PROSPECTUS
ISSN 2674-8576 Gestão e Tecnologia

Artigo Original

COMPUTAÇÃO EM NUVEM: ANÁLISE DA SEGURANÇA PARA NUVENS PÚBLICAS

CLOUD COMPUTING: SECURITY ANALYSIS FOR PUBLIC CLOUDS

Márcio Luiz Lippi[1]; Maria Cristina Aranda[2]; Pedro Domingos Antoniolli[3]

1- *Graduado em Tecnologia da Segurança da Informação pela FATEC de Americana; 2- Docente da FATEC de Americana; 3- Docente titular da FATEC de Itapira "Ogari de Castro Pacheco";* docente do Programa de Pós-Graduação em Administração *stricto sensu* da Universidade Metodista de Piracicaba - UNIMEP e *pro tempore* na Diretoria de Pequisa e Pós-Graduação da UNIMEP

Contato: pedroantoniolli@yahoo.com.br

RESUMO

Esta pesquisa propõe o estudo das vantagens da computação em nuvem, auxiliando o futuro administrador a gerenciar os recursos disponíveis pela *cloud* e prover conhecimento sobre as ofertas de serviços oferecidos pelos principais provedores de computação em nuvem. O objetivo foi explorar os conceitos básicos de virtualização, que é a fundação para a computação em nuvem, e as vantagens que a computação em nuvem tem a oferecer. O mercado de *cloud* está em crescimento e existem muitas oportunidades de negócio à serem feitas. Atualmente, as maiores companhias que estão no mercado de cloud são: Amazon, Microsoft, Google and IBM. A abordagem de cloud irá se expandir por conta dos benefícios oferecidos. Entre as vantagens que *cloud* tem a oferecer, pode-se destacar a economia, eficiência, automação, elasticidade e escalabilidade. Pela sua facilidade de uso, escalabilidade, e integração, são alternativas tecnológicas importantes para as MPEs (Micro e Pequenas Empresas). No entanto, a questão da segurança da informação deve ser devidamente equacionada, pois dependendo de como são configuradas tais nuvens públicas, podem colocar em risco as informações corporativas.

Palavras-chave: Nuvem. Virtualização. Vmware. Hyper V. AWS. Azure. Softlayer.

PROSPECTUS
ISSN 2674-8576 Gestão e Tecnologia

Artigo Original

ABSTRACT

This research proposes the study of the advantages in cloud computing, helping the administrator to manage the cloud resources and provide knowledge about the services offered by main cloud providers.The main objective was to explore basic concepts of the vitualization, which is the foundation for cloud computing, and the advantages that cloud computing have to offer. The cloud market is growing and there are a lot of business opportunities to be made. Currently, the biggest companies that are in the cloud market are: Amazon, Microsoft, Google and IBM. Cloud solutions will expand due to its many benefits offerred. Among all advantages that cloud has to offer, we could highlight the savings, efficiency, automation and elasticity. Due to its facilities, scalability, and integration, cloud solutions become interesting alterantives for SBE (Small Business Enterprises). However, information security is a question that should be properly addressed because, depending on the public cloud configuration, they can put in risk corporative informations.
Keywords: Cloud. Virtualization. Vmware. Hyper V. AWS. Azure. Softlayer.

INTRODUÇÃO

Estamos vivendo um momento importante em termos da acessibilidade e disponibilidade da informação, com acesso imediato e instantâneo a muitos dados.

A infraestrutura que suporta toda essa rede de informações e serviços também está se expandindo crescentemente, e uma das tecnologias que permite este crescimento é a virtualização dos recursos de TI (Tecnologia da Informação).

De forma geral, a virtualização é a abstração do *hardware*, proporcionando o aumento da eficiência dos recursos de TI e a redução de despesas, em uma fração muito pequena de tempo.

Grandes companhias se utilizam desta tecnologia há mais de dez anos, enquanto as pequenas e médias estão se deslocando para a virtualização somente agora.

Este trabalho aborda virtualização e computação em nuvem (*cloud computing*), bem como a importância destas tecnologias para as infraestruturas futuras, e a oportunidade de explorar a segurança que a computação em nuvem oferece atualmente.

A justificativa da escolha do tema deste artigo é devido à grande dependência que as empresas tem da TI, e a escassez de recursos (não somente financeiros, mas também humanos e organizacionais) para investimentos em TI. Assim, um dos principais fatores desta dependência é a economia e eficiência dos recursos computacionais.

Dessa forma, este trabalho tem como objetivo expôr as vantagens que a computação em nuvem oferece, bem como conceitos importantes de virtualização, que

fornecem base para a computação na nuvem. Adicionalmente, para associar os conceitos à prática, será exemplificado processo de criação de um ambiente virtual, tomando-se por base os serviços disponibilizados pela Amazon. A partir desse processo, será feita uma análise considerando-se os diversos aspectos asociados a esta solução, em especial os elementos relativos à segurança da informação.

MÉTODO

Marconi e Lakatos (2010) afirmam que uma pesquisa requer definição clara e objetiva do problema ou motivo para sua realização. Assim, para este artigo a questão norteadora é descrita por: "*Como utilizar os serviços públicos para a criação de ambientes de cloud, e quais as principais características e restrições de tais ambientes, no tocante à segurança da informação?*".

Adicionalmente, Marconi e Lakatos (2010) explicam que uma pesquisa pode ser classificada sob quatro perspectivas: natureza, forma de abordagem do problema, objetivos, e procedimentos técnicos. Em relação à sua natureza, esta pesquisa pode ser considerada aplicada, por discutir os conceitos sobre *cloud computing*, e aplicá-los na criação de uma nuvem pública, utilizando-se de um serviço disponível. Quanto à forma de abordagem do problema, ainda com base em Marconi e Lakatos (2010), este estudo é qualitativo, principalmente porque não há intenção de se utilizar técnicas e métodos estatísticos na interpretação dos resultados, somente o que tais resultados representam para a compreensão das relações de causa e efeito. Em relação aos objetivos, esta pesquisa caracteriza-se como uma pesquisa descritiva, pois busca, a partir da literatura, exemplificar um caso prático de criação de um ambiente *cloud*. Quanto aos procedimentos técnicos, esta pesquisa utilizou-se de estudo bibliográfico em artigos, livros, e artigos da *internet* sobre virtualização e computação em nuvem (*cloud*), bem como análise documental, e uma aplicação prática dos conceitos.

REFERENCIAL TEÓRICO

Virtualização e Computação em Nuvem

Estamos no meio de uma mudança em como os serviços computacionais são entregues. Como clientes, é possível se utilizar a web pelo celular, se obter direções de um GPS, e se transmitir vídeos e músicas a partir da nuvem. No coração disto tudo está a virtualização – habilidade de virtualizar um server físico em uma máquina virtual.

PROSPECTUS
ISSN 2674-8576 Gestão e Tecnologia

De acordo com a Oracle (2012), o conceito de virtualização teve a sua origem nos tempos de *mainframes*, no final dos anos 1960 e 1970, quando a IBM investiu muito tempo e dinheiro para desenvolver sistemas de tempo compartilhado, que como o nome indica, compartilhavam os recurcos computacionais entre grupos de usuários, tendo em vista aumento de eficiencia, uma vez que os recursos computacionais da época eram caros e escassos. Assim a virtualização representava um grande avanço da tecnología, tornando os custos computacionais mais acessiveis às empresas e individuos.

