferentes níveis de acesso do usuário. Essas restrições variam de acordo com o processo de negócio, tipo de informação e do nível desejado ao qual o usuário terá acesso. Daí a necessidade de se dividir a Computação em Nuvem nos seguintes modelos: privado, público, comunidade e híbrido. A Figura 2.5 ilustra esses modelos de implantação.

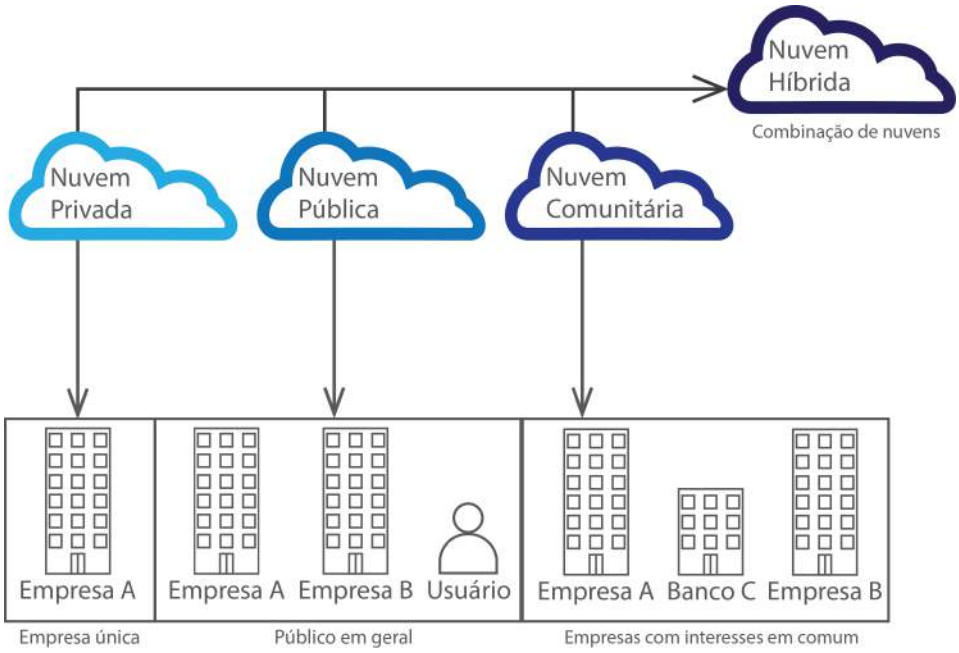


Figura 2.5: Modelos de Implantação

Privado

Nesse modelo de implantação a Nuvem possui políticas de restrição mais rígidas de acesso, onde apenas uma organização pode utilizar esses serviços, seja de modo remoto ou local. Nesse modelo existem modos de autenticação e autorização de acesso, configurações de provedores de serviços e gerenciamento de redes.

Público

Nesse modelo de implantação, o acesso pode ser feito por qualquer usuário que porventura tente acessar os serviços. Desse modo, no modelo público não é possível utilizar métodos de autenticação e autorização e restrições de acesso.

Comunidade

Nesse modelo o acesso aos serviços pode ser feito por várias empresas por meio compartilhado e administrado por uma das empresas ou por terceiros, assim como no modelo privado. Essa rede de empresas formam uma comunidade que disponibiliza os serviços e dados apenas entre presentes nessa comunidade, ficando indisponível para usuários externos. Assim como no modelo de Nuvem privada, ela pode existir tanto localmente quanto remotamente.

Híbrido

Nesse modelo é feita a junção de duas ou mais nuvens, sendo privadas, comunitárias ou públicas, as quais comunicam entre si, portando dados e aplicações através de tecnologia proprietária ou padronizada. Essas nuvens são tratadas como uma única Nuvem.

2.4.4 Papéis

Para que um serviço de Computação em Nuvem possa ser bem utilizado pelos usuários é importante que existam os papéis que visam definir os serviços de acesso, responsabilidade e perfil para cada usuário do serviço.

Os papéis na Computação em Nuvem estão dispostos em vários níveis, desde os modelos de serviço até os usuários do serviço. Nos modelos de serviço, a IaaS está localizada na parte mais baixa, fornecendo os recursos de *hardware* e *software* para PaaS. Este por sua vez, fornece as ferramentas de desenvolvimento

e execução de serviços implementados que estarão disponíveis na SaaS. No nível de usuário e provedor, os provedores controlam os três modelos de serviço, fornecendo cada um dos serviços aos outros usuários. Apenas o provedor pode fornecer acesso aos três modelos. Os usuários finais tem acesso apenas aos serviços no modelo SaaS. Os desenvolvedores fornecem serviços SaaS e consomem serviços IaaS e PaaS, ambos fornecidos pelo provedor. Este último também fica a cargo de gerenciar e monitorar os serviços disponibilizados. A Figura 2.6 destaca esses papéis.

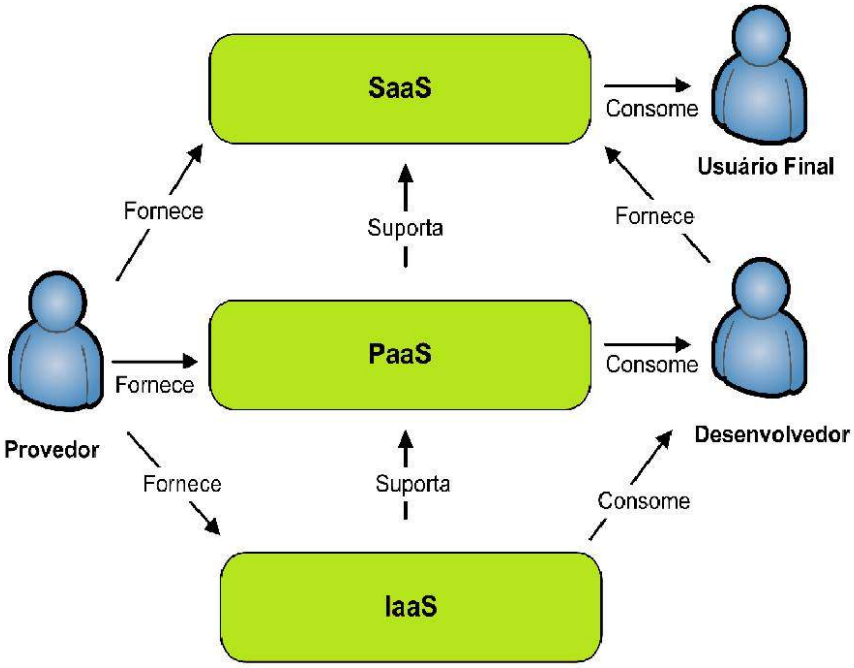


Figura 2.6: Papéis na Computação em Nuvem

2.4.5 Escalabilidade

A escalabilidade é a possibilidade que se tem de aumentar os recursos computacionais dos servidores da Nuvem e a composição dos serviços presentes na mesma,

aumentando o desempenho da Nuvem e assim deixando o usuário despreocupado quanto a limitação de recursos disponíveis.

O usuário final precisa guardar seus dados na Nuvem, porém não precisa saber onde eles serão armazenados ou como é feito o acesso a esses dados. E nisso entra a escalabilidade de uma Nuvem, seja horizontal ou vertical. Os nós disponíveis em uma Nuvem podem ser melhorados em suas capacidades através da disponibilização de recursos físicos de outro servidor ou até mesmo da conexão de dois nós, sendo essa a escalabilidade vertical. A escalabilidade horizontal é a capacidade de uma Nuvem se conectar a outras nuvens, podendo integrar seus serviços.

2.5 Riscos de Segurança e Privacidade

São muitas as questões relacionadas à segurança e privacidade da informação em Computação em Nuvem. A contratação de um serviço de Nuvem causa certos receios às organizações, tendo em vista que, suas informações, muitas delas sigilosas, estarão alocadas em *data centers* de terceiros.

Alguns dos principais problemas de segurança para Computação em Nuvem são proteção de dados, gerenciamento de vulnerabilidade, a integridade operacional, a continuidade dos negócios e a recuperação de desastres. Outra preocupação fundamental é a privacidade, quando os dados de usuários são fornecidos, ou até mesmo vendidos, para provedores de marketing, podendo levar ao mau uso e violação da privacidade. Quanto a isso, é difícil controlar, pois o cliente talvez nunca saiba que seus dados pessoais foram vendidos para esses provedores.

A privacidade torna-se um assunto delicado quando se trata de Computação em Nuvem. O Dropbox (DROPBOX, 2014) por exemplo, oferece armazenamento online gratuito, sendo uma das primeiras empresas bem sucedidas e mundialmente conhecidas a oferecer esse tipo de serviço. Mesmo podendo pagar por um serviço *premium*, muitos assinantes, cerca de 98% das pessoas que usam o

Dropbox, usufruem do serviço gratuito. Para tanto, o Dropbox precisa obter receitas de terceiros, implicando no uso de publicidade e venda de informações sobre assinantes não pagantes (DUFFANY, 2012).

No caso do Amazon Cloud Drive (DRIVE, 2014), o usuário precisa desistir conscientemente da sua privacidade, já que para usar esse serviço que oferece armazenamento gratuito, o usuário aceita os termos de condições do contrato que diz: " Você nos dá o direito de acessar, reter, usar e divulgar sua informação de conta e seus arquivos: para prover a você suporte técnico e questões técnicas de endereço; para investigar o cumprimento com os termos desse acordo, e proteger o serviço e seus usuários de fraude ou ameaças de segurança; ou como determinarmos necessário para prestar serviço ou cumprir com a legislação aplicável". Isso pode levar a uma hipótese de que a Amazon está usando este acordo para conseguir receitas, como por exemplo, através do uso de mineração de dados e vendendo essa informação para terceiros (DUFFANY, 2012). Mesmo sendo anti-ético, muitas empresas lucram com as informações de privacidade de seus usuários.

