FACULDADE DE TECNOLOGIA DE AMERICANA

Curso de Segurança da Informação

ANGÉLICA CRISTINA CELEGATO

Orientador: Prof. Marcus Vinicius Lahr Giraldi

SEGURANÇA EM *CLOUD COMPUTING*

AMERICANA / SP

2011

FACULDADE DE TECNOLOGIA DE AMERICANA

ANGÉLICA CRISTINA CELEGATO

angelica_celegato@hotmail.com

SEGURANÇA EM *CLOUD COMPUTING*

Monografia apresentada à Faculdade de Tecnologia de Americana como parte das exigências do curso de Segurança da Informação para obtenção do título de Tecnólogo em Segurança da Informação.

Orientador: Prof. Marcus Vinicius Lahr Giraldi

AMERICANA / SP

2011

FACULDADE DE TECNOLOGIA DE AMERICANA

ANGÉLICA CRISTINA CELEGATO - RA 0912205

SEGURANÇA EM *CLOUD COMPUTING*

Monografia aprovada como requisito parcial para obtenção do título de Tecnólogo em Segurança da Informação do curso de Segurança da Informação da Faculdade de Tecnologia de Americana.

Banca Examinadora

Orientador: _____
Prof. Marcus Vinicius Lahr Giraldi

Professor da Disciplina: _____
Prof. Luiz Carlos Caetano

Professor Convidado: _____
Prof. Rogério Nunes de Freitas

Americana, 14 de Dezembro de 2011.

Dedico aos amigos.

Aos amigos familiares, aos amigos professores, aos amigos do trabalho, aos amigos, simplesmente amigos.

AGRADECIMENTOS

Agradeço a Deus por guiar meus passos e me dar toda a certeza de que os desafios estão presentes em nossas vidas para serem superados.

À minha grande família, que sempre me proporciona, com carinho e humildade, todos os ensinamentos e conhecimentos para que eu possa alcançar meus objetivos.

Aos meus amigos, que foram minha motivação e minha companhia de várias aulas, trabalhos, projetos, sábados de manhã e longas noites de aula.

“Saímos pelo mundo em busca de nossos sonhos e ideais. Muitas vezes colocamos nos lugares inacessíveis o que está ao alcance das mãos.”

Paulo Coelho

RESUMO

CELEGATO, Angelica Cristina. **Segurança em *Cloud Computing***. 2011**.** 66f. Trabalho acadêmico (Graduação) – Setor de TI. Faculdade de Tecnologia de Americana.

Com o avanço da Tecnologia da Informação, novos sistemas, modelos e práticas são lançados no mercado quase que diariamente. Sendo assim, diferentes empresas e usuários adaptam seus sistemas às novas tecnologias e lidam então com problemas de segurança e buscam a correção a fim de garantir a integridade, disponibilidade e confidencialidade da informação. Sendo assim, este trabalho apresenta o modelo *Cloud Computing,* também chamado Computação em Nuvem, e seus riscos de segurança, além de um estudo de caso de aplicação deste modelo em uma residência. Em busca de responder questões de segurança sobre este modelo, foram descritas também as desvantagens e os benefícios do modelo *Cloud Computing* na área segurança da informação.

Palavras-chave: *Cloud Comptuing*. Residência. Segurança.

ABSTRACT

CELEGATO, Angelica Cristina. **Segurança em *Cloud Computing***. 2011**.** 66f. Trabalho acadêmico (Graduação) – Setor de TI. Faculdade de Tecnologia de Americana.

With the advancement of information technology, new systems, models and practices are launched almost daily. Thus, different companies and users adapt their systems to new technologies and then deal with security problems and try to correct them in order to ensure the integrity, availability and confidentiality of information. Therefore, this presents the Cloud Computing model, also called "Computação em Nuvem" in Portuguese and its security risks, as well a study of the application of this model in a residence. In seeking of answering security questions about this model, it was also described the disadvantages and benefits of cloud computing in information security area.

Keywords: Cloud Computing. Residence. Security.

LISTA DE FIGURAS E DE TABELAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ANS	Acordo de Níveis de Serviço
ASP	*Application Service Provider*
CEO	*Chief Executive Officer*
CRM	*Customer Relationship Management*
ERP	*Enterprise Resource Planning*
IaaS	*Infrastructure as a Service*
NIST	*National Institute of Standards and Technology*
MUNDO	*Mobile and Ubiquitous Networking via Distributed Overlays*
OS	*Operating System*
PaaS	*Platform as a Service*
RH	Recursos Humanos
ROA	*Return on Assets*
ROI	*Return on Investments*
SaaS	*Software as a Service*
SLA	*Service Level Agreement*
SOA	*Service Oriented Architecture*
SPI	*Software Platform Infrastructure*
TI	Tecnologia da Informação

LISTA DE SÍMBOLOS

®	Marca registrada

SUMÁRIO

1 INTRODUÇÃO

Existem centenas, se não milhares de definições para Computação em Nuvem. Uns dizem que Computação em Nuvem é apenas um nome de *marketing* para tecnologias antigas como computação de utilitário, computação em grade ou virtualização, outros dizem que esta é a tecnologia do futuro.

Diferentes pensamentos nos levam a confirmação de que a Computação em Nuvem é muito abrangente e uma tecnologia promissora.

Com um mercado tecnológico cada vez mais arriscado e competitivo, há a necessidade de criação de novas soluções, modelos, abordagens, até mesmo diferentes modelos de cobrança por uso e arquiteturas virtuais automatizadas. Podemos ver isso com o movimento Web 2.0, onde se pode utilizar serviços por meio da internet, através de um computador desktop, notebook, celulares e qualquer outro aparelho que acesse a internet ou *wi-fi*.

Independente do sistema operacional, seja ele Linux, Mac *Operating System* (OS) ou Windows, a Computação em Nuvem pode ser aplicada, ou seja, tem todos os requisitos para propor diversas soluções.

Porém, como toda nova tecnologia, a mesma está em expansão e ainda apresenta diversas falhas de segurança.

Digo em nota que muitas pessoas desconhecem o termo, porém lidam diariamente com o Google Docs, criado pelo Google, ou Lotus Notes, criado pela empresa IBM.

O objetivo deste Trabalho de Conclusão de Curso é apresentar o modelo *Cloud Computing* e seus riscos de segurança, além de um estudo de aplicação deste modelo em uma residência.

Em busca de responder questões de segurança sobre este modelo, foram descritos também os benefícios e desvantagens do *Cloud Computing* na segurança da informação.

Este trabalho começa com a definição do tema *Cloud Computing* e sua história, segue com a apresentação da arquitetura da nuvem, suas características e

modelo. Após isso clarifica os diferentes tipos de serviços no mercado de TI, descreve os modelos de referência de nuvem e começa então uma análise de segurança da nuvem, mostrando as desvantagens e os riscos de segurança.

Após isso, define os benefícios na utilização desta tecnologia e mostra um caso de aplicação da tecnologia em nuvem.

Para finalizar, dados recentes e tendências sobre o assunto.

Para poder justificar as afirmativas deste trabalho, foram utilizados livros, artigos, um estudo de caso e sites, que trouxeram diversas informações a respeito desta tecnologia.

2 O *CLOUD COMPUTING*

Cloud Computing traduzida como Computação em Nuvem não é mais uma novidade no mundo da computação, porém este termo que chegou ao ouvido de muitos apenas a partir de 2008, segue em expansão devido a sua nova forma de representação e disponibilização de rede.

Poucos podem conhecer profundamente o conceito, porém já sabem que esta tecnologia vem revolucionando a computação mundial, onde o hardware que na maioria das vezes custa muito caro e precisa de processamento rápido e/ou grande capacidade de armazenamento, é substituído pelas nuvens.

De acordo com Amrhein e Quint (2009), “a Computação em Nuvem é uma solução completa na qual todos os recursos de computação (*hardware*, *software*, rede, armazenamento, etc.) são fornecidos rapidamente a usuários à medida que a demanda exige”.

No modelo *Cloud Computing*, aplicativos, arquivos, serviços, etc, não precisam estar instalados ou guardados no computador do usuário, ou seja, os recursos ou serviços que são fornecidos possuem a capacidade de serem aumentados ou reduzidos gradualmente de forma que os usuários usem os recursos necessários, sem pagar nem mais, nem menos por isso.

Desta maneira, a nuvem pode realçar a colaboração, agilidade, escalabilidade e disponibilidade, através de computação eficiente e otimizada.

> Neste modelo de negócios possibilitado pelo Cloud Computing, a Internet passa a ser o cérebro das operações e atividades das empresas, permitindo que novas capacidades sejam entregues como serviços pela rede, sem necessidade de aumento de infraestrutura e com pagamento atrelado ao uso feito pelos usuários **(*Intel, 2009).***

Conforme Taurion (2009), o *Cloud Computing* é um fenômeno muito recente, muito atual que trará várias vantagens competitivas para as organizações. Também segundo Lowe (2009), estima-se que até 2013 não haverá mais a necessidade de

arquivos, documentos e qualquer núcleo de informações ainda estarem salvo no disco local de um computador.

Como podemos ver, existem muitas definições que tentam endereçar a nuvem da perspectiva de acadêmicos, arquitetos, engenheiros, desenvolvedores, gerentes e consumidores. Sendo assim, os termos aqui utilizados, focam na definição usada para profissionais de segurança de Tecnologia da Informação (TI) e redes.

2.1 Como surgiu o *Cloud Computing*

O termo *Cloud Computing* foi criado por um dos *Chief Executive Officer* (CEOs) – Diretores Executivos da empresa Google, o senhor Eric Schmidte durante uma de suas palestras no ano de 2006, porém a tecnologia possui um extenso e antigo histórico, já que na década de 70, alguns cientistas alemães notaram que o desenvolvimento da internet e das redes de comunicação se tornaria um espaço virtual sem dono e sem fronteiras, onde diversos tipos de *softwares* e informações circulariam e seriam acessadas por qualquer usuário na rede.

Após isso, os cientistas começaram a estudar as consequências sociais e culturais da nuvem informativa ao desenvolver o modelo *iClouds*, que faz parte do projeto *Mobile and Ubiquous Networking via Distributed Overlays* (MUNDO) que significa Rede Móvel e Ubíqua por meio de Camadas Distributivas. Este projeto visa explorar as relações que as pessoas poderão estabelecer a partir do uso de sistemas pessoais de comunicação, chamados *iClouds*, muito semelhantes a alguns sistemas de telefones celulares.

Para entendermos melhor o surgimento da necessidade de uma nova tecnologia da informação em rede, podemos utilizar a figura 1.

De acordo com a figura 1, podemos ter duas linhas de negócio em Tecnologia da informação. Uma se refere à necessidade de negócio e outra aos recursos de TI que atendem essas necessidades.

Na década de 60 a 80, a necessidade de negócio se resumia em mercados locais, orientados a produção e com o objetivo de atendimento a pequenos silos organizacionais, enquanto que os recursos que atendiam essa demanda eram o *hardware*, aplicações centralizadas e os níveis de unidade de negócio suportados pelo Mainframe.