Com o advento da internet, o conceito da virtualização encontrou a infraestrutura adequada para sua propagação pois, devido à sua capacidade de procesar grandes volumes de dados com baixo custo, bem como de utilização de arquitetura aberta com baixos investimentos em infraestrutura de TI, é amplamente reconhecida como um grande viabilizador de colaboração de negócios (CHEN *et al*., 2007; LIU e ORBAN, 2008).

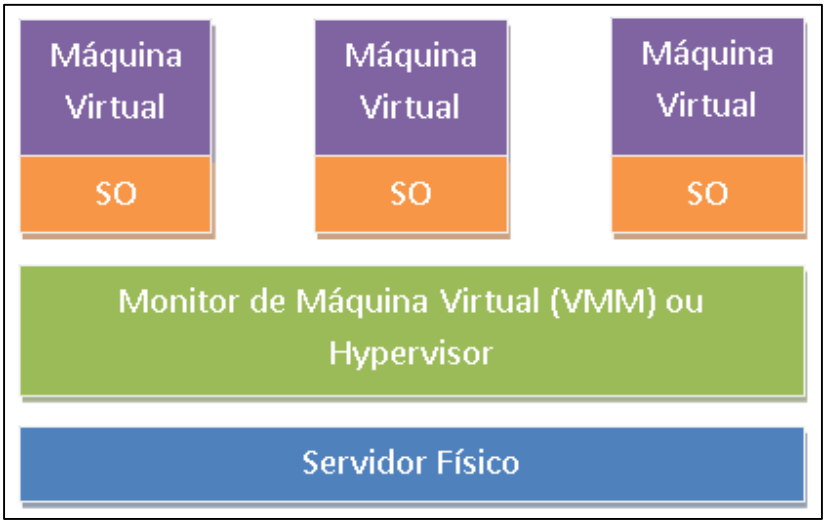
Atualmente os *datacenters* utilizam técnicas de virtualização para expandir a capacidade do *hardware* físico, criando grandes agregados de recursos lógicos como capacidade de processamento, de memória, discos, armazenamento, aplicações, redes, oferecendo tais recursos de forma ágil e escalável. Assim, mesmo que a tecnologia da virtualização tenha evoluído, seu principal propósito permanece: operar multiplos sistemas independentes, ao mesmo tempo.

Com base em Portnoy (2012), a primeira solução de virtualização comercial para computadores x86 veio da VMware em 2001. Dois anos depois, chegou o Xen como *softwar*e livre. Essas solucões de virtualização de *hardware* tomaram forma na camada de aplicação, situando-se entre o sistema operacional e a máquina virtual, ou entre o *hardware* e a máquina virtual, se instalado diretamente no *hardware*.

Virtualização em computação geralmente refere-se à abstração de algum componente físico em um objeto lógico (PORTNOY, 2012). Virtualizando-se um objeto, pode-se obter melhores resultados na utilização dos recursos que este objeto oferece. Por exemplo, LANs (*Local Area Networks*) Virtuais, ou VLANs (*Virtual Logical Areas Network*), fornecem melhor desempenho de redes e aprimoram o gerenciamento, por estarem separadas do *hardware* físico. Da mesma forma, SANs (*Storage Area Networks*) fornecem maior flexibilidade, disponibilidade e uso mais eficiênte dos recursos de armazenamento, virtualizando os dispositivos físicos em objetos lógicos, que podem ser rápida e facilmente manipulados. Ainda de acordo com o autor, servidores virtuais são sistemas encapsulados, essencialmente um conjunto de arquivos que podem ser copiados e movidos como qualquer outro arquivo. Por definição, de acordo com Portnoy (2012), a máquina virtual pode virtualizar todos os recursos de *hardware*, sendo o monitor de máquina virtual (VMM), conhecido atualmente como hypervisor, o programa que fornece o ambiente no qual uma máquina virtual (VM) será operada (Figura 1).

PROSPECTUS
ISSN 2674-8576 Gestão e Tecnologia

Figura 1 - Exemplo monitor de máquina virtual (VMM).

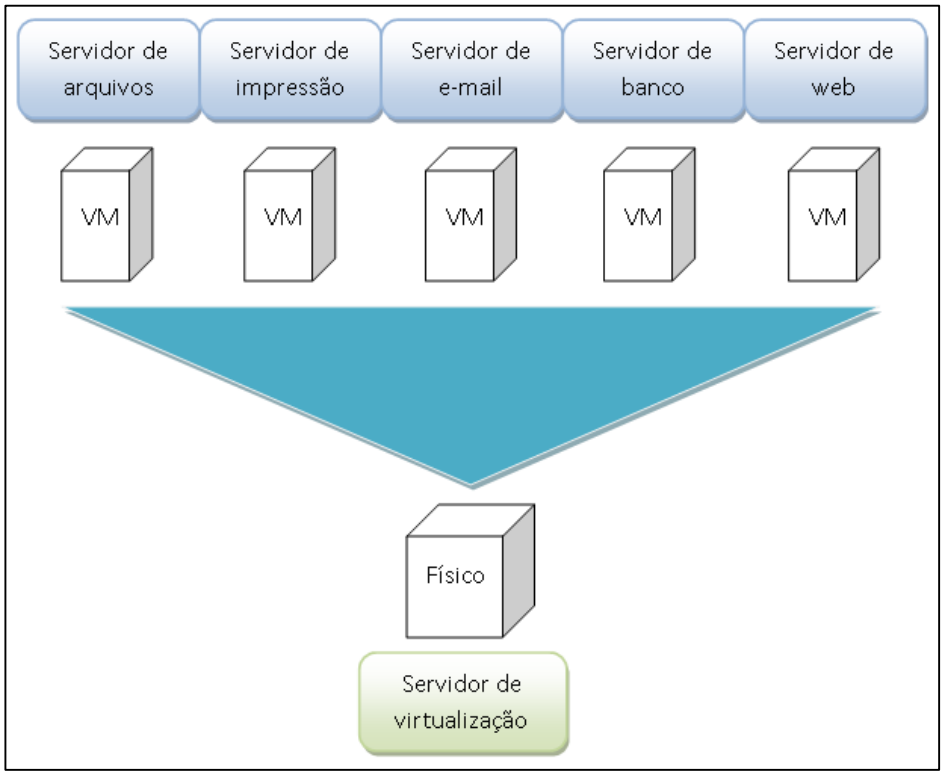


Fonte: Portnoy (2012).

Um dos benefícios da virtualização é a habilidade de condensar multiplos servidores físicos em apenas um servidor físico, que irá operar várias máquinas virtuais, permitindo com que o servidor físico seja utilizado de forma mais eficiente (PORTNOY, 2012). Esta condensação de servidores chama-se consolidação, como ilustrado na Figura 2. Pode-se calcular a taxa de consolidação de um servidor de acordo com o número de máquinas vituais neste servidor. Por exemplo, se um servidor tem oito máquinas virtuais, a taxa de consolidação será de 8:1. Mesmo com uma taxa de consolidação modesta de 4:1, poderia-se remover um quarto dos servidores de um *datacenter*.