Se a prestadora de serviço em Nuvem vende as informações pessoais de seus clientes, mesmo que sejam os clientes que usam o serviço gratuito, não se pode garantir que ela não fará uso indevido dos dados que seus clientes armazenam na Nuvem. Isso se torna um problema sério de confiabilidade entre usuário e prestador de serviço em Nuvem. É uma linha tênue de confiança e credibilidade entre eles. Mas, com o crescimento da Computação em Nuvem e aumento da concorrência, as empresas prestadoras de serviço em Nuvem estão mais preocupadas com a questão da privacidade e segurança de dados de seus clientes, tendo em vista que, um deslize pode levar o cliente a contratar seu concorrente.

No que diz respeito à segurança dos dados armazenados na Nuvem, devem ser considerados os riscos de exposição ou mineração de dados. Há a possibilidade de dados críticos serem copiados sem o conhecimento do proprietário ou até mesmo sem permissão. Existe ainda a possibilidade de ataques de *hackers*

ou ataques de negação de serviço ou, até mesmo, casos de espionagem por parte de governos. Uma caso recente de espionagem é do ex-técnico da CIA, Edward Snowden (G1, 2013), que revelou em detalhes um dos programas de vigilância usado pelo país para espionar a população americana e outros países. Consequentemente muitas organizações consideram a questão da segurança como o maior desafio que inibe a adoção deles ao modelo de serviço de Nuvem.

A virtualização pode ser considerada como a essência da Computação em Nuvem, sem ela seria impossível oferecer tantas vantagens. No entanto, a virtualização torna-se um problema inerente em relação a alocação e desalocação de recursos. Pois, se os recursos alocados em um disco rígido de um determinado cliente não forem devidamente excluídos, existe a chance de que esses recursos alocados possam ser recuperados posteriormente por outros clientes através de *softwares* que executam varredura no disco rígido em busca de vestígios de dados que podem ser restaurados e utilizados novamente.

A empresa de consultoria Gatner (BRODKIN, 2008), apontou os principais riscos de segurança em Computação em Nuvem.

- Dados críticos sendo processados fora da empresa traz consigo um nível inerente de risco. A empresa contratante de um serviço de Nuvem deve se ater ao fato de que seus dados serão processados por uma outra empresa, no caso a prestadora de serviço de Nuvem. Desse modo, ela precisa saber qual o nível de acesso a prestadora de serviço, juntamente com seus funcionários, possuem sobre esses dados.

- Falta de conformidade com a regulamentação faz com que prestadoras de serviço em Nuvem limitem seus serviços. As provedoras de Nuvem estão sujeitas à auditoria externas e certificações de segurança. A não submissão por parte das provedoras a estas regulamentações, expõem que os consumidores podem utilizar os serviços apenas para funções triviais.

- As empresas não sabem exatamente a localização de onde estão armazenados os seus dados. Ao enviar os dados para uma Nuvem, a empresa fica a mercê do provedor de serviço no que diz respeito ao local do armazenamento dos seus dados. Tendo em vista que, com a mudança de local, altera-se também a legislação do país onde estão armazenados estes dados.

- Os dados em uma Nuvem estão normalmente em um ambiente compartilhado, ao lado de dados de outros usuários. Os dados de empresas diferentes compartilhando o mesmo local físico podem, eventualmente, ser acessado sem autorização por ambas as partes.

- Um provedor que não realiza replicação de dados e aplicações está vulnerável à falhas. A infraestrutura de uma Nuvem sendo em suma composta por equipamentos eletrônicos e mecânicos, está sujeita a falhas, bem como a desastres naturais, os quais podem ocasionar a perda parcial ou total das informações armazenadas.

- Pode ser impossível investigar atividades ilegais na Nuvem. Ao tentar investigar uma atividade ilegal, torna-se difícil obter registros e dados dos usuários envolvidos, pois esses registros podem estar armazenados em vários servidores, de vários países, com legislações diferentes.

- O provedor de serviço pode falir ou ser vendido a uma empresa maior. Caso isso aconteça, existe a possibilidade dos dados da empresa contratante não estarem disponíveis. Pode acontecer ainda que os dados da empresa sejam entregues em um formato incompatível com outros aplicativos ou serviços de substituição.

Como citado em (SUBASHINI; KAVITHA, 2011), Computação em Nuvem move as aplicações de *software* e banco de dados para grandes *data centers*, onde o gerenciamento de dados e serviços não são fidedignos. Devido a isso, este

cenário específico apresenta muitos novos desafios de segurança. Estes desafios incluem riscos como os relacionados a seguir:

- Vulnerabilidade na virtualização. Sendo um dos principais componentes na Nuvem, a virtualização também oferece um dos maiores riscos de segurança. Isso se deve ao fato de que instâncias diferentes podem ser executadas em uma mesma máquina, o que é um risco alto, caso não estejam isoladas uma da outra.

- Falta de *backup*. A não realização de *backups* regularmente dos dados críticos de uma empresa pode dificultar a recuperação desses dados em caso de desastres.

- Falhas de segurança na Nuvem. Como os dados de vários usuários e organizações estão juntos em um ambiente de Nuvem, uma falha nessa Nuvem pode potencializar um ataque aos dados de todos esses usuários.

- Vulnerabilidade de acesso. Quando o acesso feito pelo usuário é realizado por meio de métodos frágeis, acaba facilitando a invasão do sistema através de ataques ao sistema de autenticação.

- Vulnerabilidade do sistema. Um sistema de Nuvem vulnerável pode resultar em vários riscos para os dados armazenados, tais como, adulteração que pode afetar a integridade e confidencialidade e a perda e roubo dos dados.

- Vulnerabilidade em aplicações Web. Uma falha de segurança em uma aplicação Web, como por exemplo uma falha no SQL (*Structured Query Language*) que leva a um ataque do tipo SQL *injection*, pode causar uma vulnerabilidade na aplicação SaaS, o que afetaria todos os usuários dessa Nuvem.

- Vulnerabilidade no controle de acesso físico. O acesso físico aos servidores por pessoas não autorizadas expõem os dados armazenados ao risco de roubo.

Além dos riscos citados acima, são estudados em (DUFFANY, 2012) outros riscos. O artigo destaca que existem riscos inerentes à Computação em Nuvem, que podem ser facilmente subestimados. Uma vez que ao passar informações para fora do próprio controle, há a possibilidade desses dados serem comprometidos. Esses riscos estão relacionados a seguir:

- Exposição e mineração de dados. Os dados armazenados na Nuvem muitas das vezes estão expostos na Internet e isso pode facilitar a mineração de dados por parte de outras empresas para a venda de informações.

- Falta de um padrão para os provedores de Computação em Nuvem. Não existe um padrão sobre a prestação de serviços em Nuvem, o que dificulta a compatibilidade entre serviços de diversos provedores.

3 METODOLOGIA

A Computação em Nuvem mostra-se vantajosa e atraente e as empresas estão investindo em ritmo crescente neste modelo de negócio. Com a virtualização de produtos e serviços computacionais, ela proporciona uma redução de custos com tecnologia e infraestrutura local, e faz com que as empresas ganhem praticidade e versatilidade (CARNEIRO; RAMOS, 2010). Além disso, dados podem ser visualizados em qualquer dispositivo móvel e de qualquer lugar do planeta, necessitando apenas de acesso à Internet.

Mas, disponibilizar dados importantes e informações confidenciais pode trazer riscos aos usuários. Com os avanços tecnológicos e o aumento de roubos e vazamentos de informações pela rede, torna-se um desafio garantir a segurança na Nuvem.

As empresas que oferecem serviços de Computação em Nuvem, precisam garantir que informações não serão perdidas, roubadas ou violadas. Sendo assim, essas empresas precisam desenvolver soluções de segurança e sigilo dos dados. Em contrapartida tecnologias avançadas estão sendo utilizadas para violar os dados, tornando a rede vulnerável à ataques de *"hackers"*.

Este projeto tem como intuito estudar os aspectos que envolvem segurança e privacidade em Computação em Nuvem. As atividades que foram executadas nesse projeto estão relacionadas a seguir:

- ***Estudo comparativo das soluções.*** Primeiramente, algumas soluções que fornecem serviços de Computação em Nuvem foram escolhidas. Após a escolha dessas soluções, foi realizado um estudo descrevendo as principais funcionalidades e características de cada uma. As soluções estudadas são:

    1. **OpenStack.** É um software de código aberto capaz de gerenciar e configurar os componentes de várias infraestruturas virtualizadas, assim como um sistema operacional convencional.

2. **Apache CloudStack.** É um serviço de código aberto que possui recursos para criação de infra-estrutura de Nuvens públicas, privadas e híbridas utilizadas pelo IaaS.
3. **Amazon EC2, VMWare e o Windows Azure.** São ferramentas pagas, foram estudadas de acordo com a disponibilidade dos fabricantes.

   Após esse estudo, foi realizado um resumo comparativo entre essas ferramentas.