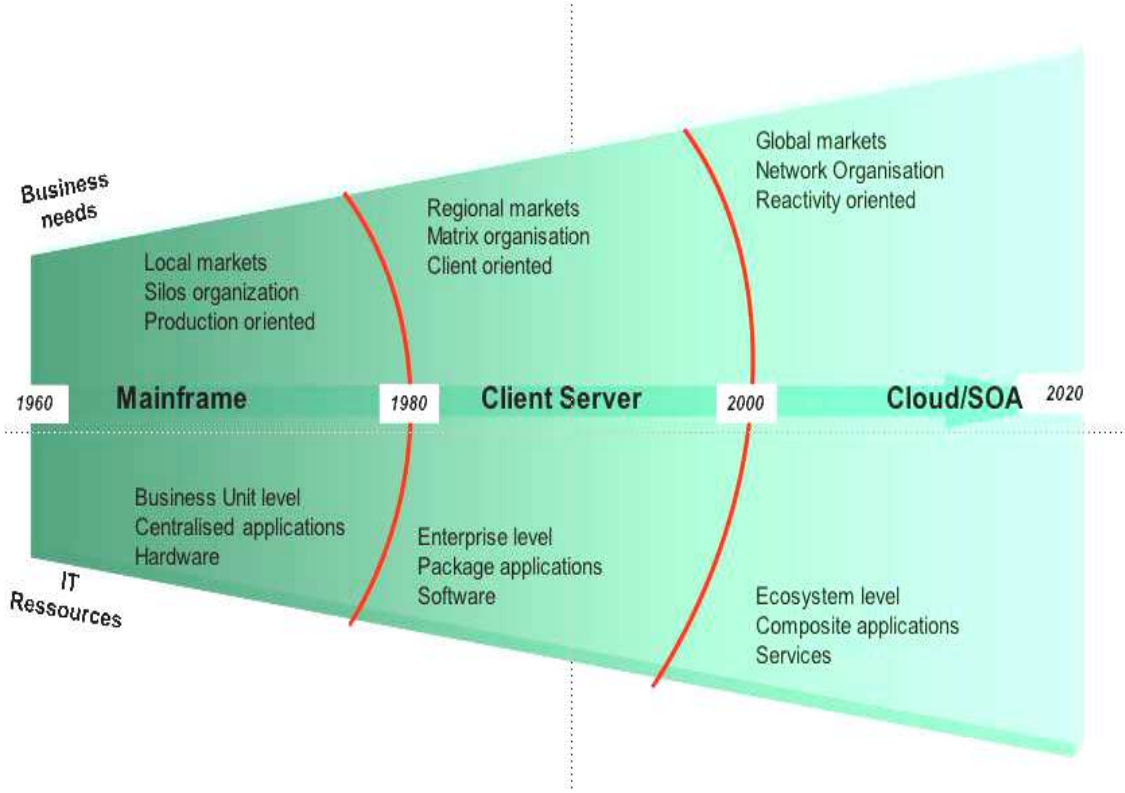

Figura 1 - Negócio e alinhamento de Tecnologia da Informação (TI) em uma economia inovadora entre as décadas. Dados que relatam o desenvolvimento do mercado computacional ao longo das décadas, desde o serviço realizado por mainframes, clinte-servidor, até os serviços prestados pela Computação em Nuvem**.** Fonte: PAC Paris (2010).

Posteriormente, aproximadamente vinte anos depois, o modelo *Client- Server* chega ao mercado para atender necessidades de negócio de mercados regionais, orientados ao cliente e atendimento a organizações de nível médio, também chamadas organizações matriciais. Essas requisições têm então nesta época, os

softwares, pacotes de aplicativos e o nível de empreendimento médio como objetivo de TI (Tecnologia da Informação).

Mais tarde surge o *Cloud/Service Oriented Architecture* (SOA) – Arquitetura Orientada a Nuvem/Serviços, que propõe do ano de 2000 adiante, atender necessidades de negócios globais, organizações baseadas em conexões de rede e prover um modelo reativamente orientado aos négocios, atendido por um sistema ecológico, baseado em serviços de TI e aplicações compostas. O *Cloud Computing* está cotado a ser a tecnologia da vez até o ano de 2020.

3 ARQUITETURA DE COMPUTÇÃO EM NUVEM

Sob a perspectiva da arquitetura, há muita confusão em torno de como a nuvem é tanto similar e diferente dos modelos computacionais existentes, e como estas similaridades e diferenças impactam nas abordagens organizacionais, operacionais, e tecnológicas para as práticas de segurança da informação e de redes.

Na visão da *Cloud Security Alliance* (2010)*, a*s chaves para entender como a arquitetura da nuvem são baseadas em uma nomenclatura comum e concisa, associada com uma taxonomia consistente de ofertas de como os serviços e arquiteturas de serviços na nuvem podem ser interpretadas, mapeadas para um modelo de controles de segurança e operacionais, *frameworks* de análise e gerenciamento de risco, e de acordo com padrões de conformidade.

O que seria então a arquitetura de Computação em Nuvem?

O *National Institute of Standards and Technology (*NIST) – Instituto Nacional de Tecnologias Padrão, define a Computação em Nuvem em cinco características, três modelos de serviço e quatro modelos de implementação.

Além dos modelos de visualização da nuvem e a tecnologia de multilocação.

3.1 Características essenciais da Computação em Nuvem

Baseando-se no modelo do NIST, os serviços na nuvem possuem cinco características que são essenciais que mostram suas relações e diferenciais em relação às abordagens tradicionais de computação:

- Amplo acesso a rede: a rede deve estar disponível e ser acessada através de mecanismos padrões que indicam o uso por plataformas heterogêneas

de *thin clients* (clientes leves) ou não (por exemplo, telefones celulares e laptops), além de outros serviços de software tradicionais ou baseados em nuvem.

- Rápida elasticidade: capacidades podem ser rapidamente e elasticamente providenciadas, na maioria das vezes automaticamente. Ou seja, o consumidor tem capacidade disponível e geralmente ilimitada para ser contratada a qualquer hora e em diferentes quantidades.
- Serviços mensuráveis: os sistemas em nuvem automaticamente controlam e aperfeiçoam o uso de recursos como armazenamento, processamento, largura de banda ou contas de usuário ativas. Com a monitoração, controle e relato de recursos, há transparência para o provedor e o consumidor do serviço.
- Auto-serviço sob demanda: o usuário pode requerer capacidades computacionais, como tempo de servidor e armazenamento de rede automaticamente conforme necessário, sem requerer interação humana com o provedor de serviços.

Figura 2 – Modelo Visual de Definição de Computação em Nuvem do *NIST.* Dados que mostram a arquitetura do modelo de Computação em Nuvem. Fonte: NIST (2010).

- *Pool* de Recursos: Os recursos de computação do provedor estão reunidos para servir a múltiplos consumidores usando um modelo multilocação, com diferenças físicas e recursos virtuais dinamicamente atribuídos e retribuídos de acordo com a demanda do consumidor. Existe um grau de independência de localização nisto que o consumidor geralmente não tem controle ou conhecimento sobre a localização exata dos recursos providos, mas pode ser capaz de especificar a localização em um nível mais alto de abstração (por exemplo, país, estado ou *data center*). Exemplos de recursos incluem armazenamento, processamento, memória, largura de banda, e máquinas virtuais. Até nuvens privadas tendem a reunir recursos entre diferentes partes da mesma organização.

A tecnologia de multilocatário, que será apresentada a seguir, não é considerada essencial pelo NIST, mas é geralmente discutido como se fosse.

3.2 Modelos de Serviços

Em ambientes onde a Computação em Nuvem é aplicada, podemos ter três principais modelos de serviços. Estes modelos são essenciais, pois definem um padrão de arquitetura para as soluções de Computação nas Nuvens.

As três classificações são geralmente referidas como “Modelo SPI”, onde “SPI” significa *Software*, Plataforma e Infraestrutura (como um Serviço).

3.2.1 *Software* como um Serviço (SaaS)

O *Software* como Serviço, também chamados de *Software as a Service (*SaaS), pode ser definido como a evolução dos *Applications Service Providers* (ASP) – Provedor de Serviços de Aplicação, porém diferente devido aos programas que são disponibilizados pelo SaaS não servirem apenas para uma única

necessidade de um usuário singular, mas sim por ser de uso de diversos clientes de seus respectivos fornecedores.

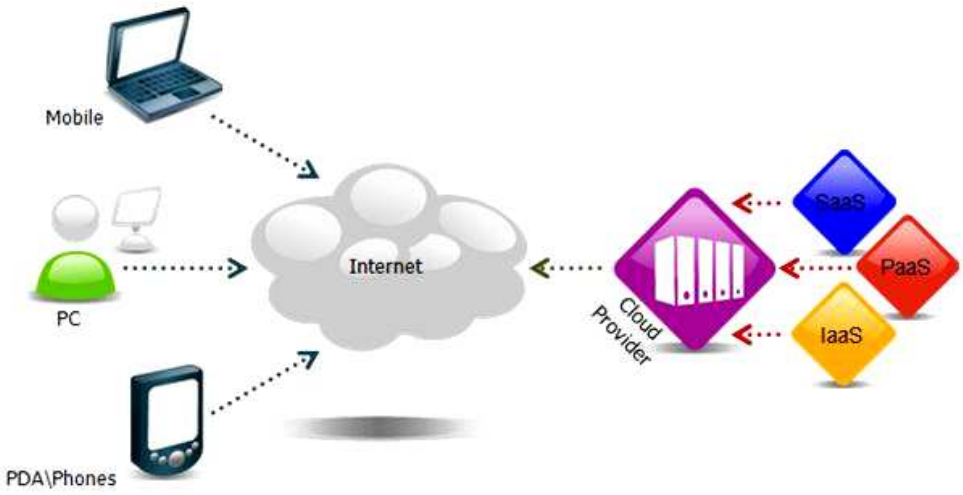

Figura 3 – Modelo SPI de *Cloud Computing.* Dados que mostram a conexão do modelo SPI a internet e aos usuários. Fonte: LEIF (2009).

O SaaS pretende mundialmente conquistar os clientes de *Cloud Computing*, pois o *software* desejado pelo usuário é executado no servidor na nuvem, sem necessidade de instalação na máquina de quem irá usufruir do software. Ou seja, o usuário acessa o *software* por meio da nuvem.

Sendo assim, um mesmo *software* pode ser utilizado por múltiplos usuários, sejam pessoas ou empresas. Conforme Aulbach (2009), esse tipo de serviço é executado e disponibilizado por servidores de responsabilidade de uma empresa desenvolvedora, ou seja, o *software* é desenvolvido por uma empresa que ao invés de vendê-lo ou usá-lo para benefício exclusivo, disponibiliza-o a um custo baixo a uma grande quantidade de usuários.

> As chances de sucesso aumentam na proporção direta do comportamento estratégico com o modelo. É absolutamente necessário identificar as novas oportunidades de negócio e desenhar as ofertas SaaS para atingir essas oportunidades ***(Taurion, 2009).***

Além do mais, de acordo com a Intel (2009), "*Software* como um Serviço é uma nova forma de entregar via web, programas com recursos já disponíveis no mercado, sem que o usuário tenha necessidade arcar com custos de licença anuais por uso, como acontece no seguimento de informática".

Figura 4 – Modelo de *Cloud Computing* SaaS. Dados que mostram os serviços oferecidos pelo modelo SaaS. Fonte: IBM (2010).

Exemplos de SaaS são: o site de declaração do imposto de renda que usa o Turbo Tax, o email GMail ou o Yahoo Mail , o Google Calendar, IBM® Lotus® Live, IBM Lotus Sametime®, Unyte, Salesforce.com, CRM, ERP, Sistemas de RH, entre outros.

3.2.2 Plataforma como um Serviço (PaaS)

Também chamada como *Platform as a Service* (PaaS), a Plataforma como Serviço tem como objetivo implementar aplicações adquiridas ou criadas pelos clientes, em uma nuvem, usando ferramentas e linguagem de programação suportadas pelo provedor.

Ou seja, este tipo de nuvem provê servidores virtualizados nos quais os usuários podem executar seus aplicativos ou desenvolver novas aplicações sem se preocupar com o sistema operacional, servidores, capacidade e armazenamento.