Para *datacenters* que operam centenas e até milhares de servidores, a virtualização representa não somente a necessidade de equipamentos físicos, mas também a demanda por energía elétrica e refrigeração, uma vez que a taxa de consolidação pode chegar a 100:1 (PORTNOY, 2012).

Figura 2 - Exemplo de consolidação (5:1).



Fonte: Portnoy (2012).

A virtualização aumenta não somente a disponibilidade de recursos, mas também a flexibilidade, uma vez que máquinas virtuais podem migrar de um *host* para outro, sem interrupção, ou seja, ao invés de se agendar uma manutenção por uma falha de *hardware* no *host*, pode-se simplesmente mover a máquina virtual responsável pela aplicação para outro *host*, enquanto é feita a manutenção, muitas vezes sem se reiniciar o sistema operacional, como com Windows e Linux (PORTNOY, 2012).

Um fator crítico para a virtualização é a habilidade do *hypervisor* em desvincular o sistema operacional do *hardware*. Assim, o *hypervisor* torna-se o gerenciador de recursos das máquinas virtuais que ele suporta, fazendo com que a máquina virtual "acredite" que o *hypervisor* seja um *hardware* (PORTNOY, 2012). Adicionalmente, sem o *hypervisor*, o sistema operacional comunica-se diretamente com o *hardware* abaixo dele. As operações de disco acessam, de forma direta, o disco, e as chamadas de memória atuam diretamente sobre a memória física. Sem o *hypervisor*, mais do que um sistema operacional de várias máquinas virtuais iria querer controlar o *hardware* simultaneamente, o que resultaria em um caos total (PORTNOY, 2012).

As funções de um *hypervisor*, com base em Portnoy (2012), são: fornecer um ambiente idêntico ao ambiente físico; fornecer este ambiente com custo mínimo de desempenho; manter o controle total dos recursos do sistema. Ainda de acordo com o autor, alguns tipos de *hypervisores* de mercado compreendem: VMWare ESX; Citrix Xen; Microsoft Hyper V.

Para Portnoy (2012) existem duas classes de hypervisores, chamadas de Tipo 1 e Tipo 2. O único item a ser observado entre eles é como eles são implementados.

O autor afirma que o *hypervisor* do tipo 1 opera diretamente no *hardware* do servidor, sem a necessidade de um sistema operacional abaixo dele. Não existe uma camada intermediária entre o *hypervisor* e o *hardware* físico. Sem uma camada intermediária, o *hypervisor* pode se comunicar diretamente com os recursos de *hardware*, tornando-os mais eficientes do que o *hypervisor* do tipo 2, pois menos sobrecarga de processamento é necessária para o hypervisor do tipo 1, o que implica que cada servidor poderá operar mais máquinas virtuais. Adicionalmente, o hypervisor do tipo 1 é considerado mais seguro por não possuir a camada intermediária de um sistema operacional (PORTNOY, 2012).

O hypervisor tipo 2 é uma aplicação que roda em cima de um sistema operacional tradicional. O sistema operacional gerencia toda a parte de *hardware*, enquanto o *hypervisor* aproveita-se desta capacidade (PORTNOY, 2012).

Para Portnoy (2012), a vantagem do *hypervisor* tipo 2 é a maior compatibilidade de *hardware*, já que estas são herdadas do sistema operacional em uso. Geralmente o *hypervisor* tipo 2 é fácil de instalar e implementar porque muitos elementos de suas configurações de *hardware*, como redes e armazenamento, já foram feitos pelo sistema operacional.

Ainda com base em Portnoy (2012), os *hypervisores* do tipo 2 não são eficientes como os do tipo 1 porque há uma camada extra entre o *hypervisor* e o *hardware*. Neste modelo, o *hypervisor* depende da camada do sistema operacional para gerenciar as requisições com o *hardware*. Isto adiciona carga de processamento maior, e também há maiores chances de erros, pois qualquer coisa que acontecer com o sistema operacional irá afetar o funcionamento do *hypervisor*.

Em relação à computação em nuvens (*cloud computing*), Velte, Velte e Elsenpeter (2011) afirmam que o termo “cloud”, refere-se a um ambiente de TI distinto, que foi planejado com o propósito de provisionar remotamente recursos de TI que podem ser escaláveis e gerenciados.

Uma das vantagens da computação na nuvem é que as aplicações não são gerenciadas localmente. Isto siginifica que o usuário não fica responsável pelos custos de servidores, atualizações de *software*, licença, e acaba tendo menor custo, dependendo do contrato (Quadro 1).

Armbrust *et al.* (2010) e Buyya *et al.* (2009) afirmam que, embora existam muitas iniciativas práticas de desenvolvimento de *Cloud Computing* nas indústrias, poucas

pesquisas e estudos acadêmicos foram encontrados e, mesmo assim, embora tragam contribuições relevantes, se aplicam ao contexto de uma Organização, e não exploram o contexto de redes de empresas.

Asmad *et al.* (2012) afirmam que o modelo de cloud computing baseado na *Internet* se torna um canal por meio do qual negócios e integrações entre parceiros podem ser realizados com agilidade, flexibilidade e baixo custo, já que os serviços são entregues sob demanda aos requisitantes.

Cloud computing pode ser definida como uma tecnologia que utiliza um conjunto de recursos virtualizados, tais como *softwares*, infraestrutura ou plataforma, que facilitam a conectividade, sendo dinamicamente reconfiguráveis para apoiar diversos níveis de requerimentos organizacionais, que possibilitam a utilização otimizada dos recursos (IBM, 2009; IBM, 2011; VAQUERO *et al*., 2008). Nestes ambientes, há substituição de aplicações locais (servidores da empresa ou desktops) por aplicações baseadas em *cloud*. Nesta substituição, as empresas participantes podem utilizar, além dos sistemas, espaço de armazenamento do fornecedor da solução (Cegielski *et al*., 2012). Em comparação com sistemas tradicionais de computação, a tecnologia de cloud computing facilita a escalabilidade do poder de computação, entrega rápida de soluções, além de suporte reduzido de infraestrutura, e menores custos (IBM, 2011). Adicionalmente, a tecnologia não está limitada a fornecedores ou configurações específicas, ou mesmo a determinada utilização. Assim, pode ser aplicada de diferentes maneiras e configurações, por membros de organizações distintas, o que faz com que a tecnologia seja útil para o contexto de processos colaborativos (IBM, 2011). Ahmad *et al.* (2012) citam ainda a reutilização de componentes na rede como um benefício adicional, já que simplifica o processo de manutenção, requerendo menores custos.

Autry *et al.* (2010) consideram *cloud computing* como uma ferramenta de TI que serve como componente de infraestrutura técnica essencial para facilitar a comunicação, coordenação e colaboração entre os sistemas das empresas distintas.

Cegielski *et al.* (2012) afirmam que a tecnologia de *cloud computing* apresenta flexibilidade. Byrd e Turner (2000) definem flexibilidade como "a habilidade de compartilhar informação entre quaisquer tipos de plataformas tecnológicas".

