ASPECTOS DA SEGURANÇA DA COMPUTAÇÃO EM NUVENS

Rafael Assis de Jesus[1]
Jamylle Santana da Fonseca(FAT) [2]

RESUMO: A computação em nuvem é uma tendência recente de tecnologia que pretende serglobal e prover serviços para todos, desde hospedag em de documentos pessoais na Internet até terceirização de toda a parte de TI para outras emp resas. Porém, alguns questionamentos são levantados, como a segurança de suas informações, o risco de alguém invadir o servidor e ter acesso aos dados das organizações que lá hospedam seus serviços, o que pode eventualmente gerar transtornos vitais, como o compartilhamento de dados por concorrentes, ou mesmo a alteração original dos dados, levando a tomada de d ecisões equivocadas.

Palavras-chave: Computação em Nuvens; Segurança da Informação; In ternet.

ASPECTS OF SECURITY IN CLOUDING COMPUTER

ABSTRACT: Cloud computing is a recent trend of technology that aims to be comprehensiveand provide services for everyone from hosting personal documents on the Internet by out sourcing all part of IT to other companies. However, some questions are raised, such as the security of your information, the risk of someone breaking into the server and access the data from their organizations that host their services, which may eventually generate vital disorders such as data sharing by competitors, or even change the original data, leading to erroneous decisions.

Keywords: Cloud Computing, Information Security, Internet

1. INTRODUÇÃO

O artigo tem como objetivo apresentar a computação em nuvens como um modelo favorável de armazenamento de arquivos e aplicativos na internet do futuro, mas também apresentar aspectos relevantes a cerca da segurança dos dados em nuvens.

A palavra nuvem sugere uma ideia de ambiente desconhecido. Por este motivo esta foi muito bem empregada na nomenclatura deste novo modelo, onde toda a infraestrutura e recursos computacionais ficam escondidos, tendo o usuário o acesso apenas a uma interface padrão através da qual é disponibilizado todo o conjunto de variadas aplicações e serviços (SILVA, 2010).

A nuvem é representada pela internet, isto é, a infraestrutura de comunicação composta por um conjunto de hardwares, softwares, interfaces, redes de telecomunicação, dispositivos

[1] Estudante do curso de Redes de Computadores da Faculdade Anísio Teixeira – FAT . e-mail: <rafael.brasa@hotmail.com>
[2] [2] Profª. Ms. do curso de Redes de Computadores da Faculdade Anísio Teixeira-FAT. E-mail: <jamyllesantana@hotmail.com>

de controle e de armazenamento que permitem a entrega da computação como serviço (HURWITZ et. all, 2010).

Com a computação em nuvem, os usuários estarão movendo seus dados e aplicações para a nuvem, podendo acessá-los de forma simples ede qualquer local. Isso é novamente um caso de utilização de processamento centralizado. C omputação em nuvem é, portanto, uma maneira bastante eficiente de maximizar e flexibilizar os recursos computacionais. Além disso, uma nuvem computacional é um ambiente redundante e resiliente por natureza. Resiliente pode ser definido como a capacidade de um sistema de informação continuar a funcionar corretamente, apesar do mau funcionamento de um ou mais dos seus componentes (TAURION, 2009).

A computação em nuvem surge da necessidade de const ruir infraestruturas de TI complexas, onde os usuários não têm que realizar instalação, configuração e atualização de softwares. Além disso, recursos de computação e hardware são propensos a ficarem obsoletos rapidamente. Assim, a utilização de plataformas com putacionais de terceiros é uma solução inteligente para os usuários lidarem com infraestrutura de TI.

O desenvolvimento do artigo foi delimitado por uma pesquisa bibliográfica com o objetivo de apresentar o conhecimento científico acumulado sobre o problema.

A seção 2 expõe alguns problemas relacionados à for ma de armazenamento da informação. A seção 3 apresenta a definição de comp utação em nuvens, bem como a infraestrutura e ferramentas necessárias para utilização do serviço. Na seção 4 foram expostos alguns problemas de segurança que devem ser resolvi dos para um armazenamento em nuvens eficiente. A seção 5 finaliza o artigo com a exposi ção das considerações finais do trabalho.

2. PROBLEMAS COM A INFORMAÇÃO

A noção que se tem de informação é bem vago e intui tivo. A palavra ―informaç ão , segundo Teixeira (2005), sempre foi ambígua e liberalmente empregada para definir diversos conceitos. Os dicionários registram que a palavra emt sua raiz no latim *informare*, que significa ―a ação de formar matéria, tal como pedra, madeira, couro etc. A definição mais comum é: a ação de informar; formação ou moldagem d a mente ou do caráter, treinamento, instrução, ensinamento, comunicação de conhecimento instrutivo.