De acordo com a IBM (2010), a Plataforma como Serviço pode suportar todas as aplicações de bases de dados, ferramentas de desenvolvimento Java e Web 2.0 como sendo uma camada de serviço.

Figura 5 – Modelo de *Cloud Computing* PaaS. Dados que mostram os serviços oferecidos pelo modelo PaaS. Fonte: IBM (2010).

Para Amrhein e Quint (2009), essa é a camada na qual vemos a infraestrutura do aplicativo emergir como um conjunto de serviços. Isso inclui, mas não se limita a *middleware* como um serviço, sistema de mensagens como um serviço, integração como um serviço, informações como um serviço, conectividade como um serviço, etc.

Exemplos de implementação da tecnologia PaaS são: as imagens virtuais do IBM® WebSphere® Application Server, Amazon Web Services, Boomi, Cast Iron e Google App Engine.

3.2.3 Infraestrutura como um Serviço (IaaS)

Infraestrutura como um Serviço, também conhecido como *Infrastructure as a Service* (IaaS), disponibiliza servidores virtuais, redes, armazenamento e software de

sistemas desenhados para aumentar ou substituir as funções de um centro de dados.

De acordo com Amrhein e Quint (2009) os serviços de infraestrutura abordam o problema de equipar de forma apropriada os datacenters, assegurando o poder de computação quando necessário. Além disso, devido ao fato das técnicas de virtualização serem comumente empregados, economias de custos decorrentes da utilização mais eficiente de recursos podem ser percebidas.

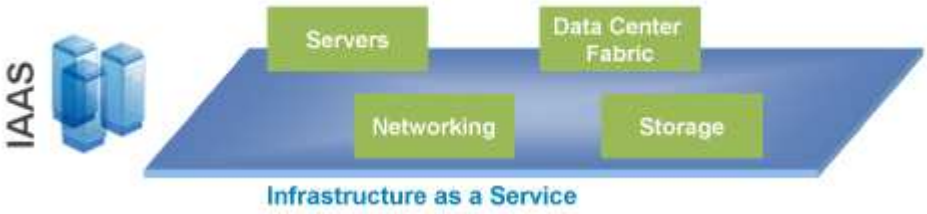

Figura 6 – Modelo de *Cloud Computing* IaaS. Dados que mostram os serviços oferecidos pelo modelo PaaS Fonte: IBM (2010).

Sendo assim, o consumidor não gerencia ou controla as camadas da infraestrutura na nuvem, mas tem o controle sobre o sistema operacional, armazenamento, aplicações e possivelmente controle limitado de componentes específicos de rede.

Exemplos de serviços de infraestrutura incluem: servidores, rede, armazenamento e *data center*.

Algumas aplicações deste modelo são encontradas no IBM BlueHouse, VMWare, Amazon EC2, Microsoft Azure Platform, Sun ParaScale Cloud Storage e mais.

3.2.4 Comparação do “Modelo SPI”

Veja na tabela 1, o resumo dos modelos dos serviços oferecidos pela nuvem e sua classificação em relação aos seus riscos. A avaliação do risco cresce de acordo

com a movimentação da nuvem, ou seja, se há uma movimentação de consumidores de IaaS para PaaS e, finalmente, para SaaS, os modelos de serviço de construção de um sobre o outro, resulta em risco acumulativo, como o provedor da nuvem assume o controle mais direto, há, portanto, maior risco de segurança para o consumidor da nuvem.

Tabela 1 – Riscos inerentes dos modelos de serviços na nuvem

Modelo de Serviço	Características	Risco
Software como um Serviço (SaaS)	Neste modelo de serviço o consumidor não administra ou controla a infraestrutura subjacente da nuvem. O que inclui componentes de rede, servidores, sistemas operacionais, armazenamento ou capacidade de aplicação individual. A possível exceção relaciona-se a algumas configurações específicas do usuário e de algumas configuração de aplicativos.	Muito Alto
Plataforma como um Serviço (PaaS)	Neste modelo de serviço o consumidor não administra ou controla os recursos de infraestrutura da nuvem subjacente, tais como componente de rede, servidores, sistemas operacionais, ou armazenamento. Porém o consumidor tem controle sobre os aplicativos utilizados na hospedagem de aplicativos e nas configurações de ambientes.	Alto
Infraestrutura como um Serviço (IaaS)	Neste modelo de serviço o consumidor não administra ou controla a infraestrutura da nuvem subjacente, mas tem controle sobre os sistemas operacionais, armazenamento de aplicativos implantados, e os componentes de rede selecionados.	Médio

Fonte: http://boozallen.com/publications. Acessado em: 08 novembro 2010 – 23h47min.

3.2.5 Outros serviços de *Cloud Computing* no mercado

Além dos serviços apresentados acima, diversos outros modelos surgiram e podem ser encontrados durante uma comercialização de *Cloud Computing*. Entre eles temos: Armazenamento como um Serviço, *Backup* como um Serviço, Banco de Dados como um Serviço, Informação como um Serviço, Processo como um Serviço, Aplicação como um Serviço, Segurança como um Serviço, Antivírus como um Serviço, Gerenciamento/Governança como um Serviço e Execução de Teste como um Serviço.

3.3 Tipos de nuvens

Independente do modelo de serviço utilizado, seja ele SaaS, PaaS ou IaaS, existem quatro modelos de implantação de serviços de nuvem, com variações para atender a requisitos específicos: Nuvem Pública, Nuvem Privada, Nuvem Compartilhada e Nuvem Híbrida.

3.3.1 Nuvem Pública

Os serviços nas nuvens públicas são vendidos por uma organização que faz com que a infraestrutura da nuvem fique disponível ao público em geral, a um determinado grupo ou a uma indústria específica. Em outras palavras, as nuvens públicas são serviços fornecidos por um provedor que gerencia a nuvem, sempre oferecendo ao consumidores responsabilidades de instalação, gerenciamento fornecimento e manutenção.

3.3.2 Nuvem Privada

As nuvens privadas são serviços oferecidos dentro de uma empresa. A empresa possui propriedade e gerenciamento sobre a nuvem local e/ou remotamente.

Diferente da nuvem pública, a empresa é responsável pela configuração e manutenção deste tipo de nuvem.

3.3.3 Nuvem Compartilhada

Sua infraestrutura é compartilhada por um grupo e suporta uma determinada comunidade que divide interesses.

Este tipo de nuvem pode ser administrado pelas organizações ou por um terceiro e pode existir no local ou fora do ambiente da empresa.

3.3.4 Nuvem Híbrida

As nuvens híbridas combinam nuvens públicas, privadas e compartilhadas. Sendo assim, a infraestrutura de uma nuvem híbrida é uma composição de duas ou mais nuvens.

Na maioria das vezes são criadas pela empresa e gerenciada pela empresa e pelo provedor de nuvem pública.

3.4 Visualização da nuvem

A Computação em Nuvem pode ser divida em duas seções. São elas: visualização frontal e traseira.

3.4.1 Visualização Frontal

A visualização frontal, também chamada *front-end* (visualização frontal) é modo de visualização do lado do usuário.

3.4.2 Visualização Traseira

A visualização traseira, também chamada *back-end* (visualização traseira) é a nuvem do sistema.

3.5 Multilocatário

Mesmo não sendo uma característica essencial da Computação em Nuvem no modelo do NIST, a multilocação é um elemento importante da nuvem.

De acordo com o *Cloud Security Alliance* (2010)*, a* multilocação de serviços de nuvem implica na necessidade de forçar a aplicação de políticas, segmentação, isolamento, governança, níveis de serviço e modelos de cobrança retroativa/faturamento aplicados a diferentes grupos de consumidores. Os consumidores poderão utilizar serviços oferecidos por fornecedores de serviços de

nuvem pública ou na verdade fazerem parte da mesma organização, como no caso de unidades de negócios diferentes, em vez de diferentes entidades organizacionais, mas ainda assim iriam compartilhar a infraestrutura.

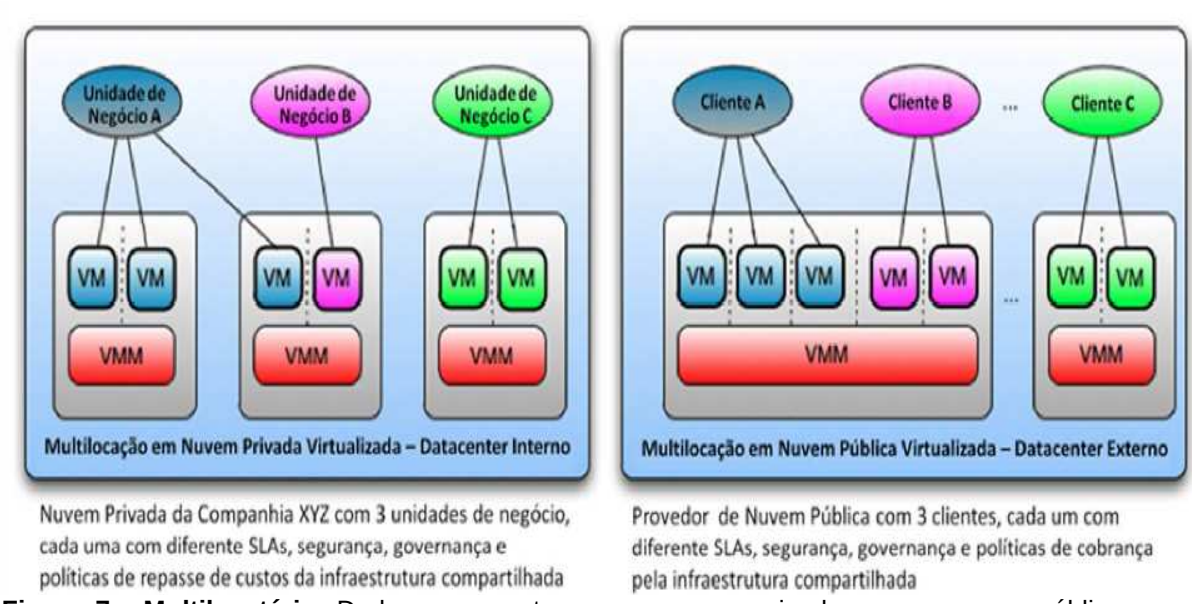

Figura 7 - Multilocatário. Dados que mostram uma nuvem privada e uma nuvem pública com a tecnologia de mutilocação. Fonte: *Cloud Security Alliance* (2010).

Se analisarmos pelo lado do provedor, a multilocação propõe um *design* e arquitetura que permite disponibilidade, gestão, economia de escala, isolamento e eficiência operacional, aproveitando o compartilhamento da infraestrutura, dos dados, serviços e das aplicações através de muitos consumidores diferentes.

> A multilocação também pode ter definições diferentes, dependendo do modelo de serviço de nuvem do provedor, na medida em que pode implicar na viabilidade das capacidades descritas acima nos níveis da infraestrutura, do banco de dados, ou da aplicação. Um exemplo seria a diferença entre a implantação de uma aplicação multilocação em SaaS e IaaS ***Cloud Security Alliance*** **(2010)**.

Os modelos de implantação de nuvem possuem importâncias diferentes em multilocação. Porém, mesmo que a nuvem seja privada, uma determinada

organização pode utilizar vários consultores e contratados terceirizados, assim como separação lógica entre as unidades de negócio. Deste modo, as preocupações da multilocação devem ser sempre consideradas.

4 DIFERENTES CONCEITOS E TENDÊNCIAS QUE RESULTAM EM *CLOUD COMPUTING*

4.1 União de conceitos e tendências

O *Cloud Computing* une conceitos e tendências da tecnologia da informação. Entre eles temos o Software como Serviço, ASP (*Application Service Provider*), *Utility Computing* e *Grid Computing*.