- ***Estudo de caso.*** Foi realizado um estudo de caso com a solução de Computação em Nuvem Windows Azure. Esse estudo de caso foi realizado, para que os mecanismos de segurança fossem testados. Esses mecanismos de segurança compreendem o controle de acesso, o armazenamento seguro e o transporte seguro dos dados. Para isso, foram criadas instâncias de alguns dos serviços fornecidos pelo Windows Azure para testar esses mecanismos de segurança. As instâncias criadas foram: uma aplicação web, uma máquina virtual e um banco de dados SQL.

  A ferramenta Windows Azure foi escolhida porque ela mostrou-se mais intuitiva, com mais material de apoio, documentação, usabilidade e exigiu menos conhecimento técnico para começar o uso.

4 SOLUÇÕES PARA COMPUTAÇÃO EM NUVEM

Este capítulo apresenta algumas das principais ferramentas que fornecem serviços de Nuvem. É apresentado um resumo comparativo dessas ferramentas. São abordadas também boas práticas de segurança e garantia de privacidade dos dados em Computação em Nuvem.

4.1 Principais Ferramentas disponíveis

Existem muitas soluções para Computação em Nuvem, algumas de uso gratuito e outras pagas. Nesta seção são apresentadas ferramentas que fornecem serviços de Computação em Nuvem.

4.1.1 OpenStack

O OpenStack foi projetado para trabalhar como um ambiente de Infraestrutura como Serviço, ou IaaS, sendo totalmente em código aberto baseado em uma combinação da plataforma de Computação em Nuvem Nebula da Agência Espacial Norte Americana, a NASA, e a plataforma Cloud Files da empresa americana de TI, Rackspace Hosting. O OpenStack vem crescendo à medida que outras 200 empresas das áreas de *software*, *hardware* e serviços começam a se envolver com ele. Além disso, o OpenStack vem ganhando espaço também em algumas distribuições baseadas no sistema operacional Linux, também de código aberto.

A arquitetura por trás do OpenStack conta com os seguintes subprojetos, os quais controlam cada parte do ambiente de Nuvem, tornando o OpenStack mais organizado quanto a distribuição das funções e utilização. Os subprojetos são os seguintes:

- *Infraestrutura de Armazenamento (Swift):* que fornece um repositório de objetos para armazenamento dos dados e conteúdo, sendo extremamente

escalável em tamanho e capacidade. Ele se origina do RackSpace Cloud Files;

- *Gerenciamento de Imagens (Glance):* que controla a descoberta, armazenamento e recuperação das máquinas virtuais, gerenciando as imagens dessas máquinas;

- *Infraestrutura Computacional (Nova):* que fornece os servidores virtuais sob demanda para a utilização das imagens das máquinas virtuais gerenciadas pelo Glance;

- *Armazenamento de Bloco (Cinder):* que fornece armazenamento persistente de bloco para instâncias de computação.

- *Serviço de Rede(Neutron):* que fornece vários serviços de rede para usuários da Nuvem, tais como a gestão de endereços IP, DNS, DHCP, balanceamento de carga e grupos de segurança.

- *Dashboard (Horizon):* responsável pela administração dos modelos, instâncias, recursos e monitoramento de eventos, estado e solução de problemas através de um painel de controle e mecanismos de controle.

- *Heat:* que organiza vários modelos de máquinas virtuais OpenStack, com definições de serviço e servidores prontos para implementação;

Todos esses subprojetos atuam em conjunto, comunicando entre si para gerenciar o ambiente do OpenStack.

O OpenStack oferece dois tipos de implantação, o modelo privado e o público, onde a empresa pode criar seu ambiente de Nuvem em sua própria infraestrutura ou através de fornecedores de serviço.

No quesito segurança, o OpensStack preza para que seus serviços ofereçam confiança ao usuário, porém ele depende de seus colaboradores para correções de segurança, por se tratar de um *software* de código aberto.

A empresa interessada em utilizar o OpenStack precisa ter ciência de que é necessário investir bastante tempo e dinheiro para conseguir uma implementação funcional, porém todo esse gasto, em tempo e dinheiro sairá mais lucrativo quando considerar os investimentos que devem ser feitos em *hardware* principalmente, pois, no OpenStack, a empresa pode contar, além de tudo, com a escalabilidade sob demanda de utilização.

4.1.2 Apache CloudStack

Baseado em software de código aberto, o Apache CloudStack gerencia e organiza grupos de armazenamento, rede e recursos de computador para construir um serviço IaaS de Computação em Nuvem, em Nuvem pública ou privada. O CloudStack suporta a criação de grandes redes de máquinas virtuais, altamente escalável e altamente disponível para implementação de serviços no modelo IaaS. O CloudStack oferece suporte aos principais monitores de máquina virtual como VMware, Hyper-V e KVM e sua API também é compatível com o EC2 e S3 da Amazon AWS (CLOUDSTACK, 2014b).

O CloudStack possuiu uma "Equipe de Segurança" responsável por responder a vulnerabilidades relatadas pelos usuários. Para tanto, essa equipe trabalha com a comunicação com relatório, a verificação do problema, a correção do problema, a criação de uma comunicação pública e a coordenação de fornecedores. Caso necessite, a equipe de segurança pode pedir ajuda de outros membros da comunidade, ajudando na verificação ou correção de algum problema relatado.

Como o CloudStack é um sistema de código aberto, qualquer vulnerabilidade de segurança em alguma versão lançada pode ser denunciada para o e-mail que o Apache CloudStack disponibiliza: security@cloudstack.apache.org, relatando os detalhes encontrados sobre tal vulnerabilidade, como ela pode ser explorada e qualquer detalhe adicional.

Quando recebe aviso de um possível problema, a equipe de segurança entra em ação para tentar resolvê-lo o mais rápido possível. No entanto, ela investiga a questão para confirmar ou negar a existência da vulnerabilidade dentro do CloudStack. Caso confirme, essa equipe atribui uma classificação de risco para a vulnerabilidade usando um *Sistema Comum de Pontuação de Vulnerabilidade*(CLOUDSTACK, 2014a).

4.1.3 Windows Azure

Totalmente hospedado e controlado pela Microsoft, o Windows Azure gerencia o *hardware* disponível em *data centers* da Microsoft a fim de prover máquinas virtuais para serviços online de alta escalabilidade e aplicações com provisionamento dinâmico. O Windows Azure oferece serviços de armazenamento, administração e computação, além de disponibilizar vários serviços para a construção de aplicações distribuídas (MICROSOFT, 2014).

O Windows Azure, assim como outros serviços de Nuvem, vem para simplificar o gerenciamento de tecnologia da informação de forma que se possa minimizar os gastos da empresa. O Windows Azure foi criado para facilitar o gerenciamento de aplicações escaláveis na Internet. Ele fornece ambos os modelos PaaS e IaaS, suportando várias linguagens de programação, ferramentas e *framework*, incluindo sistemas de terceiros.

No quesito segurança, o Windows Azure é gerenciado, monitorado e administrado por uma equipe de operações da Microsoft, pronta para agir em casos de falha na segurança. O Windows Azure possui práticas de segurança nas camadas de aplicativos e plataforma, aprimorando a segurança aos desenvolvedores de aplicativos e administradores de serviços. Dentre os mecanismos de segurança, estão:

- Roteadores de filtragem que ajudam a evitar ataques comuns que usam *drones* ou computadores zumbis para procurar servidores vulneráveis.

- *Firewall* que restringem a comunicação de dados para portas para protocolos e endereços IP de origem e destino desconhecidos e não-autorizados.
- Proteção criptográfica de mensagens de pelo menos 128 *bits* para proteger mensagens de controle enviadas entre *data centers* ou *clusters* de um determinado *data center*.
- Gerenciamento de *patches* de segurança de *software* que ajudam a proteger o sistema contra vulnerabilidades conhecidas.
- Uso de sistemas centralizados de correlação e análise de informações de monitoramento para integrar os mecanismos de segurança e criar barreiras para tráfego não autorizado.
- Uso de criptografia na comunicação entre os usuários finais e as máquinas virtuais na Nuvem.

4.1.4 VMWare vCloud Suite

O VMware vCloud Suite permite a criação e execução de uma Nuvem privada (VMWARE, 2013). O vCloud Suite fornece serviços de IaaS e PaaS.

O vCloud oferece funcionalidades ao provedor de serviços de Nuvem, proporcionando economia em escala, provisionamento de aplicativos em minutos e gerenciamento automatizado de operações.

Os principais benefícios oferecidos pelo vCloud são:

- *Eficiência operacional:* Operações orientadas por políticas administrativas que proporcionam economia ao provedor de serviços.
- *Agilidade da infraestrutura:* Implantação de aplicativos em pouco tempo com provisionamento automático.
- *Controle operacional:* Todos os aplicativos com controle, disponibilidade e segurança ideais para eles.

Há três edições disponíveis pelo vCloud Suite:

- *vCloud Suite Standard:* Solução de base para nuvens privadas para aumentar a agilidade comercial.
- *vCloud Suite Advanced:* Solução para Nuvem privada corporativa administrativa.
- *vCloud Suite Enterprise:* Solução abrangente para Nuvem privada resiliente, segura e em conformidade para todos os aplicativos.

Na questão da segurança, o vCloud Suite disponibiliza o VMWare vCloud Networking and Security, um produto que fornece serviços básicos de rede e funcionalidades de segurança para ambientes de computação virtualizados. Em sua ampla gama de serviços prestados, incluem serviços de rede e de *gateway* de segurança, *firewall*, segurança de dados, entre outros.

4.1.5 Amazon EC2:

Pertencente à plataforma de Computação em Nuvem da Amazon.com e Amazon Web Services (AWS), o EC2 permite ao usuário alugar máquinas virtuais e assim rodar suas próprias aplicações. Provê também um Web *service* no qual o usuário pode utilizar a Amazon Machine Image para criar uma máquina virtual com o *software* que desejar (AMAZON, 2013). O EC2 fornece serviços IaaS e PaaS.