GT Nexus (2013) afirma que, à medida que a estrutura de TI das empresas muda, o papel dessa TI se torna mais crucial, atuando na gestão, monitoramento, e manutenção das soluções de cloud computing para garantir que as aplicações estejam adequadamente alinhadas aos demais investimentos em *softwares*.

PROSPECTUS
ISSN 2674-8576 Gestão e Tecnologia

Quadro 1 - Atuação de TI nas Abordagens Tradicional e *Cloud.*

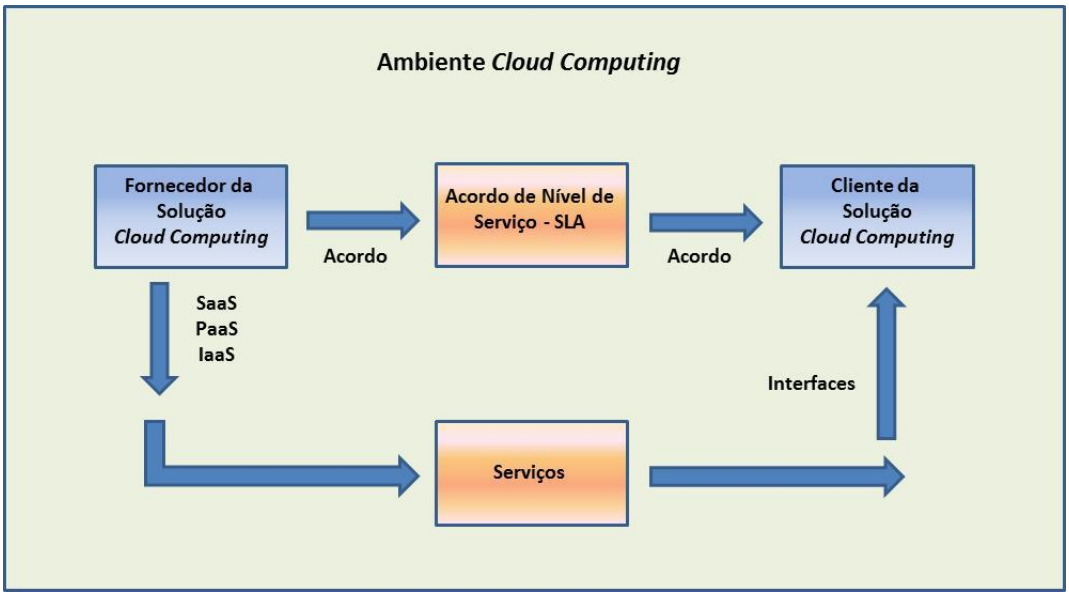
Diferenças entre TI Tradicional e Uso da Tecnologia Cloud Computing	
Equipe de TI Tradicional	**Equipe de TI Cloud**
Desenvolve e mantém grande quantidade de integrações entre sistemas / hardwares	Verifica junto ao fornecedor de Cloud se as melhores práticas de integração estão sendo seguidas.
Gerencia grande volume de capital para aquisição e manutenção de hardware	Gerencia somente despesas operacionais para subscrição em uma solução Cloud.
Paga por atualizações e manutenções nos softwares legados ERP.	As atualizações dos softwares são disponibilizadas pelo fornecedor da solução Cloud, e os custos de manutenção são compartilhados com os demais usuários da rede.
Cria novas conexões EDI ponto-a-ponto para cada parceiro que ingressa na rede	Utiliza mapas de integração padronizadas para rapidamente integrar novos parceiros e padronizar troca de dados.
Cada membro da equipe é assinalado à tarefas específicas, pouco estratégicas, com papel reativo	Os membros da equipe atuam, na maior parte do tempo, nas estratégias de negócios.
Realizam customizações nos sistemas ERP para apoiar os processos de fluxo de trabalho de negócios	Utiliza sistemas altamente configuráveis para atender as demandas das estratégias de negócios.

Fonte: GT NEXUS (2013).

Ahmad *et al.* (2012), com base em pesquisa envolvendo várias Organizações, constataram que a maioria delas tem pouco conhecimento sobre cloud computing. Destas, 55% possuem conhecimento médio sobre a tecnologia, 33% possuem pouco conhecimento, e 11% não possuem conhecimento sobre *cloud computing*. Adicionalmente, a informação disponível encontrada na maioria das Organizações é limitada, restringindo-se aos benefícios que a tecnologia oferece (33%). Pela redução que a tecnologia oferece nos custos de manutenção de TI, 22% das empresas pesquisas querem utilizar *cloud computing* de forma regular, ao passo que 44% querem utiliza-la ocasionalmente. Ahmad et al. (2012) identificaram as seguintes razões pelas quais as Organizações não querem utilizar serviços baseados em *cloud*: falta de conhecimento dos atributos da tecnologia (ex.: SLA – acordos de níveis de serviço) que correspondem a 40% da população pesquisada; questões de segurança, envolvendo 20% dos participantes;

falta de conhecimento sobre a totalidade de serviços oferecidos pelo fornecedor da tecnologia *cloud* (40%); fornecedores de serviço não confiáveis (40%); falta de interesse em adotar o ambiente *cloud* (20%); não querem migrar para a tecnologia *cloud* (20%). Ahmad *et al.* (2012) identificaram que 29% dos participantes concordam, e 66% parcialmente concordam em utilizar o ambiente de *cloud computing* (Figura 3).

Figura 3. Ambiente de *Cloud Computing.*



Fonte: AHMAD et al. (2012).

Uma das principais questões a serem consideradas com relação à tecnologia *cloud computing* é a segurança, elemento fundamental na concepção da arquitetura (IBM 2011, ASHMAD *et al*., 2012). Sob esta perspectiva, várias alternativas tecnológicas são adotadas, desde a utilização de uma entidade certificadora de segurança (*Trust Provider*), que é modelo proposto por Ashmad *et al.* (2012) até a concepção de uma infraestrutura baseada em camadas, como é o caso do modelo da IBM, o *Common Cloud Management Platform* (IBM, 2011).

De acordo com Ahmad *et al.* (2012), o ambiente de *cloud computing* pode ser implementado em vários modelos: SaaS (*Software* como Serviço), no qual as aplicações são supridas aos clientes como serviço, armazenadas no fornecedor e utilizadas remotamente; PaaS (Plataforma como Serviço), neste modelo há o fornecimento de todos os recursos para desenvolvimento das aplicações sem instalação de softwares. Neste ambiente, soluções de aplicações orientadas para a Web podem ser rapidamente e facilmente desenvolvidas; IaaS (Infraestrutura como Serviço), que considera a entrega de

hardware ou capacidade computacional como serviço (ex.: sistema operacional ou ambiente virtual); CaaS (Comunicação como Serviço), que considera a terceirização de serviços de telecomunicações, tais como serviços VoIP (voz sobre IP), IM (Instant Messaging), e soluções de videoconferência; MaaS (Monitoramento como Serviço), que provê serviços de apoio, como segurança, fornecendo proteção aos diferentes clientes contra ameaças cibernéticas. Neste ambiente o papel vital é manter a segurança em termos de confidencialidade, integridade, e disponibilidade dos ativos de TI.