Sendo assim, a Computação em Nuvem pode ser considerada um conjunto de conceitos, porém agora apresentados sob uma nova visão e organização.

4.1.1 *Application Service Provider* (ASP)

De acordo com a Intel (2009), o *Application Service Provider* (ASP) é um formato de terceirização, baseado em fornecedores que disponibilizam serviços e recursos de tecnologia e computação para projetos específicos de determinados usuários, através da Internet. Entre essas ferramentas podemos incluir softwares, infraestrutura e mesmo mão-de-obra especializada. Neste modelo, a partir de um centro de dados com grande potencial, os provedores desenvolvem e alugam aplicações e serviços, adaptados a necessidades específicas de seus clientes. Os consumidores por sua vez, pagam uma taxa mensal para usufruir dessas operações.

Sendo assim, a tecnologia ASP propõe economia aos usuários, principalmente para pequenas e médias empresas, que podem ter acesso a recursos tecnológicos excelentes a custo baixo, eliminando assim a necessidade de investir em uma infraestrutura própria ou melhorar os sistemas que já possuem.

4.1.2 Grid Community

O *Grid Computing* ou Computação em Grade disponibiliza uma grande capacidade de processamento, porém o usuário não precisa se preocupar de onde vêm esses recursos e como a manutenção é realizada.

Para a Intel (2009), através de camadas virtuais, é possível alcançar alta taxa de processamento ao se dividir as tarefas em diversas máquinas, utilizando os recursos ociosos de computadores independentes. Para compor esse supercomputador virtual, a Grid Computing pode ser desenvolvida em rede local ou de longa distância.

Desta forma, a Computação em Grade permite acesso a equipamentos de custo muito elevado, onde o desenvolvimento de uma série de aplicativos de ponta e a utilização de vários recursos computacionais sem a necessidade de investimentos em novos equipamentos é requerida.

4.1.3 ***Utility Computing***

O modelo *Utility Computing*, que traduzido significa Computação de Utilidade Pública e que é classificado como Computação sob Demanda, possui características onde o usuário pode contratar o *software*, *hardware* e serviços de acordo com sua necessidade de utilização e em função de fatores como picos, quedas e de acordo com o período de uso. Semelhante a comercialização de serviços como o fornecimento de água, luz ou telefone.

> [...] a Computação de Utilidade Pública auxilia as empresas em questões como redução de custos, controle na utilização de tecnologia e flexibilidade para contratar serviços e ferramentas de acordo com os projetos específicos que irá desenvolver, sem que para isso precise adquirir aplicativos que não terão utilidade constante após essa primeira aplicação ***Intel (2009).***

Dessa forma, o *Utility Computing* se preocupa em fazer com que o usuário se concentre apenas em usar os recursos, enquanto o fornecedor se preocupe com a disponibilidade e manutenção, além da qualidade do serviço em questão.

5 MODELOS DE REFERÊNCIA DE NUVEM

Compreender as relações entre os modelos de Computação em Nuvem é primordial para que possamos compreender os riscos de segurança de uma nuvem.

O modelo IaaS é o fundamento básico de todos os serviços de uma nuvem. O PaaS é fundamentado no IaaS e SaaS baseado no PaaS, como podemos ver no diagrama “Modelo de Referência de Nuvem”.

Sendo assim, como há herança de capacidades, também se herda as questões de segurança da informação e seus riscos.

De acordo com *Cloud Security Alliance* (2010)***:***

- O IaaS inclui todos os recursos de infraestrutura desde as instalações até as plataformas de hardware que nela residem. Ela incorpora a capacidade de abstrair os recursos (ou não), bem como oferecer conectividade física e lógica a esses recursos. Finalmente, a IaaS fornece um conjunto de APIs que permitem a gestão e outras formas de interação com a infraestrutura por parte dos consumidores.
- O PaaS trabalha em cima da IaaS e acrescenta uma camada adicional de integração com *frameworks* de desenvolvimento de aplicativos, recursos de *middleware* e funções como banco de dados, mensagens e filas, o que permite aos desenvolvedores criarem aplicativos para a plataforma cujas linguagens de programação e ferramentas são suportadas pela infraestrutura.
- O SaaS por sua vez, é construído sobre as pilhas IaaS e PaaS logo abaixo, e fornece um ambiente operacional auto contido usado para entregar todos os recursos do usuário, incluindo o conteúdo, a sua apresentação, a(s) aplicação(ções) e as capacidades de gestão.

Mesmo com as considerações acima, devemos saber que existem compensações de cada modelo em relação a funcionalidade, complexidade e segurança.

O modelo SaaS oferece a funcionalidade mais integrada e completa, mesmo tendo alto nível de risco, possui maior nível de segurança, já que o fornecedor assume a responsabilidade pela segurança.

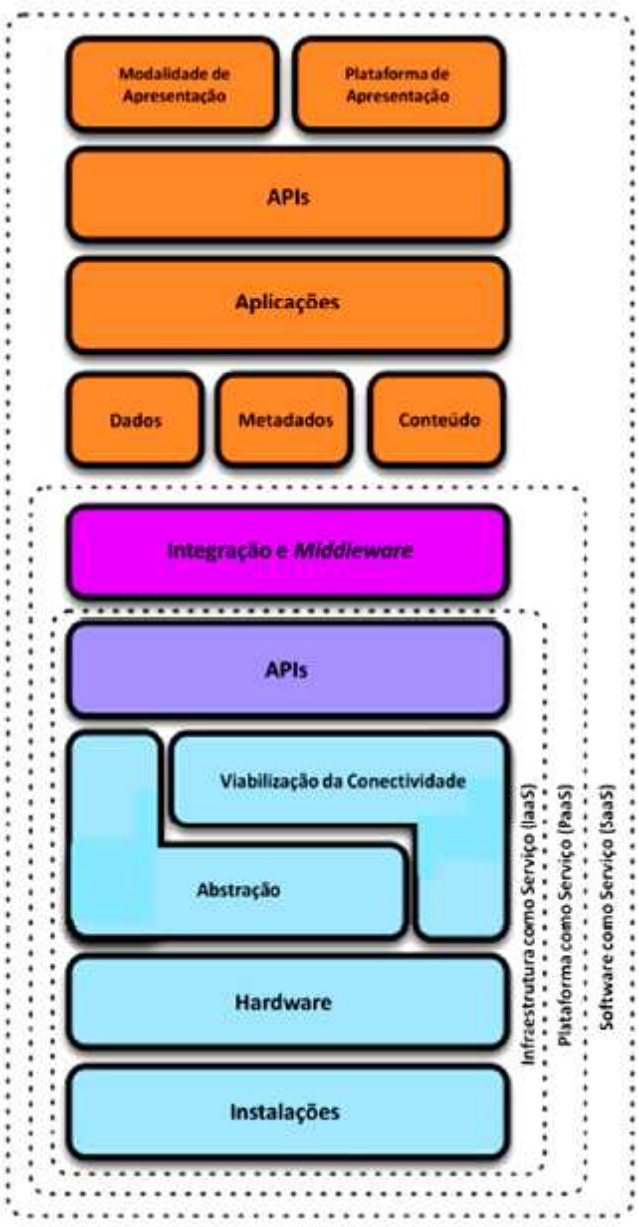

Figura 8 – Modelo de Refência de Nuvem. Dados que mostram a interligação do modelo SPI .Fonte: *Cloud Security Alliance* (2010).

O modelo PaaS permite que os desenvolvedores façam seus próprios aplicativos. Com isso ela tende a ser mais flexível e possuir características e

capacidades de segurança menos completa. Porém há maior flexibilidade em adicionar camadas extras de segurança.

Já o modelo IaaS oferece menos funcionalidades de segurança, pois os sistemas operacionais, aplicativos e o conteúdo possam ser gerenciados e protegidos pelo consumidor da nuvem.

Uma análise essencial sobre a segurança na nuvem é que quanto mais baixo na pilha o prestador de serviços de nuvem parar, mais recursos de segurança terão que ser utilizados e os consumidores serão responsáveis por implementar e gerenciar.

No caso do SaaS, isso significa que os níveis de serviço, segurança, governança, conformidade, e as expectativas de responsabilidade do prestador de serviço estão estipuladas, gerenciadas e exigidas contratualmente. No caso de PaaS ou IaaS é de responsabilidade dos administradores de sistema do cliente gerenciar eficazmente o mesmo, com alguma compensação esperada pelo fornecedor ao proteger a plataforma e componentes de infraestrutura subjacentes que garantam o básico em termos de disponibilidade e segurança dos serviços. *Cloud Security Alliance* (2010).

Analisando e estreitando as tarefas e capacidades específicas, assim como as funcionalidades dentro de cada um dos modelos de ofertas de nuvem, ou empregando o agrupamento dos serviços e recursos entre eles, podemos ter classificações derivadas. Um exemplo é o “Armazenamento como um Serviço” (“*Storage as a Service*”) é uma sub-oferta específica dentro da “família” do IaaS.

6 SEGURANÇA EM NUVEM

Em lugares onde há ambientes computacionais é comum vermos que vários requisitos de segurança são ignorados comparados aos requisitos necessários dos sistemas. Isso resulta em desenvolvimento de sistemas e ambientes com grande vulnerabilidade a ataques e segurança falha.

Quando falamos em vulnerabilidade em Computação em Nuvem, logo relacionamos modelos de entrega e sistemas hospedados em fornecedores terceiros, onde o geralmente engloba-se milhares de questões relacionadas à privacidade e segurança das informações residentes neste servidor na nuvem.

Apesar das preocupações citadas acima, como privacidade e segurança, o assunto sobre segurança na nuvem muitas vezes esquece-se da importância de criar planos de contingência e Acordo de Níveis de Serviço (ANS) (em inglês SLA – *Service Level Agreement*), designados a prover confiabilidade e a certeza de que os negócios não sofrerão grandes impactos no caso de um desaste.

Na computação tradicional, ambientes *in-house*, os usuários têm total controle sobre seus dados, processos e seu computador. Por outro lado, na Computação em Nuvem todos os serviços e manutenção são fornecidos por um provedor de nuvem. Sendo assim, o cliente (usuário) muitas das vezes desconhece onde exatamente os dados estão armazenados devido ao dinamismo da nuvem. Desta maneira, o cliente não tem controle sobre todas as atividades dos seus dados.

De acordo com Paul Simmonds (2010), "ainda é preciso trabalhar muito antes que a indústria entenda de onde vêm os furos de segurança em Computação em Nuvem".

Isso impulsiona diversas equipes de pesquisas a buscar melhores práticas em segurança, caso empresas queiram ou pretendam desfrutar dos benefícios da Computação em Nuvem.

A implantação e consumo de nuvem devem ser pensadas não só no contexto do ‘interno’ versus ‘externo’, como em relação à localização física dos ativos, recursos e informações, mas também no contexto de quem são os seus

consumidores e de quem é o responsável pela sua governança, segurança e conformidade com políticas e padrões.

Isto não é sugerir que a localização da nuvem seja dentro ou fora da empresa de um ativo, um recurso ou uma informação não afete a condição de segurança e de risco de uma organização porque elas são afetadas, mas sim para ressaltar que esse risco também depende dos tipos de ativos, recursos e informações sendo gerenciadas, de quem as gerencia e como as gerencia, de quais controles estão selecionados e como eles estão integrados e questões de conformidade.

Até a presente pesquisa sobre Computação em Nuvem, temos alguns tópicos de examinação de segurança em nuvem. Os mesmos estão listados a partir do tópico 6.1.