Dentre os sistemas de segurança utilizados para proteger a informação contra ataques cibernéticos, a Amazon Web Services utiliza um serviço que permite ao usuário definir o nível de segurança que ele deseja para o tipo de serviço que vai oferecer.

A rede da AWS provê proteção contra os problemas de segurança mais comuns e o usuário pode também implementar mecanismos de proteção adicionais. Dessa forma, ataques bastante utilizados na Internet são facilmente detectados e evitados logo que o sistema detecta a ameaça, de forma automatizada.

O EC2 possui sistemas de segurança em vários níveis, sendo capazes de interceptar sistemas ou usuários não autorizados que venham a tentar o acesso aos *data centers* e que não prejudiquem a flexibilidade na configuração desejada pelo consumidor.

O EC2 possui várias instâncias de máquinas virtuais sendo executadas ao mesmo tempo em uma máquina, porém todas são isoladas entre si. Isso é possível porque utilizam uma versão altamente customizada do hipervisor Xen. O sistema proprietário de virtualização de disco da AWS restabelece cada bloco de armazenamento utilizado pelo consumidor, assim os dados desse consumidor nunca serão expostos a outros consumidores de forma não intencional.

4.1.6 Resumo Comparativo

Na Tabela 4.1, é apresentado um resumo comparativo das ferramentas estudadas. Nesta tabela, mostra-se quais os modelos de serviço (IaaS, PaaS e SaaS) oferecidos pelas ferramentas, os modelos de implantação (Pública, Privada, Híbrida e Comunitária) que cada uma utiliza, se a licença das ferramentas é gratuita ou paga e quais os tipos de avaliação gratuita oferecidos por cada ferramenta. A avaliação gratuita do Windows Azure compreende todos os serviços oferecidos, já a Amazon oferece uma avaliação com certas restrições.

Tabela 4.1: Resumo das características das ferramentas

Ferramentas	Modelos de Serviço			Modelos de Implantação				Licença		Avaliação gratuita
	IaaS	PaaS	SaaS	Pública	Privada	Híbrida	Comunitária	Gratuita	Paga	
OpenStack	X			X	X			X		N/A
CloudStack	X			X	X			X		N/A
Windows Azure	X	X		X	X				X	US$200/30 dias
vCloud Suite	X	X		X	X	X			X	Não possui
Amazon EC2	X	X		X	X				X	750 horas

4.2 Práticas de Segurança e Garantia de Privacidade

A Computação em Nuvem ainda precisa lidar com questões relacionadas à segurança e privacidade das informações. Muitas organizações temem que a transição para a Nuvem poderia causar danos aos seus dados críticos. No entanto, boas práticas de segurança e garantia da privacidade podem minimizar os riscos inerentes à Nuvem.

Os provedores de Nuvem devem garantir que os recursos de computação são seguros e que o acesso físico às máquinas, como também os dados dos clientes, é restrito e todo acesso ao local deve ser documentado. E o pessoal autorizado precisa ser treinado, de modo que não venha a cometer falhas que poderiam ser evitadas. Desse modo, os riscos inerentes dos dados críticos sendo processados fora da empresa podem ser mitigados.

Os prestadores de serviços de Nuvem são responsáveis pela implantação de procedimentos de segurança operacional, incluindo controles de segurança em Nuvem, documentação de operações, aliados a opções de segurança como a criptografia ou biometria. Também são necessárias outras medidas de segurança, tais como auditoria, monitoramento e registros de eventos. Essas providências podem evitar alguma falha na Nuvem que possa potencializar um ataque aos dados de todos os usuários que estão de forma compartilhada na Nuvem.

Os dados na Nuvem são armazenados em servidores físicos espalhados pelo mundo. Estes servidores estão sujeitos a falhas operacionais, desastres naturais e outros fatores que podem acarretar a suspensão do funcionamento desses servidores. Por isso, os prestadores de serviços de Nuvem devem contar com um plano de continuidade de negócios e também planos contra desastres. A realização de *backups* periodicamente pode facilitar a recuperação desses dados em caso de desastres ou problemas operacionais.

Atividades ilegais também podem acontecer na Nuvem, mas torna-se difícil o processo de investigação pois os registros podem estar armazenados em vários servidores, de vários países, com legislações diferentes. O ideal é que exista um compromisso contratual onde a empresa dará suporte às investigações criminais quando forem necessárias. Para que este suporte possa ser efetuado, os provedores desses serviços devem realizar registro de eventos para uma eventual auditoria, sendo que esses registros precisam estar devidamente protegidos e acessíveis para investigação forense.

O acesso aos dados deve ser autenticado, de forma que não haja vulnerabilidade de acesso. É preciso proteger os locais onde estão situados os servidores. Essa proteção deve ser realizada através de sistemas e procedimentos de segurança, pois a vulnerabilidade destes locais podem ocasionar roubos, riscos a integridade dos dados entre outros problemas.

Para os aplicativos que forem hospedados e utilizados na Nuvem, valem as mesmas regras de boas práticas de programação utilizadas para *software* tradicionais. Com isso, é possível diminuir a chance de um ataque feito por um *hacker* ou programas maliciosos.

A empresa precisa garantir a privacidade dos seus clientes. Dados sendo minerados e usados de forma ilícita podem violar segredos empresariais, dados pessoais, entre outros dados críticos.

A falta de um padrão para a prestação de serviços em Nuvem dificulta a compatibilidade em relação aos dados armazenados na Nuvem por terceiros. A conformidade com regulamentações pode trazer mais confiabilidade aos serviços de Nuvem. O CSA (*Cloud Security Alliance*) é uma organização que promove a utilização das melhores práticas de segurança dentro da Computação em Nuvem (ALLIANCE, 2014). Esta organização tem como membros as maiores fornecedoras de Nuvem e oferece também várias certificações relacionas à segurança. Ou

seja, a Computação em Nuvem começa a tomar forma no quesito segurança e privacidade dos dados.

Na próxima seção, é apresentado um estudo de caso com a ferramenta Windows Azure para testar os mecanismos de segurança fornecidos.

5 ESTUDO DE CASO

Foi realizado um estudo de caso com a ferramenta da Microsoft, o Windows Azure, para verificar os mecanismos de segurança oferecidos. Foram realizados testes que possibilitaram verificar funcionalidades e mecanismos de segurança da ferramenta.

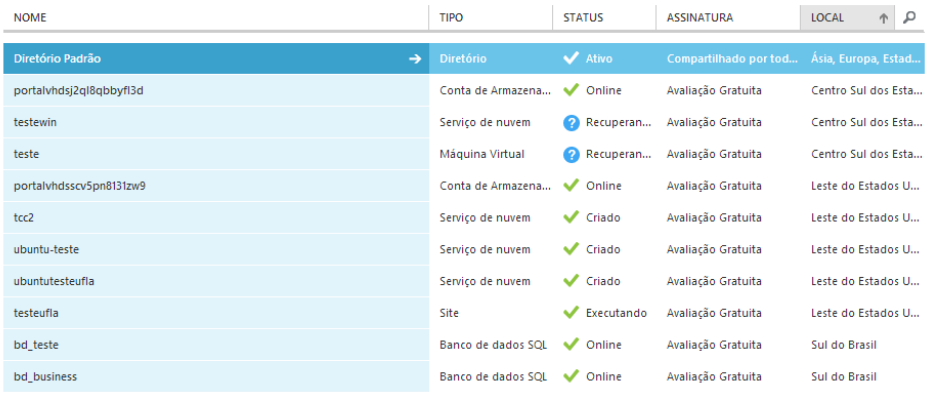
A Microsoft oferece um crédito de US$200 para que o usuário, em caráter de experimentação, possa usufruir dos serviços que são pagos. Para ter acesso ao serviço Windows Azure, é necessário ter uma conta da Microsoft e em poucos minutos o ambiente do Windows Azure é disponibilizado, com uma interface amigável e intuitiva.

O serviço oferece uma aplicação web, na qual pode ser feita a utilização e configuração dos serviços. O acesso ao portal de gerenciamento pode ser feito por qualquer navegador de qualquer sistema operacional. Tanto o acesso ao portal quanto o acesso às máquinas virtuais utilizam os protocolos SSH (*Secure Shell*) ou RDP (*Remote Desktop Protocol*).

O usuário pode escolher qual tipo de serviço quer usufruir, entre eles, aplicações web, máquinas virtuais e bancos de dados. Na Figura 5.1, é ilustrada a interface do portal de gerenciamento do Windows Azure, com as instâncias dos serviços criados neste estudo de caso. Além do tipo e status dos serviços criados, a figura também ilustra o local, isso porque a ferramenta permite a escolha da localização física do *data center* onde os serviços são instanciados.

Um outro recurso importante é que a ferramenta permite uma análise dos gastos dos serviços utilizados, como pode ser observado na Figura 5.2. Por exemplo, pode-se verificar separadamente gastos com a transferência de dados, armazenamentos de dados e horas de processamentos. Isso é importante para que uma empresa possa ter um controle dos seus gastos e planejar a alocação de serviços.

Nas seções a seguir, são descritos os serviços que foram criados no Windows Azure e os mecanismos de segurança testados sobre cada um desses serviços.