Adicionalmente, é importante que sejam estabelecidos níveis de acordo de serviço (SLA – *Service Level Agreements*) formais entre cliente e fornecedor do serviço *cloud*. Para Ahmad *et al*. (2012) um SLA "define os elementos e contabiliza uma perspectiva geral sobre serviços, prioridades, responsabilidades e garantias".

Para Velte, Velte e Elsenpeter (2011), existem muitos riscos de segurança quando o assunto é a migração de dados para *cloud*, mas companhias com boa reputação trabalham duro para manter os dados seguros e protegidos.

Segundo Velte, Velte e Elsenpeter (2011), quando um dado deixa de ser interno e passa a ser armazenado em *cloud*, há perda de uma camada de controle. Além disso, a porta está aberta para os investigadores do governo acessarem essa informação. Torna-se muito mais fácil para o governo obter informações de terceiros do que um servidor de propriedade privada.

Existe o risco de provedores menos conhecidos compartilharem suas informações para companhias de *markenting*. Dependendo do contrato acordado, o provedor pode catalogar suas informações e usá-las de maneiras não autorizadas pela empresa (VELTE, VELTE e ELSENPETER, 2011). Por exemplo, a política do Google afirma que a empresa irá compartilhar os dados com o governo se ele tiver uma "boa razão" em que o acesso seja necessário, para atender às solicitações legais. Em alguns casos em que os provedores recebem uma intimação, este fica proibido de dizer aos seus clientes que os dados foram acessados pelo Governo. Resumindo, *cloud* não é o lugar mais seguro para armazenar dados confidenciais.

Entretanto, proteger os dados não significa que estes não devam ser armazenados em *cloud*, mas sim que devam ser protegidos. A melhor maneira de proteção ao dado é a criptografia. Um arquivo criptografado só poderá ser acessado mediante uma senha (VELTE, VELTE e ELSENPETER, 2011). Mesmo que a segurança do provedor de *cloud* seja quebrada, os dados criptografados ainda estarão seguros.

Embora raro, pode haver perda de acesso as aplicações caso a *internet* venha a falhar. Isto acontece porque as aplicações não estão rodando localmente, mas sim em um datacenter remoto do provedor de *cloud*.

Mas não é só a conexão com a *Internet* que está vulnerável a falhas. O problema pode acontecer também na infrastrutura do provedor de *cloud*, como aconteceu em julho de 2008 com a Amazon, onde o serviço de armazenamento caiu por oito horas (VELTE, VELTE e ELSENPETER, 2011).

Pode haver aplicações ou dados os quais seria melhor mantê-los localmente. Informações confidenciais e proprietárias não devem ser armazenadas em máquinas de terceiros.

Integração de aplicações podem também causar problemas. Por exemplo, se duas aplicações precisam trocar informações, seria mais fácil se as duas aplicações estivessem no mesmo lugar. Se uma aplicação local tiver que comunicar com outra aplicação na nuvem, isto se torna mais complicado e vulneravel a falhas maiores.

No entanto, os grandes provedores de *cloud* possuem rigorosas políticas de segurança e empregam fortes medidas de segurança, como o método da criptografia para efetuar a autenticação dos usuários. Com isso, os dados ficam mais seguros em *cloud* do que estariam internamente.

Computação em Nuvem é uma area em expansão, e muitos provedores estão para entrar no negócio em um futuro próximo. Alguns dos principais provedores são: Amazon, Google e Microsoft.

Velte, Velte e Elsenpeter (2011) explicam que a Amazon foi uma das principais empresas a oferecer serviços de computação em nuvem para o público. A Amazon oferece uma série de serviços, incluindo: Elastic Compute Cloud (EC2) – Máquina virtual; Simple Storage Service (S3) – Armazenamento de arquivos com até 5GB em tamanho; Simple Queue Services (SQS) – Permite comunicação entre máquinas, API; SimpleDB – Serviço web de consulta à dados estruturados em tempo real.

Os mesmos autores afirmam que a Google oferece blocos de construção para que o desenvolvedor possa fazer desde simples websites até aplicações complexas. Alguns destes serviços oferecidos são: AppEngine – Ambiente para desenvolvimento de aplicações (PaaS); Compute Engine – Máquina Virtual; Cloud Storage – Serviço de armazenamento; Cloud DataStore – Serviço de banco de dados.

Velte, Velte e Elsenpeter (2011) explicam que a solução de "*cloud*" da Microsoft chama-se Windows Azure, um sistema operacional que permite com que as Organizações rodem aplicações Windows, e armazenem dados nos *datacenters* da Microsoft.