6.1 Segurança, governação, gestão de riscos e conformidade

As organizações utilizadoras da tecnologia *Cloud Computing* precisam ter visibilidade da segurança aplicada na nuvem. Isso inclui ampla transparência no processo de mudança, falhas ocorridas, gerenciamento de incidentes, assim como emissão de relatórios aos inquilinos da nuvem com as logs de auditoria.

Quando falamos em *Cloud Computing* podemos afirmar que para a nuvem ser segura, a visibilidade do cliente é um ponto chave para que a segurança seja eficaz.

De acordo com IBM (2009), a Lei Sarbanes-Oxley, exige que os recursos de auditoria sejam sempre abrangentes. Uma vez que as nuvens, principalmente as públicas são, por definição uma incognita para o usuário, podendo em muitas das vezes não ser capaz de mostrar se está *compliance* ou não com os requisitos de segurança. A nuvem privada ou híbrida, por outro lado, podem ser configuradas para atender aos requisitos de segurança.

Além do mais que, os fornecedores do serviço de *Cloud Computing*, algumas vezes, precisam adquirir auditorias de terceiros e seus clientes podem ser

direcionados a investigações forenses quando alguma nuvem está sendo suspeita de violações.

Isso adiciona ainda mais importância para a manutenção de visibilidade adequada de uma nuvem.

Em geral, as organizações muitas vezes citam a necessidade de Acordos de Nível de Serviço (SLAs) que são adaptados à cada situação específica, com base em suas experiências com estratégica de terceirização ou serviços gerenciados.

6.2 Pessoas e identidade

Quando se fala em *Cloud Computing*, as organizações também precisam se certificar de que os usuários autorizados em toda a empresa tenham acesso aos dados e ferramentas que eles precisam, quando precisam, antes do bloqueio de acesso não autorizado ser feito.

Ambientes de nuvem normalmente suportam uma comunidade grande e diversificada de usuários, assim estes controles são ainda mais críticos. Além disso, as nuvens introduzem um novo nível de usuários privilegiados: os administradores que trabalham para o provedor de nuvem.

A monitoração deve incluir monitoramento físico e checagem de antecedentes.

6.3 Proteção de dados e informações

A maioria das organizações citam a proteção de dados como o seu problema de segurança mais importantes. Típicas preocupações incluem a maneira pela qual os dados são armazenados e acessados, *compliance* e requisitos de auditoria e questões de negócios envolvendo o custo das violações de dados, requisitos de

notificação aos danos e valor da marca. Todos os dados sensíveis ou regulados precisam ser devidamente segregados na infraestrutura de armazenamento em nuvem, incluindo os dados arquivados.

Criptografia e gerenciamento de chaves de criptografia de dados em trânsito na nuvem ou dados parados no provedor de dados é fundamental para proteger a privacidade dos dados e cumprimento de exigências de conformidade. Ou seja, somemente o provedor da nuvem ou o consumidor de uma nuvem privada (por exemplo), deve ter acesso as chaves de criptografia, pois a implantação da nuvem pode levantar questões relativas as leis jurídicas, caso haja violação da informação criptografada. Sendo assim, a implementação da nuvem jamais pode expor e ameaçar os dados do usuário. Em outras palavras, se os dados envolvidos são críticos, a assessoria jurídica da organização deve realizar uma revisão completa de todos os requisitos de segurança antes da implantação nuvem, certificando-se que o provedor pode manter o controle sobre a localização geográfica de dados na infraestrutura.

Em áreas que envolvem usuários e dados com diferentes classes de risco (tais como serviços públicos e financeiros), o provedor precisa manter a nuvem de dados de acordo com a escala de classificação do usuário. A classificação dos dados irão reger quem tem acesso, como esses dados são criptografados e arquivados, e como as tecnologias são usadas para evitar perda de dados.

6.4 Rede e servidor

Dentre os vários tipos de nuvem, no ambiente de nuvem compartilhada, existe a necessidade de garantia por parte do usuário e da empresa fornecedora da nuvem, de que todos os domínios estejam adequadamente isolados, de modo que nenhuma possibilidade de trafégo de dados entre os compartilhadores da nuvem exista.

Para alcançar este objetivo, os usuários precisam ter a capacidade de configurar domínios virtuais de confiança ou baseado em políticas de zonas de segurança.

Como nas nuvens os dados do usuário se movem longe do controle do mesmo, é necessário um sistema de Detecção de Instrusão para prevenir ataques maliciosos ao ambiente. A preocupação não é apenas intrusões, mas também o potencial de vazamentos de dados, ou seja, extrusões. Em outras palavras, é fazer uma utilização abusiva do domínio de um cliente para montar ataques a terceiros.

Em um ambiente de nuvem compartilhada por exemplo, todas as partes devem concordar com as suas responsabilidades e revisar a política de segurança da nuvem, além do provedor da nuvem assumir a liderança de gestão de contratos para garantir que hajam avaliações de risco

6.5 Infraestrutura física

A infraestrutura da nuvem, incluindo servidores, roteadores, dispositivos de armazenamento, fontes de alimentação e outros componentes que suportam as operações, devem ser fisicamente seguros.

Isso inclui um controle adequado que engloba monitoramento de acesso físico utilizando o controle de acesso biométrico, circuito fechado de televisão de monitoramento, entre outros.

Os provedores da nuvem precisam explicar claramente ao usuário como o acesso físico dos servidores que hospedam dados e cargas de trabalho é gerenciado.

7 PRINCIPAIS FALHAS DE SEGURANÇA

Nos últimos anos, o instituto Gartner (2008) alertou os usuários de Tecnologia da Informação sobre os principais riscos de segurança na utilização de Computação nas Nuvens:

1. Acesso privilegiado para determinados usuários: dados críticos sendo processados fora da empresa trazem, obrigatoriamente, um alto nível de risco, ou seja, os serviços de terceiros não abrangem controles “físicos, lógicos e de pessoal”.
2. Regulamentação: as empresas são as responsáveis pela segurança e integridade de seus próprios dados, mesmo que haja gerenciamento por um determinado provedor de serviços
3. Localização dos dados: quando há o uso de utilização de nuvem, a empresa provavelmente não sabe exatamente onde os dados estão localizados. Por exemplo, a empresa pode não saber em que país em que as informações estão guardadas.
4. Segregação dos dados: geralmente dados de uma empresa na nuvem dividem o armazenamento de dados com outros clientes. A criptografia é efetiva, mas não é a melhor solução. Sendo assim, sempre se deve tentar descobrir onde os dados estão sendo armazenados.
5. Recuperação dos dados: em caso de desastre, mesmo o cliente não sabendo onde os dados estão localizados, a empresa fornecedora em *cloud*, deve saber como proceder em caso de perda.
6. Apoio à investigação: a investigação de atividades ilegais pode se tornar impossível em *Cloud Computing*.

> Serviços em cloud são especialmente difíceis de investigar, por que o acesso e os dados dos vários usuários podem estar localizados em vários lugares, espalhados em uma série de servidores que mudam o tempo todo. Se não for possível conseguir um compromisso contratual para dar apoio a formas específicas de investigação, junto com a evidência de que esse fornecedor já tenha feito isso com sucesso no passado ***Gartner (2008).***

7. Viabilidade em longo prazo: a empresa fornecedora do serviço de computação na nuvem deve garantir que todos os dados continuarão disponíveis caso a empresa falir, ou seja, adquirida por uma empresa maior.

> Pergunte como você vai conseguir seus dados de volta e se eles vão estar em um formato que você pode importá-lo em uma aplicação substituta ***Gartner (2008).***

Além dos riscos apresentados acima pelo instituto Gartner, temos outros riscos que podem agredir a segurança da nuvem ao ver da IDG News Service (2010):

8. Perda de dados ou vazamento: não há um nível de controle de segurança aceitável na nuvem. Alguns aplicativos podem deixar dados vazarem como resultado de um controle de API, geração de chaves, armazenamento ou gestão fracos. Além disso, políticas de destruição de dados podem estar ausentes.

9. Vulnerabilidades de tecnologias compartilhadas: na nuvem, uma única configuração errada pode ser duplicada em um ambiente nos quais vários servidores virtuais compartilham essa informação. A organização deve aplicar acordos de nível de serviço (SLAs) para o gerenciamento de atualizações e as melhores práticas para a rede e configuração do servidor.

10. Internos maliciosos: o nível de verificações que os provedores da nuvem realizam em uma equipe pode variar de acordo com o controle de acesso ao datacenter estabelecido pela empresa. A recomendação é realizar uma avaliação de fornecedores e definir um nível de seleção de funcionários.

11. Desvios de tráfego, contas e serviços: muitos dados, aplicativos e recursos são concentrados na nuvem. Sem autenticação segura, um intruso pode acessar uma conta de usuário e obter tudo o que estiver na máquina virtual daquele cliente. Para evitar isso, o ideal é monitorar proativamente ameaças de autenticação.

12. Interfaces inseguras de programação de aplicativos: é importante ver a nuvem como uma nova plataforma e não apenas como terceirização quando se trata de desenvolvimento de aplicativos. Deve existir um processo de investigação

relacionado aos ciclos de aplicações, no qual o desenvolvedor entende e aplica certas orientações para controles de autenticação, acesso e criptografia.

13. Abuso da Computação em Nuvem: usuários mal intencionados estão cada vez mais preparados. Registros indicam que crackers estão aplicando novas ameaças rapidamente, além da habilidade de se adaptar ao tamanho da nuvem. E tudo que é preciso é um cartão de crédito.

14. Perfil de risco desconhecido: a questão da transparência continua preocupando os provedores de nuvem. Usuários de contas interagem apenas com a interface final e não sabem muito sobre as plataformas ou níveis de segurança que os provedores estão empregando.

8 BENEFÍCIOS NA UTILIZAÇÃO DE *CLOUD COMPUTING*

Depois de apresenter os riscos e problemas de segurança oferecidos pela computação em nuvem, vamos aos benefícios**.**

Um dos benefícios é a redução de custo. Como na maioria dos negócios, as empresas sempre estão sob pressão para que haja corte de custos, o que é basicamente irreal no tipo de economia que temos, onde sempre há demanda de economia de dinheiro e melhora de margem de lucro.

Com a Computação em Nuvem pode-se diminuir significativamente o capital de invesitmento, pois serviços em nuvem estão disponíveis em modelos onde se paga de acordo com o uso. Isto significa que não há altos gastos inicias para os serviços requisitados, ao menos que haja aquisição de novas aplicações.

Além do mais que se houver melhoria na qualidade de serviço, indiretamente haverá a redução de custos dos serviços da nuvem.

De acordo com Taurion (2009), a Computação em Nuvem trará diversas vantagens de imediato para as organizações que decidirem utilizá-las.

Em um estudo publicado pelo banco de investimentos *Merrill Lynch*, em maio de 2008, intitulado "*The Cloud Wars: $ 100 billion at stake*" é feito a comparação (no mercado norte-americano) entre o modelo tradicional e a *Cloud Computing*. O estudo mostra que para uma empresa utilizando o modelo tradicional cerca de 65% à 85% da capacidade de processamento de um servidor não é utilizado. Este tipo de informação nos leva a crer que comparado ao modelo de computação, podemos afirmar que as organizações somente irão consumir o que realmente demandarem e não terão capacidade de processamento excessiva. Em outras palavras, o *Cloud Computing* provê elasticidade para solucionar problemas de capacidade de processamento, fazendo com que o cliente apenas pague a capacidade que de fato utilizou.