NOME	TIPO	STATUS	ASSINATURA	LOCAL
Diretório Padrão	Diretório	Ativo	Compartilhado por tod...	Ásia, Europa, Estad...
portalvhdsj2ql8qbbyfl3d	Conta de Armazena...	Online	Avaliação Gratuita	Centro Sul dos Esta...
testewin	Serviço de nuvem	Recuperan...	Avaliação Gratuita	Centro Sul dos Esta...
teste	Máquina Virtual	Recuperan...	Avaliação Gratuita	Centro Sul dos Esta...
portalvhdsscv5pn8131zw9	Conta de Armazena...	Online	Avaliação Gratuita	Leste do Estados U...
tcc2	Serviço de nuvem	Criado	Avaliação Gratuita	Leste do Estados U...
ubuntu-teste	Serviço de nuvem	Criado	Avaliação Gratuita	Leste do Estados U...
ubuntutesteufla	Serviço de nuvem	Criado	Avaliação Gratuita	Leste do Estados U...
testeufla	Site	Executando	Avaliação Gratuita	Leste do Estados U...
bd_teste	Banco de dados SQL	Online	Avaliação Gratuita	Sul do Brasil
bd_business	Banco de dados SQL	Online	Avaliação Gratuita	Sul do Brasil

Figura 5.1: Interface do portal de gerenciamento do Windows Azure.

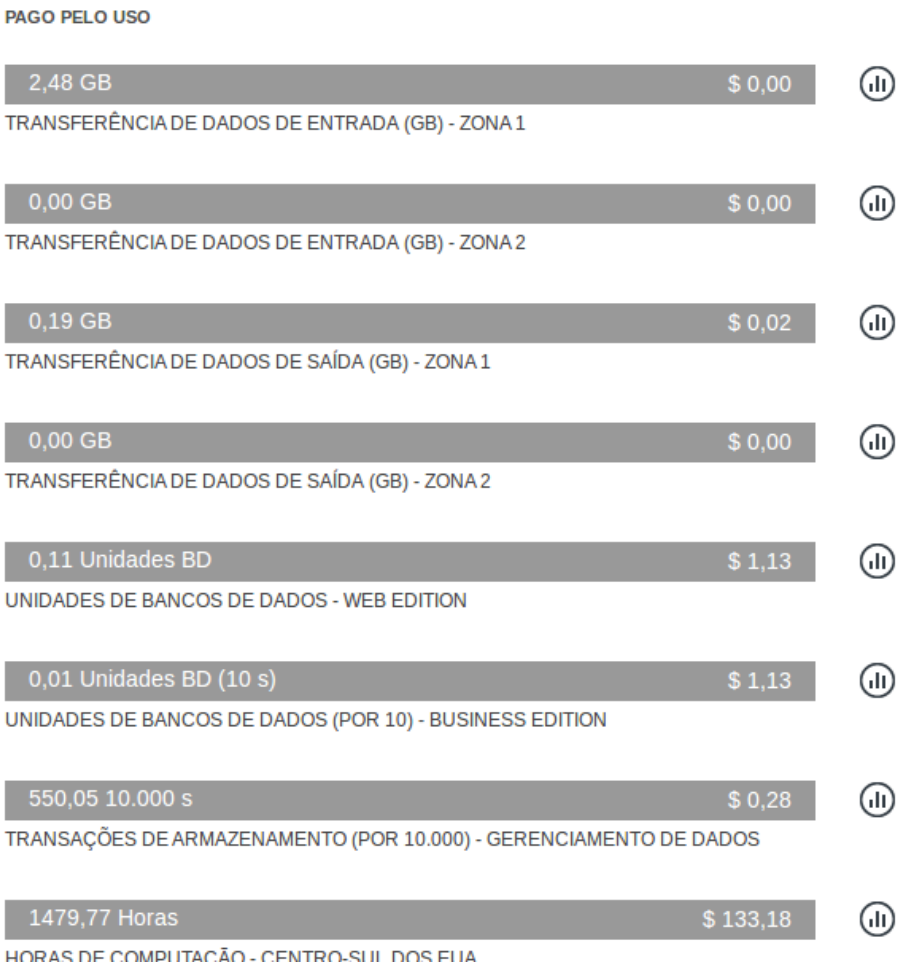


Figura 5.2: Relatório de gastos do serviços utilizados.

5.1 Ambiente Operacional do Azure

O Windows Azure permite a criação de vários serviços. Podem ser criadas várias instâncias de cada um desses serviços simultaneamente sem vínculos entre si. Todos esses serviços podem ser gerenciados através de uma aplicação web. Essa aplicação web oferece todas funções de gerenciamento em um único portal web, onde são feitas as configurações do serviços e controles de acesso. Essas configurações de acesso podem ser realizadas através do ponto de extremidade. Esse ponto de extremidade é caracterizado por um serviço de rede associado à uma porta, como, por exemplo, o PowerShell com o protocolo SSH na porta 5986.

Um dos serviços oferecidos é a criação das máquinas virtuais. Em cada máquina virtual, existe uma gama de sistemas operacionais que podem ser instalados, por exemplo, o Windows Server 2012 e 2008 e diversas distribuições Linux, como o Ubuntu, CentOS e openSUSE.

Neste estudo de caso, foram criadas instâncias dos seguintes serviços: uma aplicação web, uma máquina virtual e um banco de dados SQL. As subseções seguintes descrevem cada um desses serviços criados.

5.1.1 Aplicação Web

O Windows Azure oferece várias opções para criação de aplicações web e portais de conteúdo. Para portais de conteúdo são oferecidos suporte para o WordPress e Joomla. Existem ainda *templates* para a criação de várias aplicações web em diversas linguagens como PhP, ASP.NET, Node.js e HTML5.

No painel de gerenciamento, é possível monitorar todo o acesso e administração das páginas e do banco de dados da aplicação web. Na Figura 5.3, mostra-se este painel de monitoramento. Neste painel é possível acompanhar o monitoramento em tempo real do website e do servidor onde este está hospedado. Esse monitoramento consiste no número de acessos ao website, erros do servidor

HTTP, tempo de utilização de CPU e entrada e saída de dados do servidor. Com isso, o usuário tem um melhor controle do seu website, podendo aumentar a capacidade do servidor manualmente caso sinta necessidade do mesmo. É através deste painel de monitoramento que são gerenciadas as características da aplicação web criada. São oferecidos os seguintes planos de hospedagem: Grátis, Compartilhado, Básico e Padrão, que possuem diferentes conjuntos de recursos e funcionalidades. Os planos Padrão e Básico são os mais completos, com recursos dedicados aos sites e menos restrições em relação às funcionalidades disponíveis.

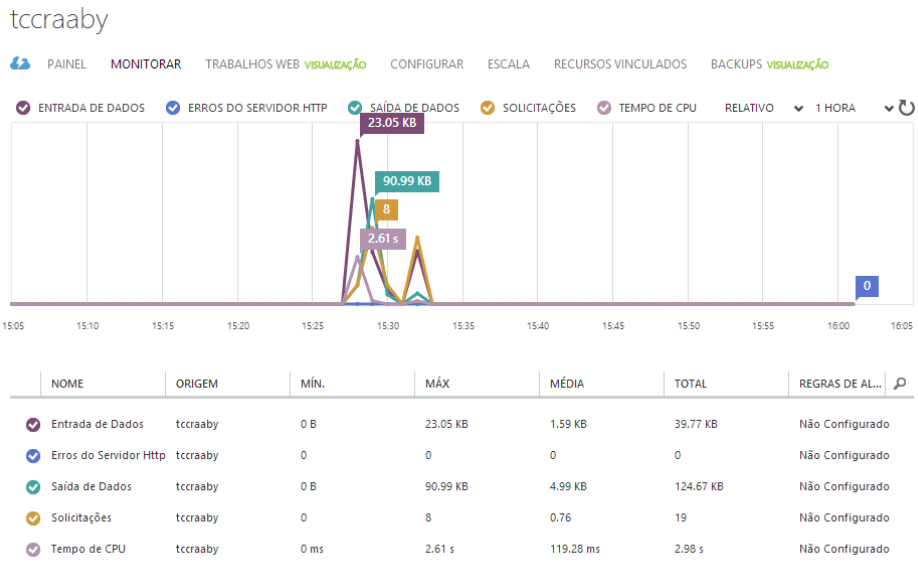


Figura 5.3: Painel de monitoramento.

Para este estudo de caso, foi criado um website utilizando o WordPress no plano de hospedagem Grátis. Em poucos minutos, o website já estava disponível para utilização. O website encontra-se no endereço tccraaby.azurewebsites.net. Na Figura 5.4, mostra-se o site que foi criado. Uma das principais vantagens da ferramenta, é que uma instituição pode criar um website ou uma aplicação web de maneira rápida com todas funcionalidades integradas. Entre essas funcionali-

dades podemos destacar: criação e design, controle e monitoramento do acesso ao recurso, hospedagem e custos envolvidos.

Figura 5.4: Site WordPress.

5.1.2 Máquina Virtual

No Windows Azure, é possível criar várias máquinas virtuais a partir de diversas imagens de sistemas operacionais disponíveis. Além disso, é possível escolher dentre dez modelos de *hardware* para a máquina virtual. O modelo de *hardware* mais simples consiste em um núcleo de processamento compartilhado e 768 MB de memória RAM. O modelo mais complexo conta com um processador com 16 núcleos e 112 GB de memória RAM.