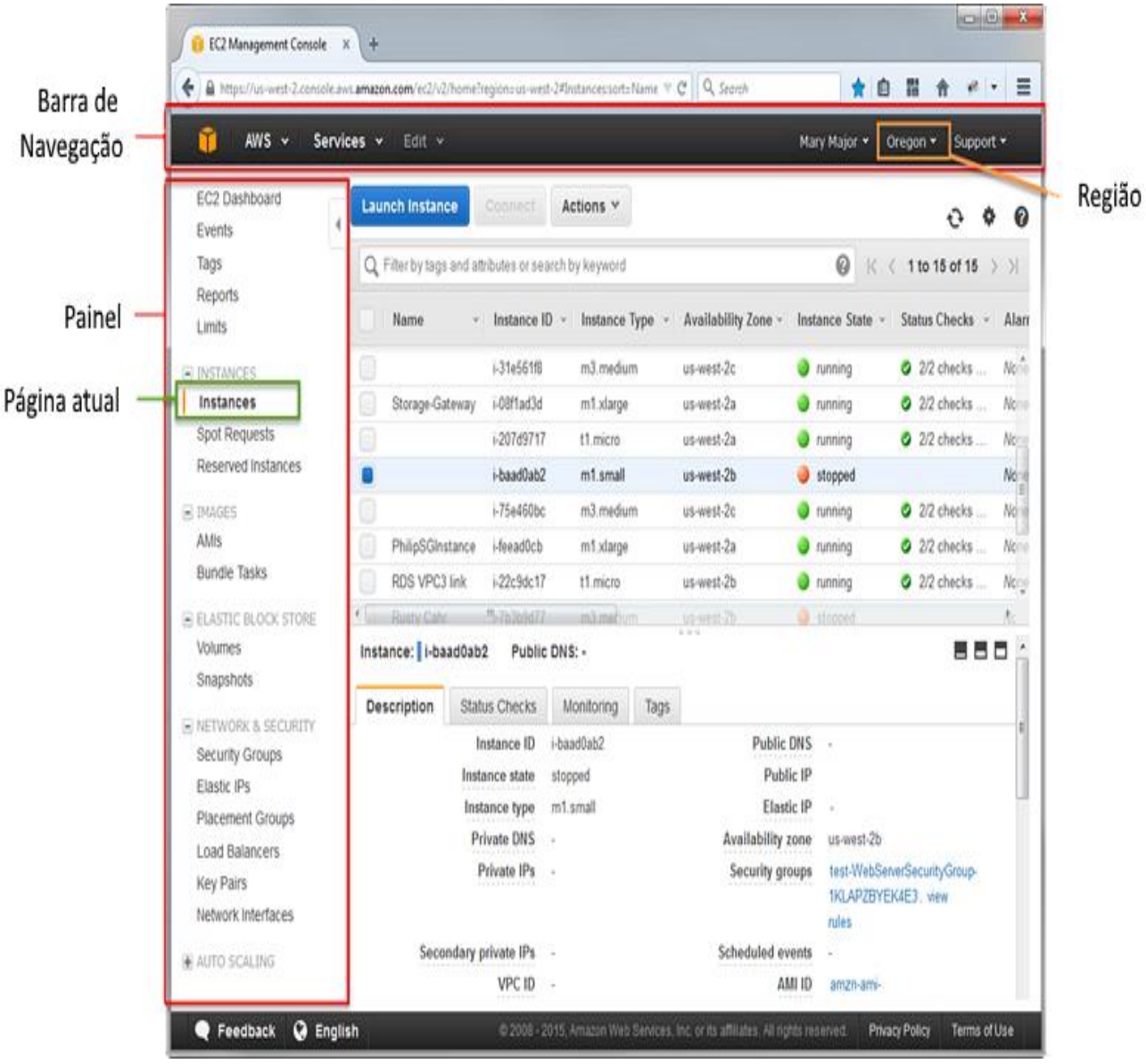
ESTUDO DE CASO

Para o estudo de caso, foi feita uma simulação considerando-se a configuração de uma estrutura em *cloud*. Para tanto, a Amazon Web Services (AWS) fornece recursos computacionais por demanda e serviços em *cloud*, com pagamento atrelado ao que a empresa utilizar. Nesse sentido, é possível se utilizar a AWS para facilitar a construção e gerenciamento de *websites* e aplicações, sendo mais comum para uso do AWS: armazenamento de dados privados ou públicos; hospedagem de websites, tanto estáticos quanto dinâmicos; criação de laboratórios virtuais para estudantes; manuseio de cargas de trabalho excessivas.

PROSPECTUS
ISSN 2674-8576 Gestão e Tecnologia

A console de gerenciamento da AWS é uma aplicação *web* para gerenciamento dos serviços de *cloud* da Amazon, e possui uma *interface* de interação com o usuário muito intuitiva para a realização de tarefas, tais como criação de armazenamento, máquinas virtuais, alarmes e assim por diante. A console também fornece informações sobre a sua conta e cobranças, conforme representado pela Figura 4.

Figura 4 - Console de Gerenciamento AWS.

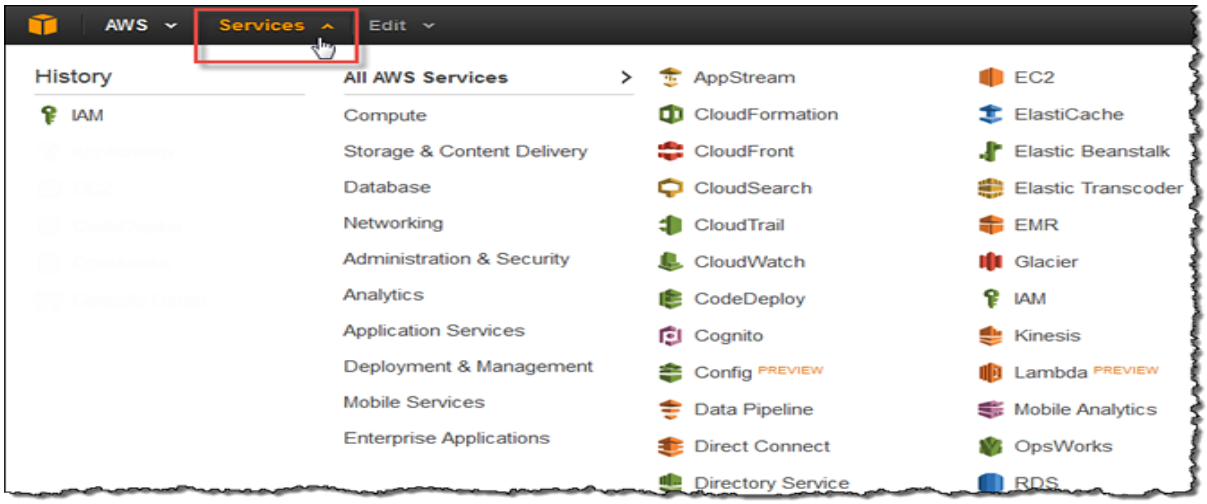


Fonte: Amazon (2016).

Para acessar um serviço na console são necessários os seguintes passos:

1. Clique em ***Services*** para abrir a lista de serviços (Figura 5);

Figura 5 - Todos os Serviços AWS.



Fonte: Amazon (2016).

2. Clique em alguma categoria, como **Compute & Network**, para visualizar a lista de serviços disponíveis na categoría (Figura 6);

Figura 6 - Recursos Computacionais e de Rede do AWS.

Fonte: Amazon (2016).

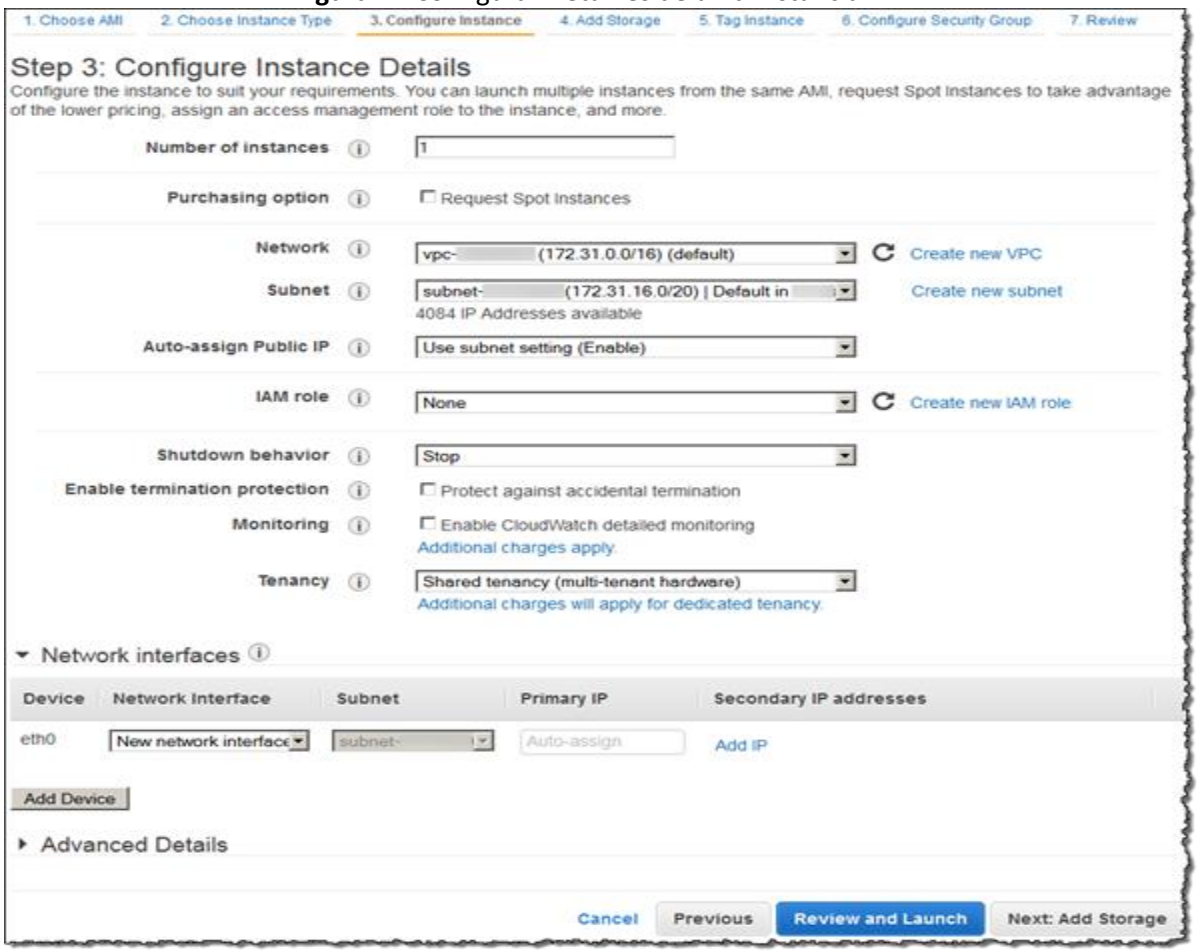
PROSPECTUS
ISSN 2674-8576 Gestão e Tecnologia