Os custos implicados pelo modelo tradicional de serviços são elevados em comparação ao modelo da Computação em Nuvem. Principalmente pelo fato que independente da empresa estar utilizando o servidor ou não o mesmo encontra-se

ligado 24 horas por dia 7 dias por semana que acaba recursos para manutenção como eletricidade, ar condicionado para resfriamento, entre outros.

Outro benefício é o fato da organização não precisar mais se preocupar com a manutenção dos parques tecnológicos, o que ajuda a melhorar o ROI (*Return on Investments* – retorno sobre investimentos) e o ROA (*Return on Assets* – retorno sobre ativos) para os acionistas da organização.

> A Computação em Nuvem já está aparecendo na tela de radar dos executivos de Tecnologia da Informação. A vantagem principal da utilização do modelo de *Cloud Computing* para clientes corporativos ou residenciais, além dos já mencionados, é por ser um modelo que contempla a criação de um serviço contingencial no caso de perdas de informações ***Taurion (2009).***

Em outras palavras, se houver perda de informações, de clientes residenciais ou corporativos, devido vírus, longa idade do computador, roubo ou desastres como incêndios, por exemplo, é possível a restauração destas informações através do modelo de nuvem. Tudo devido ao fato dos servidores estarem fisicamente armazenados em outra localidade ao redor do mundo.

As nuvens também oferecem *performance*, administração facilitada, updates gratuitos (SaaS/PaaS), aumento de agilidade, facilidade de uso, acessibilidade, entre outros.

9 CASO DE APLICAÇÃO E ANÁLISE DE SEGURANÇA

Antes de mover um ativo para nuvem, deve-se identificar o que está se movendo. Os ativos suportados pela nuvem podem ser divididos em duas categorias:

- Dados
- Aplicações/Funções/Processamento

Com a Computação em Nuvem, nossos dados ou aplicações não precisam estar em uma mesma localidade, ou seja, podemos mudar apenas pequenas funções para a nuvem. Um exemplo seria: podemos hospedar as aplicações e dados no *data center* da empresa, quando ainda há terceirização de uma parte através da nuvem pelo modelo *Platform as a Service*.

A primeira checagem de avaliação de segurança de uma nuvem é determinar minuciosamente qual é o dado será armazenado ou a função que se moverá para a nuvem. Esta análise deve incluir uma análise exata de utilização do ativo, uma vez que o mesmo seja transferido para uma nuvem.

Sendo assim, deve-se:

1. Avaliar o ativo

Determinar qual a importância do dado ou função para a empresa ou usuário. Dificilmente consegue-se avaliar o ativo, pois as organizações não mantêm um processo para isso. Mas é necessária ao menos, uma avaliação de quão importante e sensível é o ativo.

Como poderíamos ser prejudicados se o ativo se tornou amplamente público e distribuído?

Como poderíamos ser prejudicados se um funcionário do provedor de serviço de nuvem acessou o ativo?

Como poderíamos ser prejudicados se o processo ou função foi manipulado por terceiros?

Como poderíamos ser prejudicados se o processo ou função falhar ao fornecer os resultados esperados?

Como poderíamos ser prejudicados se a informação/dado for alterada inesperadamente?

Como poderíamos ser prejudicados se o ativo estiver indisponível por um período de tempo?

Com as perguntas acima, analisamos confidencialidade, integridade e disponibilidade e como o ativo será afetado na nuvem.

É parecido com uma análise de projeto de terceirização de serviços, porém na Computação em Nuvem há uma grande gama de opções de implementação.

2. Mapear o Ativo ao Modelo de Implantação em Potencial

Após mapear os ativos, devemos entender a importância do mesmo, para poder selecionar o modelo mais confortável a ser adotado, que preencha os requisitos de segurança.

Antes de procurar por provedores de nuvem, devemos analisar os modelos a ser utilizados para então aceitar os riscos de segurança implícitos em nuvens privadas, públicas, comunitárias ou híbridas e aos modelos de hospedagem interno, externo ou misto.

De acordo com o *Cloud Security Alliance* (2010)*:*

Para cada ativo, determine se você está disposto a aceitar as seguintes opções:

- Público.
- Privado, interno/dentro da organização.
- Privado, externo (incluindo infraestrutura dedicada ou compartilhada).
- Comunitário, levando em conta o local da hospedagem, provedor de serviço em potencial e identificar outros membros da comunidade.
- Híbrido. Para avaliar efetivamente o potencial de implantação hibrida, você deve ter em mente pelo menos uma estrutura aproximada de onde os componentes, funções e dados serão hospedados.

Nesta fase, deve-se ter total compreensão e conforto em transferir os dados para um modelo de nuvem, além de escolher um local de implementação adequado para os requisitos de segurança e risco.

3. Avaliar Potenciais Modelos de Serviços na Nuvem e Provedores

Neste passo, o principal é avaliar o grau de controle que se terá em caso de necessidade de gerenciamento de riscos. Ou seja, deve-se analisar o fornecedor e os riscos oferecidos.

4. Esboçar o Potencial Fluxo de Dados

Nesta fase, é necessário analisar o fluxo de dados entre o usuário, o serviço da nuvem e qualquer outro ponto de acesso.

Antes de implementar a Computação em Nuvem, é de extrema necessidade entender como os dados podem se mover dentro e fora da nuvem

Com os passos acima, é possível entender a importância de analisar o que se moverá para a nuvem antes de sua implementação, além de identificar o modelo a ser utilizado.

Para ativos menos valiosos não precisa ter o mesmo nível de controles de segurança e podem-se pular muitas das recomendações – como inspeções locais, facilidade de descoberta e esquemas complexos de criptografia. Um ativo valioso e regulamentado implicará em requisitos de auditoria e retenção de dados. Para outros ativos valiosos e não sujeitos a restrições de regulamentações, pode focar mais em controles técnicos de segurança. Nem todas as implantações de nuvem precisam de todos os controles de risco e segurança possíveis. *Cloud Security Alliance* (2010).

9.1 O *Cloud Computing* em Residências

Serviços de Computação em Nuvem para o mercado residencial começam a ser divulgados pela Internet por trás de grandes marcas como: Google, Microsoft, Amazon e Symantec.

Estes serviços são oferecidos de forma gratuita e outros são pagos, porém a característica principal deste tipo de nuvem é a garantia contra a perda de documentos, planilhas, arquivos e fotos dos usuários.

A empresa Symantec (desenvolvedora do sistema de antivírus Norton), por exemplo, incluiu o serviço de Computação em Nuvem no seu programa antivírus Norton 360, que além de garantir a proteção do computador doméstico contra vírus, *hackers*, *spams* e falhas do sistema operacional, o Norton 360 também faz *backups* automáticos de pastas pré-definidas (como a pasta Meus Documentos, por exemplo, do sistema operacional Microsoft Windows).

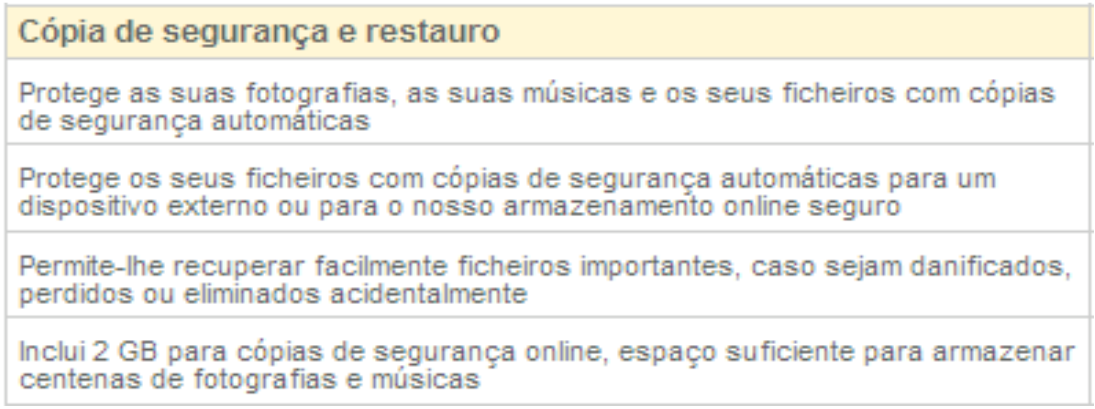

Figura 9 - Descrição de *Cloud Computing* do Norton 360 Versão 5.0. Fonte: http://antivirus.norton.com/norton. Acessado em: 11 novembro 2010 – 21h412min.

Para a instalação do Norton 360 necessita-se de no mínimo:

Requisitos do sistema operacional:

- Microsoft® Windows® XP (32 bits) com Service Pack 2 ou posterior Home/Professional/Media Center.
- Microsoft® Windows Vista® (32 bits e 64 bits) Starter/Home Basic/Home Premium/Business/Ultimate.
- Microsoft® Windows® 7 (32 bits e 64 bits) Starter/Home Basic/Home Premium/Professional/Ultimate.

Requisitos mínimos de hardware**:**

- Processador de 300 MHz ou mais rápido.
- 256 MB de RAM (512 MB recomendados).
- 300 MB de espaço disponível no disco rígido.
- Precisa atender os requisitos mínimos do sistema operacional Microsoft Windows XP/Vista/Win7.
- Internet Explorer® 6.0 ou superior, ou Mozilla Firefox® 3.0 ou superior.
- Conexão com a Internet (conexão de alta velocidade necessária para o backup on-line).

Nas figuras podemos ver como o Norton 360 trabalha.

A figura 10 mostra uma tela do Norton 360, onde há armazenamento de arquivos em nuvem.

A figura 11 exibe a janela de gerenciamento de *backups* do Norton 360.

A figura 12 mostra a tela do que está definido para que o Norton 360 faça o backup automático.

Os arquivos selecionados pelos usuários são enviados ao servidor da Symantec que estão em nuvem.

Os arquivos podem então serem acessados a qualquer momento, de qualquer lugar com o *login* e senha e solicitar a restauração em caso de perda ou necessidade.

A figura 13 mostra a página do *Nortonmyaccount* que mostra a visualização dos documentos salvos no servidor para *download*.

Figura 10 - Tela inicial do Norton 360. Fonte: SYMANTEC (2010).

Figura 11 - Tela de gerenciamento dos *backups* do Norton 360. Fonte: SYMANTEC (2010).

Figura 12 - Tela da definição de quais arquivos deverão ser armazenados na nuvem. Fonte: SYMANTEC (2010).

Figura 13 - Tela da Internet do Nortonmyaccount que permite o *download* dos documentos salvos. Fonte: SYMANTEC (2010).

9.2 Análise de Segurança

Ativos selecionados para serem armazenados na nuvem: Fotos pessoais, relatórios da faculdade, músicas, etc.

Grau de controle da empresa: Total controle sob os dados na nuvem.

Potencial Fluxo de Dados: Fluxo de dados mediante a senha.

Se analisarmos o cenário de segurança no ambiente de Computação em Nuvem apresentado acima (Norton 360), podemos perceber que antes da utilização deste tipo de serviço, um modelo de governança de segurança deve ser adotado a fim de mitigar os riscos inerentes do modelo de prestação de serviços na nuvem a usuários domésticos.

> A percepção de que a nuvem é um aglomerado de informações pode caracterizá-la como sendo um alvo propício a ataques por potenciais invasores. Ameaças como esta podem afetar diretamente os pilares da segurança da informação: disponibilidade, confidencialidade e integridade, e conseqüentemente comprometer toda a nuvem ***Turion (2009).***

Sendo assim, temos uma tabela com a avaliação de segurança dos ativos listados previamente. A mesma visa responder o que será feito se os arquivos pessoais forem roubados, destruídos, alterados e/ou manipulados por terceiros.

Com os dados mostrados, percebemos que a Norton tem total responsabilidade sobre os dados armazenados na nuvem e promete aplicar os princípios de segurança listados na tabela 2.