O valor cobrado para cada máquina é proporcional à capacidade de processamento e memória da máquina. Também é possível definir a região onde estará localizado o servidor da máquina virtual. Durante a criação da máquina virtual, por padrão, já são definidos alguns pontos de extremidade, por exemplo, serviços de rede com os protocolos de acesso *Remote Desktop* e PowerShell nas portas 3389 e 5986, respectivamente. No entanto, a qualquer momento, o usuário pode gerenciar os pontos de extremidade, acrescentando novos ou excluindo os existentes de acordo com suas necessidades.

Para este estudo de caso, foi criada uma máquina virtual utilizando o Windows Server 2012, com 2 núcleos e 3,5 GB de memória RAM. Na Figura 5.5, mostra-se o painel de configuração da máquina virtual. Neste painel, estão disponíveis as seguintes funções de gerenciamento: monitoramento de acesso, gerenciamento dos pontos de extremidade, controle de acesso dos clientes, configuração da capacidade de processamento, entre outros. Estes recursos permitem uma avaliação detalhada do uso do espaço em disco, quantidade de dados transmitidos, entre outros. Enfim, as empresas clientes tem um amplo controle para reconfigurar suas máquinas virtuais. Além disso, elas podem fazer um diagnóstico completo do uso dessas máquinas, e assim, alocar e liberar recursos de acordo com a demanda atual.

Para acessar a máquina virtual, o Windows Azure oferece a opção de conexão de área de trabalho remota. Para isso, é disponibilizado um arquivo do tipo RDP (*Remote Desktop Protocol*), através do qual é possível ter acesso ao ambiente

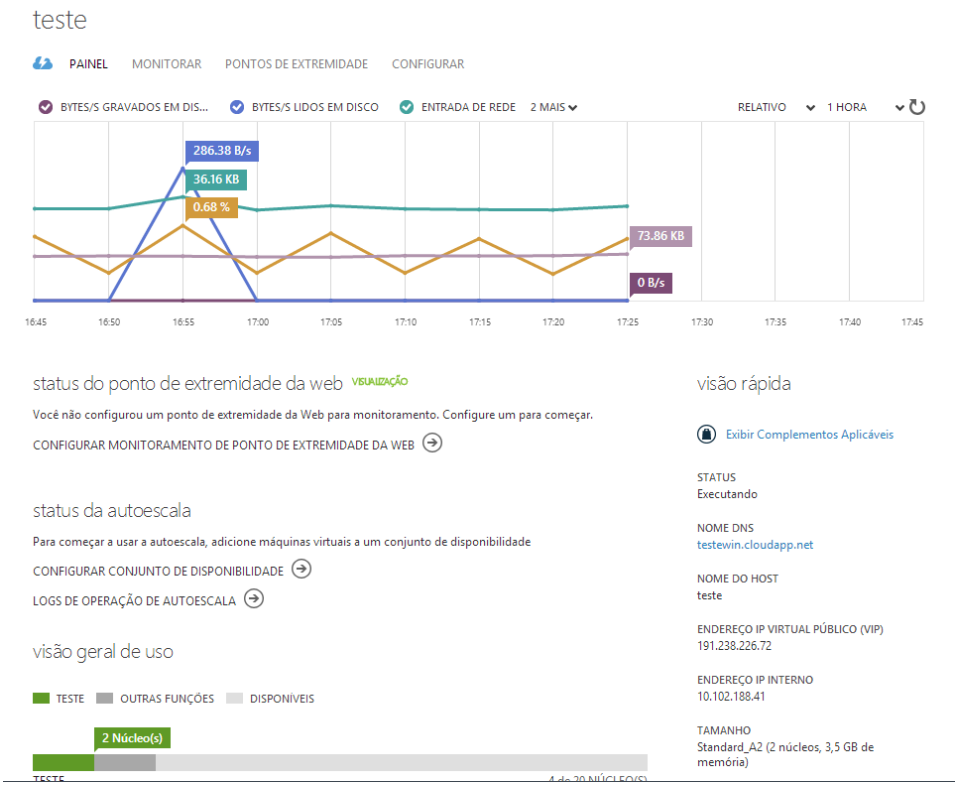


Figura 5.5: Painel de configuração da máquina virtual.

gráfico da máquina virtual. Na Figura 5.6, mostra-se o ambiente gráfico da máquina virtual criada. Este ambiente gráfico serve tanto para acessar o *desktop* e os aplicativos instalados na máquina virtual (como ilustrado na Figura 5.7), quanto para usar o ambiente de gerenciamento da própria máquina. Esse ambiente compreende funcionalidades como a adição de funções e recursos ao sistema, bem como atalhos para configurações gerais do sistema operacional.

Com a máquina virtual criada, e o RDP fornecido, tem-se o acesso ao Windows Server 2012. Foi criada uma aplicação web que consiste em uma calculadora simples feita em HTML, JavaScript e CSS, hospedada na máquina virtual. Na Figura 5.8, mostra-se a interface dessa aplicação.

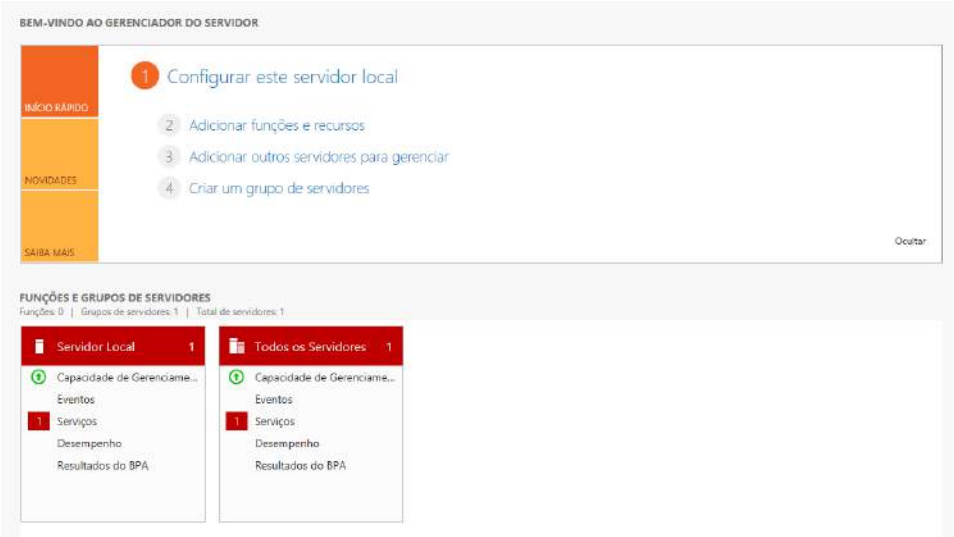


Figura 5.6: Ambiente de gerenciamento da máquina virtual.

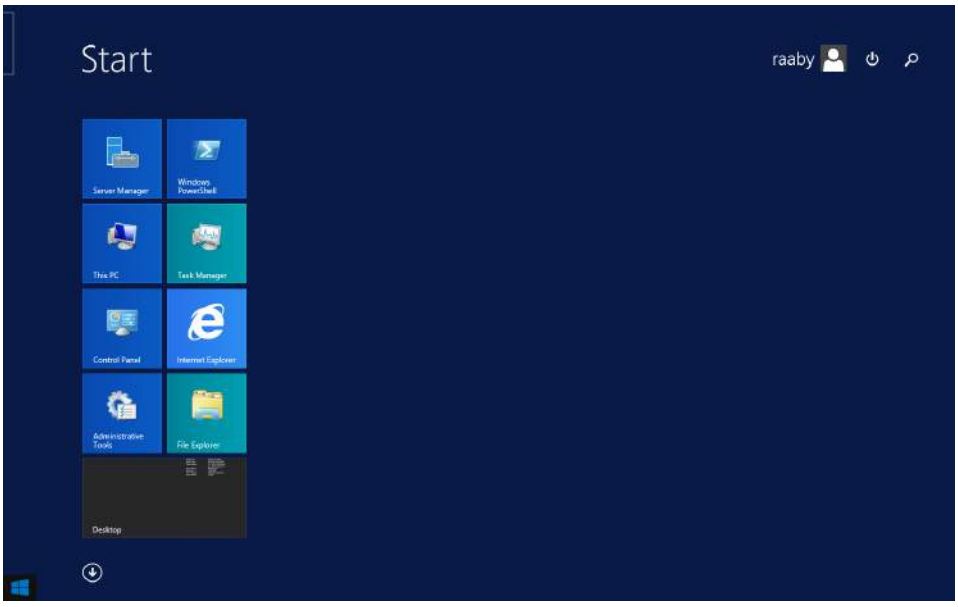


Figura 5.7: Desktop da máquina virtual.