Conforme a *International Organization for Standardization* (ISO/IEC 17799, 2005), a informação pode existir em diversas formas. Ela pod e ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada

em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

Dispositivos de armazenamento de dados eletrônicos de alta capacidade como servidores de arquivos, redes de área de armazenamento são caros. Além disso, dispositivos de armazenamento de dados eletrônicos têm muitos inconvenientes, tem tempo de vida útil, exigem sistemas de backup e recuperação, exigem con dições ambientais específicas, exigem pessoal para gerenciar e consumem quantidades consideráveis de energia para alimentação e resfriamento.

A conectividade oferecida pela Internet também introduziu uma série de facilidades no dia-a-dia das pessoas, como: downloads, games *online*, shopping *online*, transações financeiras e a própria *World Wide Web*, dentre muitas outras, permitindo o acesso quase que anônimo a quase todos os tipos de informações. Sabe-se que no mundo ―real não existem sistemas totalmente seguros e o mundo ―virtual segue esse mesmo preceito. Por maior que seja a proteção adotada, o usuário sempre estará sujeito ainvasões, roubos e ataques.

Apesar dos benefícios de captar a computação nas nu vens de alguém, existem armadilhas potenciais. Uma delas é a segurança. Você deve confiar em um estranho para proteger seus aplicativos e informações neles conti das?

A segurança da informação pode ser definida como um conjunto de medidas que se constituem basicamente de controles e políticas de segurança, tendo como principal objetivo a proteção das informações de clientes e empresa (ben s/ativos), controlando o risco de revelação ou alteração por pessoas não autorizadas (ISO/IEC 1 7799, 2005).

De acordo com Cunha (2005), podemos definir ameaças como sendo agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades.

As ameaças, quanto a sua intencionalidade, podem se r divididas nos seguintes grupos:

Naturais: são decorrentes de fenômenos da natureza, como incêndios, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento e poluição. Involuntárias:

são ameaças inconscientes, quase sempre causadas pelo desconhecimento, elas podem ser causadas por acidentes, erros, faltas de energia e etc.

Voluntárias: são propositais, causadas por agentes humanos como hackers, invasores, espiões, ladrões e etc.

3. COMPUTAÇÃO EM NUVENS: DEFINIÇÃO

A computação na nuvem ou *Cloud Computing* é um novo modelo de computação que permite ao usuário final acessar uma grande quantidade de aplicações e serviços em qualquer lugar e independente da plataforma, bastando para isso ter um terminal conectado à ―nuvem.

O normal é utilizar aplicações instaladas em nossos próprios computadores, assim como a armazenar arquivos e dados dos mais variados tipos neles. Em empresas a realidade é diferente, já que é mais fácil encontrar aplicaçõesdisponíveis em servidores que podem ser acessadas por qualquer terminal autorizado por meio de uma rede.

A principal vantagem do modelo tradicional está nofato de ser possível, pelo menos na maioria das vezes, utilizar as aplicações mesmo sem acesso à internet ou à rede. Em outras palavras, é possível usar estes recursos de maneira *off-line*. Entretanto, todos os dados gerados estão restritos a este computador, exceto quando co mpartilhados em rede, coisa que não é muito comum no ambiente doméstico. Mesmo no ambiente corporativo, isso pode gerar algumas limitações, como a necessidade de se ter uma licenç a de um determinado software para cada computador, por exemplo.

Em contrapartida a evolução nos permite um acesso à internet cada vez mais amplo e mais rápido. Nos países desenvolvidos, tais como Japão, Alemanha e Estados Unidos, já é possível um acesso rápido à Internet pagando-se pouco. O que vem a favorecer a popularização da *Cloud Computing*, embora esse conceito esteja se tornando conhecido no mundo todo, inclusive no Brasil.

Para utilizarem os serviços, os usuários necessitam apenas ter em suas máquinas um sistema operacional, um navegador e acesso a Internet. Todos os recursos computacionais estão disponíveis na nuvem e as máquinas dos usuários nãonecessitam ter altos recursos computacionais, diminuindo o custo na aquisição de máquinas. Todo hardware pode ser utilizado para realizar alguma tarefa que seja adequada ao seu poder de processamento. Novos recursos de hardware podem ser adicionados a fim de aumentar o poder de processamento e cooperar com os recursos existentes.

A infraestrutura do ambiente de computação em nuvem normalmente é composta por um grande número, centenas ou milhares de máquinasfísicas ou nós físicos de baixo custo, conectadas por meio de uma rede. Cada máquina física tem as mesmas configurações de software, mas pode ter variação na capacidade de ha rdware em termos de CPU, memória e armazenamento em disco (Soror et al. 2010).