Tabela 2 - Análise de Segurança e Risco do Antivírus Norton 360

Princípios da Segurança	Cenário do Risco	Questões	Norton
Integridade	Invasões por hackers aos ambientes da nuvem. Violação de leis de proteção de dados.	Quais são as garantias sobre a preservação da integridade dos dados?	A Symantec oferece total garantia sobre a preservação e integridade dos dados.
Confidencialidade	Aplicações de diversos usuários estão nos mesmos sistemas de armazenamento.	Como é protegida a propriedade intelectual e segredos comerciais dos dados?	Utilização de senha.
Disponibilidade	Recuperação de dados gerenciados por terceiros.	Como é garantida a arquitetura de disponibilidade? A recuperação de informações críticas, está sujeita a atrasos?	Disponibilidade total dos dados armazenados. Não está sujeito a atrasos.
Autenticidade	Verificação da autenticidade das entidades comunicantes.	Que recursos são utilizados na autenticação e controle de acesso dos usuários?	Login e senha.
Não-repúdio	Auditabilidade das ações executadas por usuários no sistema.	Os usuários do modelo são capazes de negarem suas ações?	Os usuários não são capazes de negarem suas ações

10 DADOS ESTATÍSTICOS

Hoje, segurança é uma das primeiras barreiras quando falamos em Computação em Nuvem.

Para que as organizações movam seus recursos de computação e aplicações para a nuvem, o valor deve exceder o risco. Os riscos da migração de nuvens se resumem em uma palavra - "Segurança"

Grande parte das empresas ou usuários que não estão adotando a Computação em Nuvem, citam a segurança como a principal razão.

Aprofundando, as organizações se preocupam muito ainda com a segurança na proteção de dados, integridade (controles de acesso e vulnerabilidades), e disponibilidade.

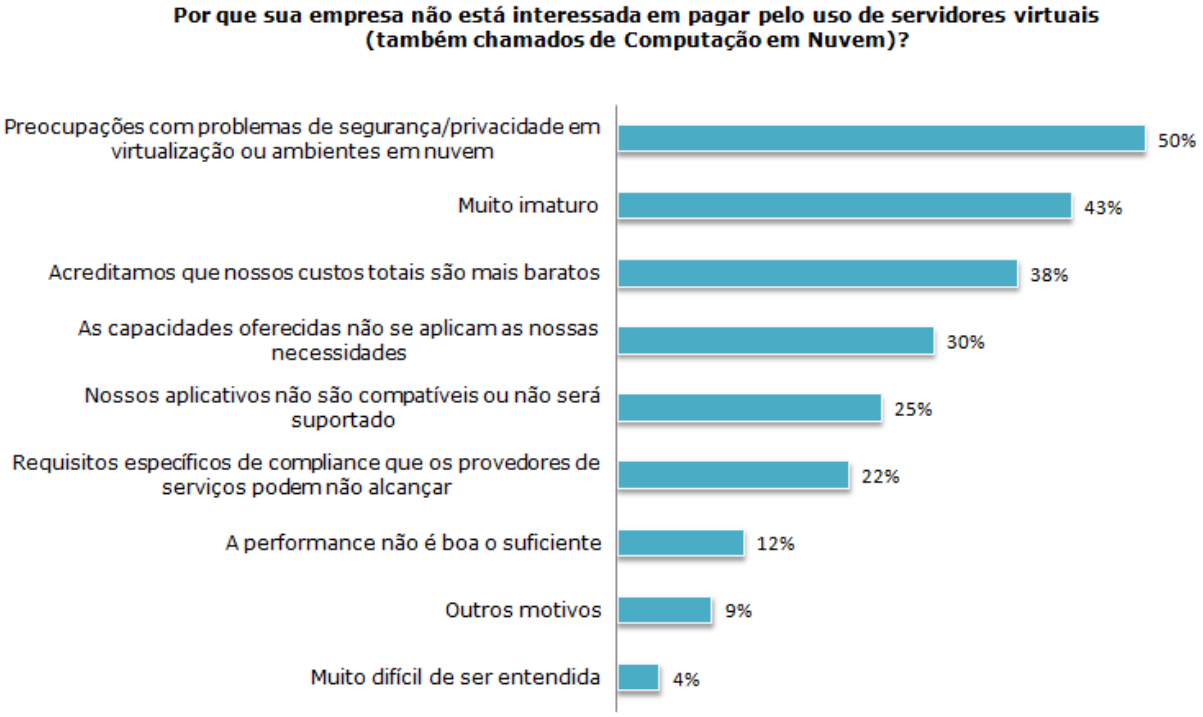

Figura 14 – Segurança e Privacidade são os primeiros fatores para não adotar o modelo de nuvem. Dados mostram que 50% das empresas não estão dispostas a pagar conforme o uso, devido a problemas de segurança. Mais 43% diz que a tecnologia é imatura. Fonte: Penn (2010).

Porém se comparamos os problemas de segurança com os serviços de nuvem, eles não preocupam tanto a maioria das empresas, tanto quanto outras tendências de TI, como *smartphone* ou a proliferação de mídias sociais.

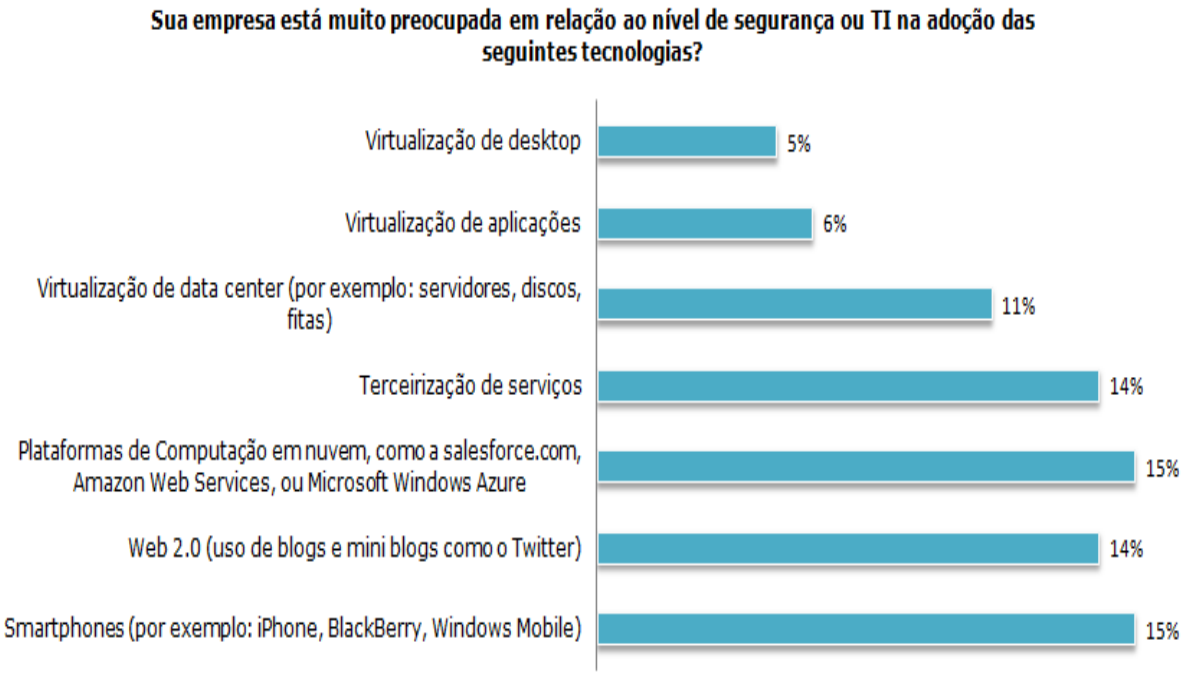

Figura 15 – Quanto preocupada está sua empresa sobre o nível de segurança ou risco em TI em relação à adoção diferentes tecnologias. Dados mostram que 15% das empresas estão muito preocupadas com problemas de segurança relacionados à *smartphones*. Empatado está o *Cloud Computing*. Fonte: Penn (2010).

Ao longo prazo, acredita-se que segurança não será a principal característica de venda dos serviços na nuvem, nem um grande diferencial entre os provedores de *Cloud Computing*. Sua grande proposição de venda continuará centrada nos benefícios de negócios de TI e no valor derivado da eficiência dos recursos que reduzem dia-a-dia os encargos operacionais.

Mesmo assim, para os próximos anos, a indústria de tecnologia terá a oportunidade de melhorar a segurança de ambientes de nuvem através do desenvolvimento de novas soluções adequadas para o mercado.

TENDÊNCIAS DE *CLOUD COMPUTING*

11.1 Tendências no mundo

De acordo com a mesma pesquisa da Cisco (2010), as tendências mundiais de *Cloud Computing* são:

- Uso futuro de nuvens: A grande maioria (88%) dos entrevistados de TI prevê a armazenagem de alguma porcentagem dos dados e aplicativos das suas empresas em nuvens privadas ou públicas nos próximos três anos.
- Nuvens privadas: Um em cada três profissionais de TI disse que mais da metade dos dados e dos aplicativos das suas empresas estarão em nuvens privadas nos próximos três anos. A previsão da adoção de nuvem é mais alta no México (71%), Brasil (53%) e EUA (46%).
- *Timing* para nuvens públicas: Dos entrevistados nos treze países que afirmaram que irão usar nuvens públicas, um em cada três (34%) pretende fazê-lo em um ano, e 44% dizem que suas empresas irão usar nuvens públicas dentro de dois anos, enquanto que 21% dentro de dois ou três anos.

11.2 Tendências no Brasil

Mesmo com diversos problemas relacionados à segurança, o Brasil está superando a média mundial na adoção de *Cloud Computing .*

As empresas instaladas no Brasil estão à frente da média mundial no uso de tecnologias como *Cloud Computing*. De acordo com o estudo mundial Cisco Connected World, 27% das companhias no país já utilizam aplicações baseadas em *Cloud Computing*, enquanto que a média mundial é de 18%. A Alemanha aparece

empatada com o Brasil neste quesito, seguida da Índia (26%), Estados Unidos (23%) e México (22%). Cisco (2010).

Sendo assim, nosso país permanecerá acima da média mundial nos próximos anos, pois a estimativa é que 70% das companhias possuam a tecnologia - ficando abaixo apenas da Índia (76%). A média mundial do ano de 2010 foi de 52%.

Para Marcelo Ehalt, diretor de engenharia da Cisco Brasil, a pesquisa mostra o amadurecimento do Brasil na utilização do *Cloud Computing*. "Até pouco tempo, as empresas perguntavam o que era *Cloud Computing* e hoje querem saber de que forma adotar a tecnologia, pois já entenderam sua importância e benefícios, como redução de custos e ganho de flexibilidade e agilidade em TI", destaca o executivo.

A pesquisa "*Cisco Connected World Report*" foi realizada em 13 países: Brasil, EUA, México, Reino Unido, França, Espanha, Alemanha, Itália, Rússia, Índia, China, Japão e Austrália, entre 16 de agosto e 7 de setembro de 2010.

11.3 Companhias com diferentes motivações para alavancar o uso de *Cloud Computing*

Diferentes companhias da área de tecnologia da informação estão estabelecendo mercado em *Cloud Computing* no Brasil e no mundo. Empresas como a Google, IBM e Microsoft foram as pioneiras a enfrentar esta nova era digital.

A tecnologia que antes era utilizada apenas em laboratórios, agora esta ingressando em grandes mercados no mundo todo.