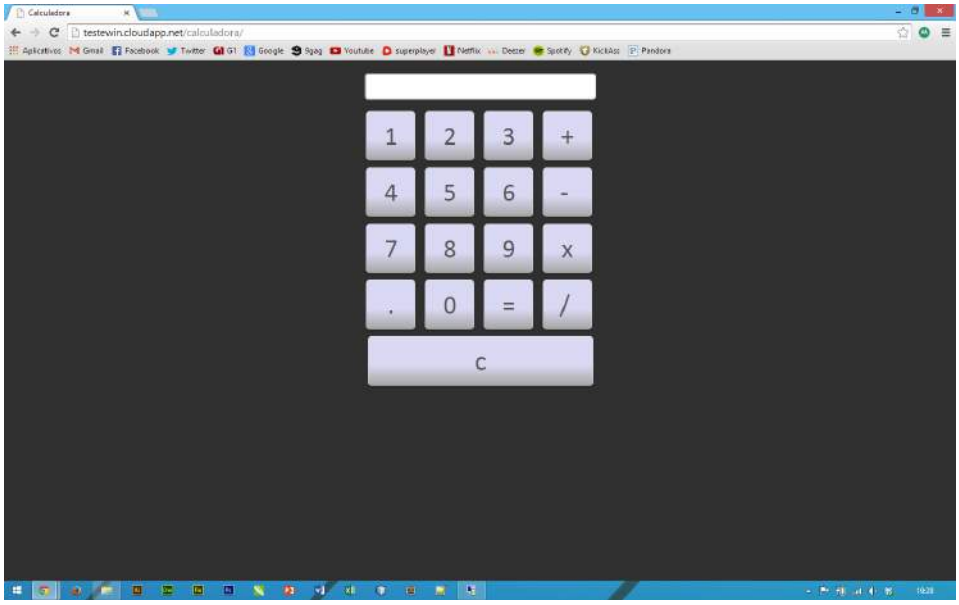


Figura 5.8: Aplicação Web

5.1.3 Banco de Dados

O Windows Azure oferece no portal de gerenciamento a opção de criação de um Banco de Dados SQL. É possível definir o tipo do banco de dados (Web e Business), bem como o tamanho máximo desejado para o banco de dados. É possível também escolher se deseja utilizar um servidor específico para o banco de dados que já exista ou criar um novo. Para o gerenciamento do banco de dados, o Windows Azure fornece um portal de gerenciamento online hospedado no servidor criado. Nesse portal é possível importar ou criar um banco de dados a partir de um *script*. Uma outra alternativa, é uma ferramenta gráfica onde é possível criar tabelas na base de dados sem a necessidade de editar o código SQL. Essa alternativa consiste em criar campos, definir seus tipos e tamanhos e preencher os dados manualmente.

Para este estudo de caso, foi criado um banco de dados do tipo Web, com 1 GB de tamanho máximo. Foi criada uma tabela simples utilizando o próprio portal de gerenciamento, com quatro campos (ID, Nome, Endereço e Telefone). A figura 5.9 ilustra a tabela com três tuplas criadas com dados arbitrários para demonstração do banco de dados.

Figura 5.9: Tabela de banco de dados.

5.2 Mecanismos de Segurança

A partir dos serviços criados conforme descrito na seção anterior, foi possível testar mecanismos de segurança do Windows Azure.

Foram avaliados os seguintes mecanismos de segurança: controle de acesso, armazenamento seguro e transporte seguro dos dados. Esses mecanismos são descritos nas subseções subsequentes.

5.2.1 Controle de Acesso

No caso da aplicação web, não foi possível obter nenhum resultado relacionado ao controle de acesso. Pois na criação do website, foi utilizado o plano Grátis, e o controle de acesso não está disponível nesse modo.

No caso da máquina virtual Windows Server 2012, foram definidos pontos de extremidades para liberar o acesso das portas. Os pontos escolhidos foram SSH, Remote Descktop, PowerShell, HTTP e HTTPS. Dentro de cada ponto de extremidade é possível definir regras de permissão e negação por meio de listas de controle de acesso (ACL). A Figura 5.10 mostra essa lista de controle realizado na aplicação Web que foi hospedada na máquina virtual criada.

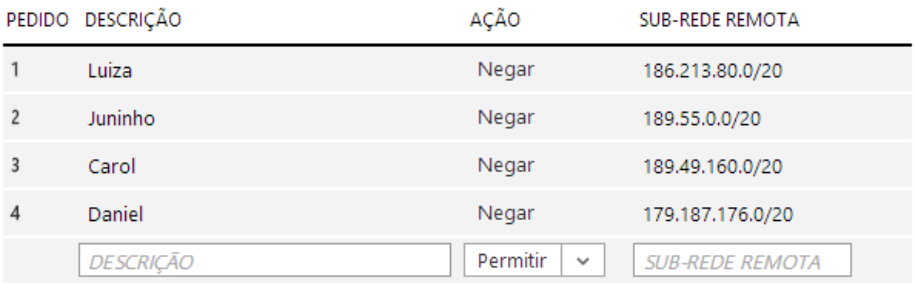


Figura 5.10: Lista de bloqueio de Ips.

O teste foi realizado da seguinte maneira. Primeiramente, foram liberados todos os IPs. A partir disso, alguns IPs foram escolhidos para que pudessem ser bloqueados, com isso, esses IPs não conseguiram acesso à essa aplicação.

Mas, utilizando um *proxy* para camuflar o IP real, foi possível acessar a aplicação mesmo com o IP bloqueado. Ou seja, não é correto fazer o controle negando o acesso para alguns IPs, o mais apropriado é negar para todos e permitir o acesso somente aos interessados. Para isso, foi feito um segundo teste para um controle mais efetivo. Neste teste, a aplicação foi bloqueada para todos, através do IP 0.0.0.0/0 e permitido para alguns IPs. Mas, para que esses IPs liberados pudessem ter acesso à aplicação, foi necessário seguir a regra de precedência. Nessa regra vale a ordem que estão os IPs na lista, ou seja, a ordem de execução será do primeiro item da tabela ao último. Na Figura 5.11 mostra-se a lista ACL do segundo teste.

PEDIDO	DESCRIÇÃO	AÇÃO	SUB-REDE REMOTA
1	Raaby	Permitir	177.44.48.74/31
2	Luiza	Permitir	186.213.80.54/31
3	Junior	Permitir	189.55.51.89/31
4	Todos	Negar	0.0.0.0/0
	DESCRIÇÃO	Permitir	SUB-REDE REMOTA

Figura 5.11: Lista ACL.

Além do controle de acesso dos pontos de extremidades, podem ser instaladas outras opções de controle de acesso no próprio sistema operacional, como por exemplo *firewall* do Windows dentro da máquina virtual.

No caso do banco de dados SQL, só é permitido o acesso ao portal de gerenciamento do banco de dados quando o IP é adicionado à lista de endereços de IP permitidos, caso contrário o *firewall* bloqueia o acesso. A Figura 5.12, mostra essa lista de IPs permitidos. Na Figura 5.13, mostra-se a tentativa de acesso e o bloqueio à essa tentativa ao servidor do banco de dados através de um IP não adicionado à lista de permissão.

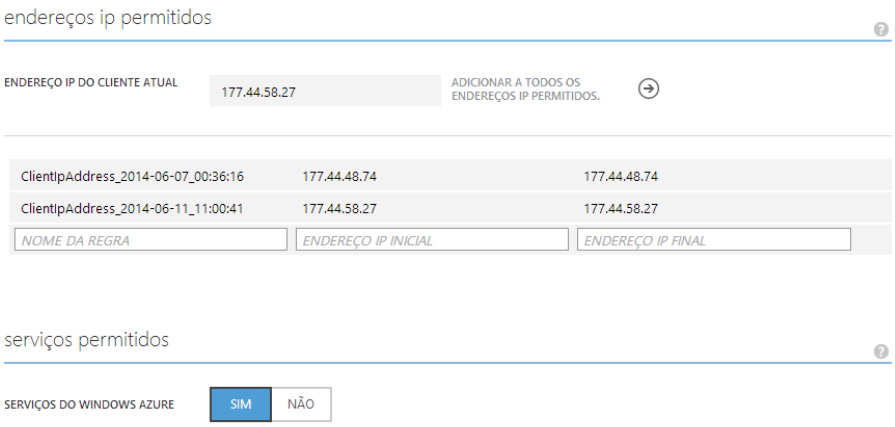


Figura 5.12: Endereços de IPs permitidos.

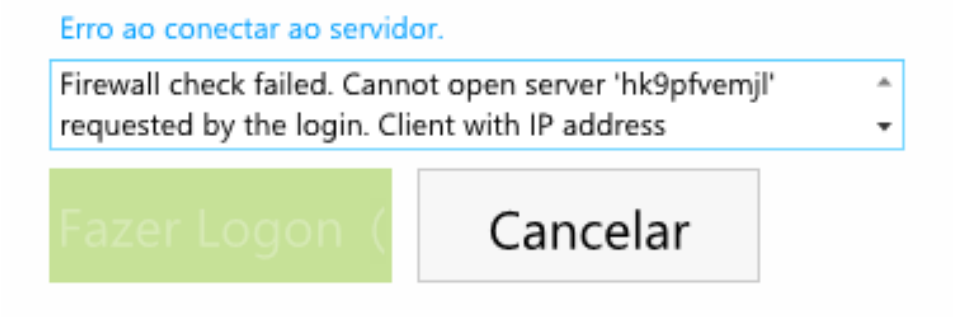


Figura 5.13: Acesso negado ao banco de dados.

5.2.2 Armazenamento Seguro

Nas três instâncias de serviços criadas, o Windows Azure não implementa armazenamento seguro de dados através de criptografia. Pois, a criptografia no Azure não é nativa, ou seja, caso o usuário queira criptografar os seus dados, ele precisa utilizar ferramentas com essa finalidade.

Uma opção que o Windows Azure fornece para o armazenamento seguro dos dados são os contêineres que fornecem um agrupamento lógico para os arquivos presentes nos armazenamentos criados no Azure, que contém por exemplo um VHD (*Virtual Hard Disk*) de uma máquina virtual.

A máquina virtual no Azure é uma máquina como qualquer outro *host*. Então, quando se fala de máquina virtual toda segurança dos dados precisa ser feita pelo próprio usuário, tal qual é feito em um sistema operacional em uma máquina física. Dois mecanismos que podem aumentar a segurança dos dados armazenados na Nuvem, é o Bitlocker, um programa de criptografia presente no Windows, que codifica as partições inteiras do HD e o EFS (*Encrypting File System*) que criptografa arquivos individualmente.