3. Clique em algum serviço para abrir a console do serviço escolhido;

Para se criar um servidor virtual, devem que sejam seguidos os seguintes passos:

1. Abra em seu navegador a console **Amazon EC2**;
2. Selecione **Launch Instance**;
3. No Passo 1: Selecione uma imagem para a sua instância;
4. No Passo 2: Selecione o tipo de instância;
5. No Passo 3: Configure os detalhes da instancia (Figura 7).

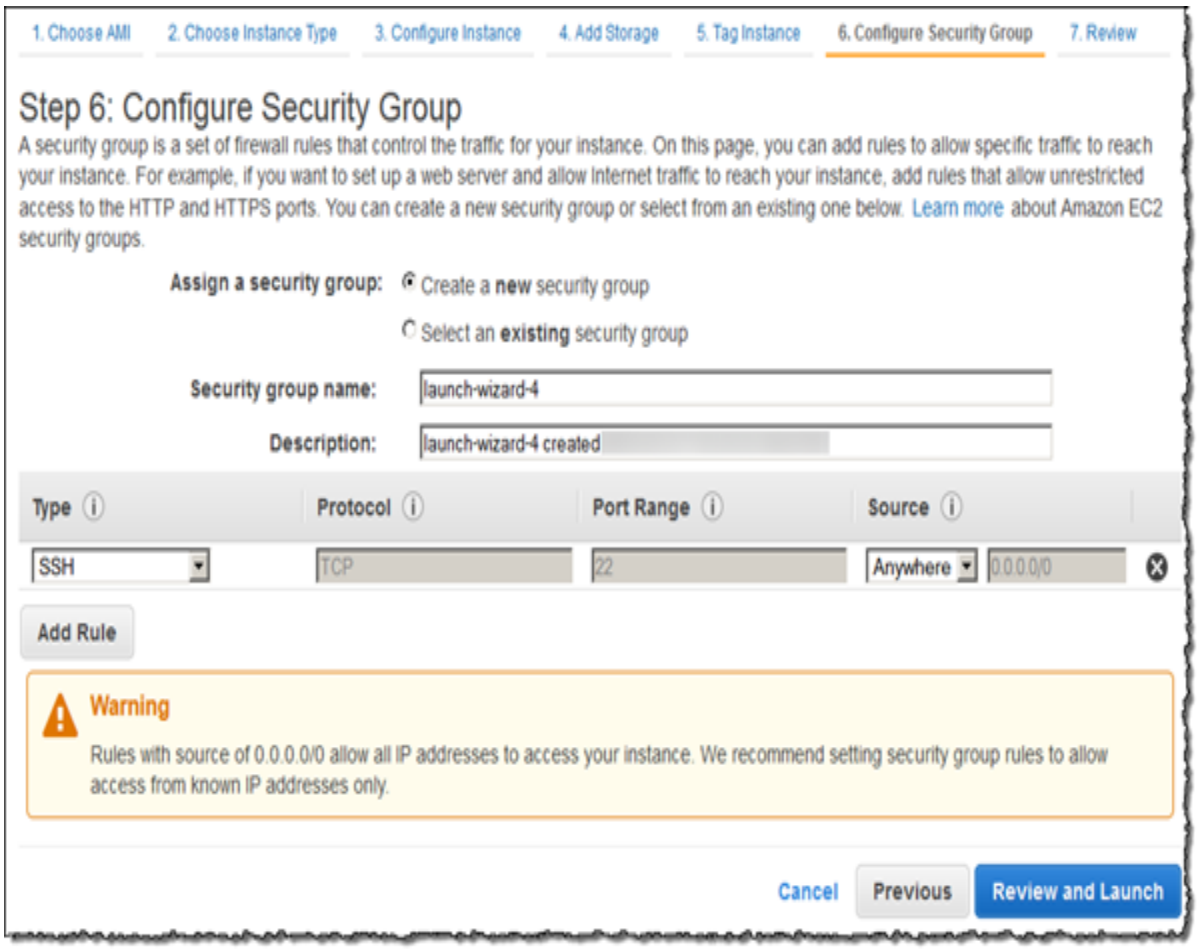
Figura 7 - Configurar Detalhes de uma Instância.



Fonte: Amazon (2016).

6. No Passo 4: Adicione armazenamento;
7. No Passo 5: Nomeie a sua instância;
8. No Passo 6: Configure o grupo de segurança (Figura 8).

Figura 8. Configurar Grupos de Segurança.