Se analisarmos a figura 16, podemos ver que empresas como a AT&T, Google, EMC/VMware, Sun, Amazon, HP, Intel, Yahoo, Citrix, Netsuite, Salesforce.com, Microsoft, SAP, Dell, Oracle, entre outas, oferecem ou planejam oferecer o serviço em nuvem.

Algumas empresas como a Microsoft, oferecem os três tipos de serviços que são: SaaS, PaaS e IaaS.

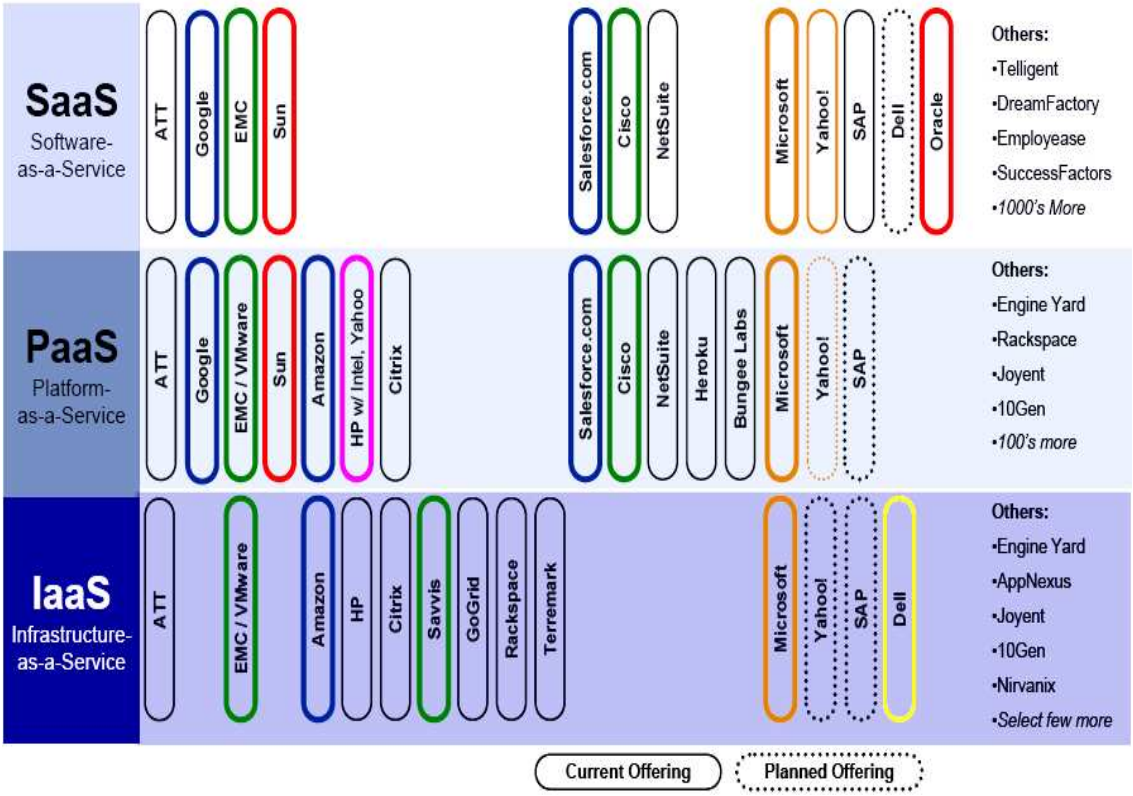

Figura 16 – Diferentes companhias que oferecem o serviço *Cloud Computing*. Fonte: IBM Corporate Strategy, IBM MI, STG, Tivoli (2010).

12 CONSIDERAÇÕES FINAIS

Com o estudo feito sobre o tema *Cloud Computing*, podemos conhecer mais a história, a arquitetura e os modelos oferecidos pelo serviço na nuvem, além de aprofundar na questão que é a grande preocupação neste tipo de tecnologia: a Segurança.

Considerando os dados coletados para esta monografia, podemos concluir que com o crescente avanço da utilização da internet, da computação em nuvem e armazenamento de dados por empresas terceirizadas, a segurança dos dados é fundamental, porém ainda um risco.

De fato, *Cloud Computing* é um assunto muito complexo e de extensa abrangência na área de Tecnologia da Informação, em especial para as organizações que contratam este tipo de serviço e temem com problemas de integridade, confidencialidade, disponibilidade, autenticidade e não repúdio gerados pela nuvem.

Diversos estudos ainda são realizados para que haja mitigação e futuramente menor presença de objeções sobre esta tecnologia, pois estas objeções muitas das vezes acarretam na falta de interesse de aplicação deste modelo em novas empresas e residências.

Ou seja, podemos ver que por maiores e atraentes que possam ser os benefícios relacionados ao menor custo, menor capital de investimento e menor risco de perda de dados (já os mesmos estão na “*web*”), ainda desconfia-se da eficácia na utilização do *Cloud Computing*.

De certa maneira, podemos concluir também que serviços hospedados em nuvens de menor porte, como o oferecido pelo antivírus Norton 360, não possuem falhas de segurança consideráveis, pois geralmente os dados armazenados são de caráter pessoal (fotos, músicas, vídeos, trabalhos escolares, entre outros). Sendo assim, o impacto ao usuário em caso de danos é baixo (como mostra a análise feita durante este trabalho).

Porém se falarmos de empresas de grande porte que usam a nuvem através de serviços oferecidos na maioria das vezes pelas empresas Google, Microsoft, IBM, Amazon, etc, qualquer perda, invasão e/ou modificação, podem causar impactos gigantes, onde envolve dinheiro, dados valiosos, SLA, multas e até cancelamento de contrato.

Mesmo estando cotado para ser a tecnologia do futuro, e alguns dizerem que é a tecnologia da vez, há muito para se aprender, estudar e melhorar quando entramos no quesito SEGURANÇA.

Se esta tecnologia perdurar como previsto, que venham as melhorias na área de Tecnologia da Segurança da Informação e permaneçam os benefícios já oferecidos!

REFERÊNCIAS BIBLIOGRÁFICAS

AMRHEIN, D., QUINT, S. **Cloud Computing for the enterprise: Part 1: Capturing the Cloud**. IBM. 2009. Disponível em: <http://www.ibm.com/developerworks/websphere/techjournal/>. Acesso em: 24 agosto 2011.

AULBACH, S., JACOBS, D., KEMPER, A et all. **A Comparison of Flexible Schemas for Software as a Service**. 35th SIGMOD - International Conference on Management of Data, 2009.

BUECKER, A., LODEWIJKX, K., MOSS, H et al. **Cloud Security Guidance: IBM Recommendations for the Implementation of Cloud Security**. IBM Redpaper. Poughkeepsie, novembro, 2010.

CISCO (Brasil). **Brasil supera média de cloud computing**. CISCO. 2010. Disponível em: < http://www.brasscom.org.br/en/box_brasscom_news/brasil_ supera_media_de_cloud_computing>. Acesso em: 04 novembro 2011.

COLE, Dave. **Cloud Antivirus Forecast: Foggy, with a Chance of Irrelevance**. Disponível em: <http://www.baboo.com.br/conteudo/modelos/Norton-AntiVirus-2010-e-Internet-Security-2010-Trial_a36312_z0.aspx>. Acesso em: 02 novembro 2011.

CSA (Cloud Security Alliance). **Guia de Segurança para Áreas Críticas Focado em Computação em Nuvem**. São Paulo, dezembro, 2010.

IBM (Brasil). **Essentials of Cloud Computing**. IBM. 2009. Disponível em: <https://w3-01.sso.ibm.com/learning>. Acesso em: 02 outubro 2011.

IDG (EUA). **Cloud Computing researches**. International Data Group. 2010. Disponível em: <http://www.idg.com/www/SearchIDG.nsf/ByID/IDGC-8NKHQX>. Acesso em: 07 setembro 2011.

INTEL NEXTGENERATION (Brasil). Intel (Org.). **Dialogo TI – Cloud Computing.** Disponível em: <www.nextgenerationcenter.com>. Acesso em: 10 outubro 2011.

GARTNER. **Conheça os Sete Riscos de Segurança em Cloud Computing**. Computer World. 2008. Disponível em: <http://computerworld.uol.com.br/negocios>. Acesso em: 02 setembro 2011.

LEIF. **Advantages of Cloud Computing**. Disponível em: <http://www.fcontactdubai.com%2Fadvantages-of-cloud-computing>. Acesso em: 17 setembro 2011.

LOWE, Janet. **Google**. Rio de Janeiro: Campus, 2009.

MILLER, J., Candle, L., Wald, H. **Information Security Governance: Government Considerations for the Cloud Computing Environment**, August 2009 – USA . Disponível em<http://boozallen.com/publications>. Acesso em: 17 setembro 2011.

MULLER, Nicolas**. Computação nas nuvens**. Disponível em: **<**http://www.oficinadanet.com.br/artigo/923/computacao_nas_nuvens>. Acesso em: 16 setembro 1011.

NIST (National Institute of Standards and Technology) – **The NIST Definition of Cloud Computing**, Version 15, 10-7-2009, National Institute of Standards and Technology, Information Technology Laboratory – Gaithersburg, Maryland – USA. Disponível em: <http://www.nist.org>. Acesso em: 01 novembro 2011.

POUJOL, Mathieu. **PAC Paris Webinar Series: Global Trends in Cloud Computing**. Poughkeepsie, março, 2010.

TAURION, Cezar. **Computação em Nuvem: Transformando o Mundo da Tecnologia da Informação**. Rio de Janeiro: Brasport, 2009.

GLOSSÁRIO

Abstração. Habilidade de concentrar nos aspectos essenciais de um contexto qualquer, ignorando características que não são tão importantes.

Backup. Cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

Compliance. Estar em conformidade com leis e regulamentos internos e externos.

Data Center. Central de Dados, na qual servidores são alocados.

Design. Atividade técnica e criativa, normalmente orientada por uma intenção ou objetivo, ou para a solução de um problema.

Download. Cópia um arquivo da rede para o computador.

Client - Server. Modelo computacional que separa clientes e servidores, sendo interligados entre si geralmente utilizando-se uma rede de computadores.

Cloud. Nuvem. É o local onde os dados da tecnologia computação em nuvem são armazenados.

Frameworks. Conjunto de conceitos usado para resolver um problema de um domínio específico. Não se trata de um software executável, mas sim de um modelo de dados para um domínio***.***

Hardware. Equipamento físico usado para atividades de entrada, processamento e saída de um sistema de informação

Login**.** Nome que o usuário utiliza para acessar um servidor da rede. Para entrar na rede, é preciso entrar com a identificação (*login*), seguido de uma senha (*password*).

Mainframe. Computador muito grande e caro capaz de suportar centenas, ou até mesmo milhares, de usuários simultaneamente.

Merrill Lynch. Banco norte-americano de investimentores e provedores de outros serviços financeiros.

Middleware. No campo de computação distribuída, é um programa de computador que faz a mediação entre outros softwares. É utilizado para mover informações entre programas ocultando do programador diferenças de protocolos de comunicação, plataformas e dependências do sistema operacional.

Nortonmyaccount. Tela do programa Norton 360 que mostra os dados dos us ários e os arquivos armazenados na nuvem.

Performance. Conjunto dos resultados obtidos em um teste.

Service Level Agreement. É um acordo firmado entre a área de TI e seu cliente interno, que descreve o serviço de TI, suas metas de nível de serviço, além dos papéis e responsabilidades das partes envolvidas no acordo.

Software. Consiste em instruções detalhadas e pré-programadas que controlam e coordenam os componentes do *hardware* de um sistema de informação

Timming. Sensibilidade para o momento propício de realizar ou de ocorrer algo, ou senso de oportunidade quanto à duração de um processo, uma ação.