5.2.3 Transporte Seguro de Dados

Em ambos os casos, na aplicação web e no servidor do banco de dados, o Windows Azure oferece conexão segura de dados através do protocolo SSL (*Secure Socket Layer*) para conexão com os seus aplicativos.

Os aplicativos do Windows Azure que estão disponíveis para acesso externo, ou seja, fora do portal de gerenciamento, possuem conexão segura ativada por padrão, sem a necessidade de interferência do usuário. Os dados devem ser criptografados antes de serem transferidos entre usuários clientes e os *data centers* da Microsoft. Essa combinação de transporte e armazenamento seguro garante um nível aceitável de privacidade e segurança.

6 CONCLUSÃO

Os avanços tecnológicos dos últimos anos, proporcionaram um crescimento da utilização dos serviços de Computação em Nuvem. A ideia de não precisar investir em infraestrutura computacional, podendo alugar este serviço e pagar apenas pelo que usar, tornou-se atrativa para usuários e organizações, principalmente pequenas e médias empresas.

A Computação em Nuvem oferece muitos benefícios além do pagar apenas pelo uso. A elasticidade rápida, onde o sistema realiza de forma automática a alocação de recursos de acordo com a necessidade do momento, utilizando a virtualização, proporciona ao usuário a impressão de que ele possui recursos infinitos.

Mas, mesmo diante de tantos benefícios oferecidos, há um certo receio das organizações na transição de seus dados para a Nuvem em relação à segurança e privacidade destes, já que esses dados seriam armazenados por terceiros.

Este trabalho abordou as questões que envolvem segurança e privacidade dos dados em Computação em Nuvem e como boas práticas de segurança e garantia de privacidade pode melhorar a utilização dos serviços de Nuvem.

Como foi abordado, os riscos de segurança de serviços em Nuvem se tornam complexos no ambiente computacional. Muitos desses riscos decorrem do fato de que os dados estão espalhados por vários servidores no mundo todo. Além disso, dados de diferentes usuários são compartilhados no mesmo servidor. Outro fator é a falta de uma padronização dos serviços oferecidos.

Com o estudo de caso, foi possível estudar serviços, funcionalidades e mecanismos de segurança oferecidos pelo Windows Azure que está entre as principais ferramentas do mercado de implementação de serviços na Nuvem.

Pode-se concluir com o estudo de caso, que as empresas ainda não prezam tanto por segurança e privacidade dos dados. O objetivo da prestadora de serviço em questão é disponibilizar os serviços de Nuvem, a facilidade para se obter esses serviços a baixo custo e de maneira rápida, sem oferecer um nível adequado de

segurança e privacidade de dados críticos, já que a criptografia não é oferecida por ela.

Devido a acontecimentos recentes de espionagem e falhas de segurança até mesmo em dados criptografados, as empresas fornecedoras de serviços de Computação em Nuvem devem começar a tomar medidas para prevenir casos semelhantes no futuro.

Mesmo com os riscos de segurança e privacidade em Computação em Nuvem, são inegáveis as vantagens da utilização dos serviços oferecidos. E são essas vantagens que estão atraindo muitas organizações, mesmo diante desses riscos, para este novo paradigma computacional.

6.1 Trabalhos Futuros

Como visto neste trabalho, a Computação em Nuvem vem ganhando cada vez mais espaço. Mas ainda há muito o que melhorar, principalmente no que diz respeito à segurança e privacidade dos dados. Para tanto, é necessário estudos mais elaborados sobre esse novo paradigma.

Como trabalhos futuros, propõe-se:

- *Estudar novas ferramentas*. Pesquisar e estudar outras ferramentas que fornecem serviços de Computação em Nuvem.

- *Projetar uma arquitetura de solução integrada para a segurança*. Essa solução consiste em uma integração da segurança do armazenamento dos dados nos modelos de implantação, com a segurança das transmissões dos dados nos modelos de serviço e com a segurança das aplicações e segurança relacionadas a recursos de terceiros nas características essenciais da Nuvem. Dessa forma, pode-se reduzir os riscos de segurança e privacidade da Computação em Nuvem.

- *Realizar estudo de caso para avaliar soluções de implantação de uma infraestrutura para serviços de Computação em Nuvem.* Realizar um estudo de caso para a implantação de uma Nuvem que ofereça serviços IaaS e PaaS. Após este estudo de caso, realizar uma comparação com a ferramenta Windows Azure.

REFERÊNCIAS BIBLIOGRÁFICAS

ALLIANCE, C. S. *Cloud Security Alliance*. 2014. Site. Acessado em Maio de 2014. Disponível em: https://cloudsecurityalliance.org.

AMAZON. *Amazon Web Services: Overview of Security Processes*. 2013. PDF. Acessado em Janeiro de 2014. Disponível em: http://awx.amazon.com/security/.

BRIAN, H.; BRUNSCHWILER, T.; DILL, H.; CHRIST, H.; FALSAFI, B.; FISCHER, M.; GRIVAS, S. G.; GIOVANOLI, C.; GISI, R. E.; GUTMANN, R. *et al.* Cloud computing. *Communications of the ACM*, v. 51, n. 7, p. 9–11, 2008.

BRODKIN, J. *Gartner: Seven cloud-computing security risks*. 2008.

CARNEIRO, R. J. G.; RAMOS, C. A segurança na preservação e uso das informações na computação nas nuvens. *João Pessoa*, 2010.

CLOUDSTACK, A. *Apache CloudStack: Security*. 2014. Site. Acessado em Janeiro 2014. Disponível em: http://cloudstack.apache.org/security.html.

CLOUDSTACK, A. *CloudStack Documentation*. 2014. PDF. Acessado em Janeiro de 2014. Disponível em: http://docs.cloudstack.apache.org/en/latest/concepts.html.

DELL. A história e o futuro da computação em nuvem. 2013. Acessado em Novembro de 2013. Disponível em: http://www.dell.com/learn/br/pt/brbsdt1/sb360/social_cloud.

DRIVE, A. C. *Amazon Cloud Drive*. 2014. Site. Acessado em Janeiro 2014. Disponível em: https://www.amazon.com/clouddrive/home/.

DROPBOX. *Dropbox*. 2014. Site. Acessado em Janeiro de 2014. Disponível em: https://www.dropbox.com/.

DUFFANY, J. L. Cloud computing security and privacy. In: *10th Latin American and Caribbean Conference for Engineering and Technology*. [S.l.: s.n.], 2012. p. 1–9.

G1. *Entenda o caso de Edward Snowden, que revelou espionagem dos EUA*. 2013. Site. Acessado em Novembro de 2013. Disponível em: http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html.

KHAN, A.; OTHMAN, M.; MADANI, S.; KHAN, S. A survey of mobile cloud computing application models. IEEE, 2013.

MELL, P.; GRANCE, T. The nist definition of cloud computing (draft). *NIST special publication*, v. 800, n. 145, p. 7, 2011.

MICROSOFT. *Microsoft Windows Azure*. 2014. Acessado em Janeiro de 2014. Disponível em: http://azure.microsoft.com/pt-br/.

MORENO-VOZMEDIANO, R.; MONTERO, R. S.; LLORENTE, I. M. Key challenges in cloud computing: Enabling the future internet of services. *Internet Computing, IEEE*, IEEE, v. 17, n. 4, p. 18–25, 2013.

NIST. *National Institute of Standards and Technology*. 2014. Site. Acessado em Janeiro 2014. Disponível em: www.nist.gov.

OLIVEIRA, W. *Técnicas para hackers e soluções para segurança: versão 2*. [S.l.]: Centro Atlantico, 2003.

PETNEWS. História da computação. 2012. Acessado em Novembro de 2013. Disponível em: http://www.dsc.ufcg.edu.br/~pet/jornal/agosto2012/materias/historia_da_computacao.html.

SOUSA, F. R.; MOREIRA, L. O.; MACHADO, J. C. Computação em nuvem: Conceitos, tecnologias, aplicações e desafios. *III Escola Regional de Computação Ceará-Maranhão-Piauí, ERCEMAPI*, v. 1, 2009.

SUBASHINI, S.; KAVITHA, V. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, Elsevier, v. 34, n. 1, p. 1–11, 2011.

VAQUERO, L. M.; RODERO-MERINO, L.; CACERES, J.; LINDNER, M. A break in the clouds: towards a cloud definition. *ACM SIGCOMM Computer Communication Review*, ACM, v. 39, n. 1, p. 50–55, 2008.

VIRTUALBOX. *VirtualBox*. 2013. Site. Acessado em Novembro de 2013. Disponível em: https://www.virtualbox.org/.

VMWARE. *vCenter Sever*. 2013. Site. Acessado em Novembro de 2013. Disponível em: http://www.vmware.com/br/products/vcenter-server/.

VMWARE. *VMware vCloud Suite Datasheet*. 2013. PDF. Acessado em Janeiro de 2014. Disponível em: http://www.vmware.com/files/br/pdf/products/vCloud/VMware-vCloud-Suite-Datasheet.pdf.

VMWARE. *VSphere ESX and ESXi Info Center*. 2013. Site. Acessado em Novembro 2013. Disponível em: http://www.vmware.com/br/products/esxi-and-esx/overview.html.

XEN. *XEN*. 2013. Site. Acessado em Novembro 2013. Disponível em: http://www.xenproject.org/.

XIAO, Z.; XIAO, Y. Security and privacy in cloud computing. *Communications Surveys & Tutorials, IEEE*, IEEE, v. 15, n. 2, p. 843–859, 2013.