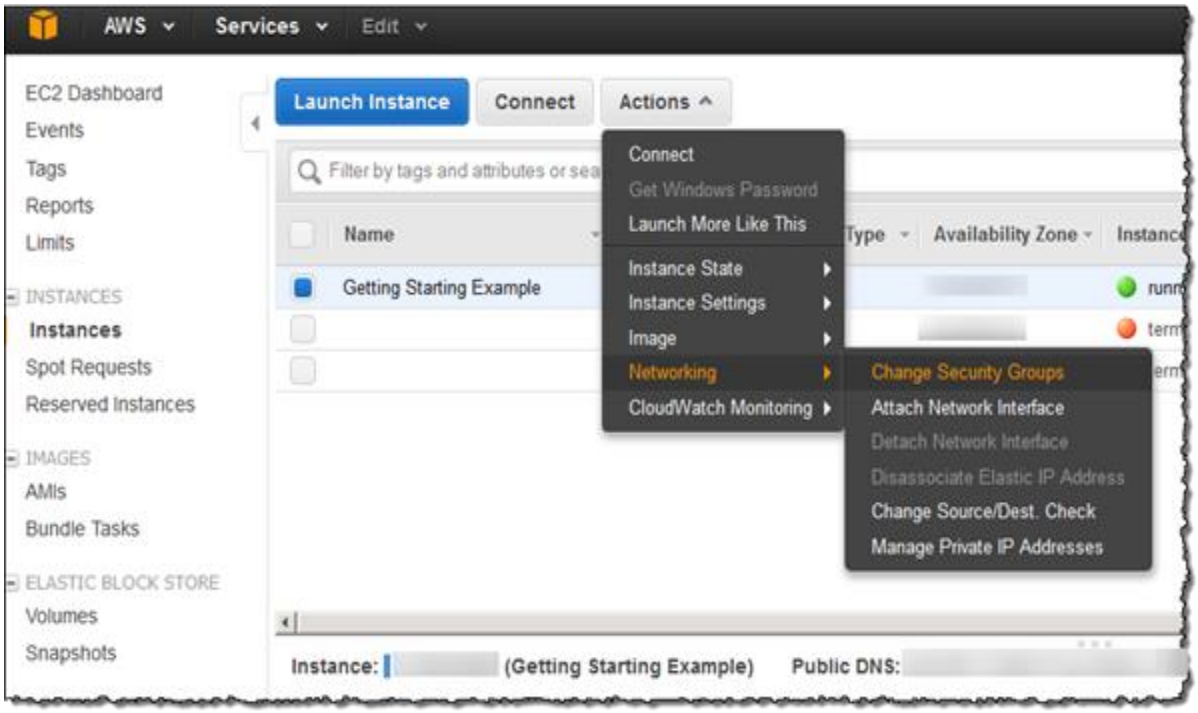


Fonte: Amazon (2016).

9. No Passo 7: Revisar os detalhes e concluir (Figura 9).

PROSPECTUS
ISSN 2674-8576 Gestão e Tecnologia

Figura 9. Painel de Instrumentos EC2.



Fonte: Amazon (2016).

Desta forma, caso não sejam implementadas as opções adicionais de segurança, a arquitetura está concluída, porém com riscos, gerando vulnerabilidades. Portanto, embora o serviço de criação de cloud facilita muito o trabalho para a criação de ambientes, necessitam de profissionais mais especializados, além de mecanismos adicionais de segurança em relação aos dados a serem armazenados, tais como criptografía, autenticação, e validação.

CONCLUSÕES

Nesta pesquisa foram abordados conceitos de virtualização, que é uma abstração proveniente do hardware, e computação em nuvem (*cloud computing*), bem como das suas principais ofertas de serviços. Mais do que uma tecnologia, *cloud* se tornou um conceito de como os serviços de TI são entregues, a maneira como algumas tarefas do administrador foram automatizadas, o que possibilitou que este se concentre em tarefas críticas para o negócio, aliada à grande econômia e eficiência que *cloud* traz consigo.

Contudo, abordamos a parte de segurança dos dados e conseguimos apontar algumas brechas de segurança, que embora podem ser remediadas com esforço mútuo entre o cliente e provedor *cloud*, se torna uma opção pouco provável ou não aconselhavel no armazenamento de dados sigilosos.

Embora grandes provedores de *cloud* estejam investindo e avançando nesta questão, percebe-se que os três pilares da segurança da informação não são assegurados atualmente, isto é, pode-se dizer que apenas a disponibilidade é assegurada, mas que a confidencialidade e integridade estão seriamente abaladas.

Com os dados armazenados em cloud, onde o acesso a eles é feito por intermédio da *internet*, podemos concluir que a ameaça existe e que não vale a pena correr o risco armazenando dados sigilosos em cloud. Não bastando as ameaças de hackers, os provedores de cloud podem ser forçados a permitir que o Governo tenha acesso aos dados de um cliente, e este não ser notificado por isso.

Cloud possibilita uma série de benefícios, mas ainda tem muito que progredir em relação à confidencialidade e integridade dos dados. Portanto, na hora de migrar seus dados para cloud, tenha em mente as ameaças e vulnerabilidade existentes, para formular um plano de remediação destes.

REFERÊNCIAS

AHMAD, S.; AHMAD, B.; SAQIB, S. M.; KHATTAK, R. M. Trust Model: Cloud's Provider and Cloud's User. **International Journal of Advanced Science and Technology**, v. 44, July 2012, p. 69-80, 2012.

AMAZON. **Passo 1:** criar seus recursos EC2 and iniciar sua instância EC2. Disponível em: http://docs.aws.amazon.com/pt_br/efs/latest/ug/gs-step-one-create-ec2-resources.html Acesso em: 01/05/2016

AMAZON. **Trabalhando com a console de gerenciamento da AWS**. Disponível em: http://docs.aws.amazon.com/pt_br/awsconsolehelpdocs/latest/gsg/getting-started.html Acesso em: 08/05/2016.

ARMBRUST, M.; FOX, A.; GRIFFITH, R.; JOSEPH, A.D.; DATZ, R., KONWINSKI, A.; LEE, G.; PATTERSON, D.; RABKIN, A.; STOICA, I.; ZAHARIA, M. A view of cloud computing. **Communications of the ACM**, v. 53, n. 4, p. 50-57, 2010.

AUTRY, C. W.; GRAWE, S. J.; DAUGHERTY, P.; RICHEY, R. G. The effects of technological turbulence and breadth on supply chain technology acceptance and adoption. **Journal of Operations Management**, v. 28, n. 6, p. 522-558, 2010.

BUYYA, R.; YEO, C. S.; VENUGOPAL, S.; BROBERG, J.; BRANDIC, I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. **Future Generation Computer Systems**, v. 25, n. 6, p. 599-616, 2009.

CEGIELSKI, C.G.; JONES-FARMER, L.A.; WU, Y.; HAZEN, B.T. Adoption of Cloud Computing Technologies in Supply Chains. **International Journal of Logistics Management**, v.23, n. 2, p.184-211, 2012.

GT NEXUS. **Cloud information technology:** A Model for the Networked Company. Disponível em: http://www.gtnexus.com/resources/white-papers-and-reports/. Acesso em: 07/05/2016.

HURWITZ, J. **Cloud Services for Dummies**. 4ª Edição, São Paulo, John Wiley & Sons Inc., 2006.

IBM (2009). **The benefits of cloud computing**. Disponível em: ftp://public.dhe.ibm.com/common/ssi/ecm/en/diw03004usen/DIW03004USEN.P DF. Acesso em: 08/05/2016.

IBM Global Technology Services (2011). **Getting cloud computing right**. Disponível em: http://public.dhe.ibm.com/common/ssi/ecm/en/ciw03078usen/CIW03078USEN.PDF. Acesso em: 08/05/2016.

ORACLE. **Uma breve história da virtualização**. Disponível em: https://docs.oracle.com/cd/E26996_01/E18549/html/VMUSG1010.html Acesso em: 24/02 ás 12:07
PORTNOY, M. **Virtualization Essentials**. 4ª Edição, São Paulo, John Wiley & Sons Inc., 2012.

VAQUERO, L. M.; RODERO-MERINO, L.; CACERES, J.; LINDNER, M. A break in the clouds: towards a cloud definition, ACM SIGCOMM. **Computer Communication Review**, v. 39, n. 1, p. 50-5, 2008.

VELTE, A. T.; VELTE, T. J.; ELSENPETER, R. **Computação em Nuvem: uma abordagem prática**. 1ª Edição, Rio de Janeiro, Alta Books, 2011.

Os autores declararam não haver qualquer potencial conflito de interesses referente a este artigo.