Com essa tecnologia muitos aplicativos, assim como arquivos e outros dados relacionados não precisam mais estar instalados ou armazenados no computador do usuário ou em servidores. Estes ficam disponíveis nas nuvens, isto é, na Internet. O fornecedor da aplicação se responsabiliza desenvolvimento, armaze namento, manutenção, atualização, backup, escalonamento, etc. O usuário não precisa se preocupar com nada disso, apenas com acessar e utilizar.

Alecrim (2008) destaca as principais características da Computação nas Nuvens:

Acesso às aplicações independente de sistema operac ional ou hardware;

O usuário não precisará se preocupar com a estrutura para execução da aplicação: hardware, backup, controle de segurança, manutenção , entre outros, ficam a cargo do fornecedor de serviço;

Compartilhamento de dados e trabalho colaborativo se tornam mais fáceis, uma vez que todos os usuários acessam as aplicações e os dados do mesmo lugar;

Dependendo do fornecedor, o usuário pode contar comalta disponibilidade, já que, se, por exemplo, um servidor parar de funcionar, os demais que fazem parte da estrutura continuam a oferecer o serviço.

Já Souza et al. (2009) identifica outras características relevantes, como:

Self-service sob demanda. Onde o usuário pode adquirir unilateralmente recursocomputacional, como tempo de processamento no servidor ou armazenamento na rede na medida em que necessite e sem precisar de interação humana com os provedores de cada serviço.

Amplo acesso. Os recursos são disponibilizados por meio da rede e acessados através de mecanismos padronizados que possibilitamo uso por plataformas *thin* ou *thinclient*, tais como celulares, laptops e PDAs;

Serviço medido. Sistemas em nuvem automaticamente c ontrolam e otimizam o uso de recursos por meio de uma capacidade de medição. A automação é realizada em algum nível de abstração apropriado para o tipo de serviç o, tais como armazenamento, processamento, largura de banda e contas de usuário ativas.

Manoel Lemos (2012), diretor geral digital da Abril Mídia, publicou na revista Exame Info do mês de maio deste ano, a importância do papel dos arquitetos dos sistemas de computação na nuvem. São eles, os arquitetos, que d esenharam os mecanismos de integração, de segurança, de suporte a falhas e de operação des sa nova geração de serviço. Outro ponto importante é a responsabilidade de quem oferece os serviços, as questões dos direitos e obrigações se tornam cada vez mais complexa. Vender computação pelo tempo de uso, e em

breve pelo consumo de energia pela infraestrutura, levantam algumas questões do tipo, quem esta usando e pra que esta usando e que tipo de dados é armazenado na infraestrutura? Quando virtualizamos e distribuímos a infraestrutura computacional de nossas vidas, empresas, produtos e serviços é preciso entender bem que entramos em um mundo com outras regras, com uma dinâmica muito acelerada e com uma volatilidade que é parte de sua natureza.

3.1 Infraestrutura, Ferramentas e Serviços

Atualmente, as organizações estão implementando trê s modelos principais de fornecimento de nuvens: privado, público e híbrido. Segundo a Academia de Tecnologia da IBM (2010), em nuvens privadas, as atividades ou funções de TI são fornecidas como um serviço, através da intranet, dentro da empresa e protegida pelo *firewall* da organização. Em nuvens públicas, as atividades ou funções de TI são fornecidas como um serviço através da Internet. Em nuvens híbridas, os métodos internos e externos de fornecimento são integrados, com as atividades ou funções feitas cm base nas exi gências de segurança, na arquitetura de estado crítico e outras políticas estabelecidas.

Com a evolução deste modelo, é capaz de temos máquinas com o mínimo de equipamento possível: uma placa-mãe, processador, R AM e pouca quantidade de espaço na memória persistente, rodando apenas um sistema oper acional e um *browser* conectado à internet. Basta isso para nós usufruirmos normalmen te como hoje, mas todo o processo nas nuvens. Outra vantagem proporcionada por este projeto é a ausência de travamentos no desktop, onde tudo será feito através de grandes servidoresde aplicativos, ocorrendo distribuição de dados em toda a nuvem, continuando a execução de um a solicitação.

Sendo a evolução dos sistemas operacionais em nuven s, poderá possibilitar ainda mais a simplificação de computadores físicos conectados no sistema, na qual necessita-se de um simples programa para acessar o *browser*, chegando até a nuvem desejada. Com esta redução de componentes nos computadores, poderá ocorrer quedas significativas no preço dos mesmos, facilitando o seu uso e a própria manutenção.

3.1.1 Software como Serviço (SaaS)

Este talvez seja o modelo mais fácil de entender doponto de vista de quem está adquirindo o serviço e provavelmente é o modelo que vai trazer um impacto maior na redução de custos. O modelo de Software como um Serviço bas eia-se na ideia de fornecer ao consumidor um determinado serviço que está sendo operado e mantido na nuvem com execução

no dispositivo do usuário. Dispositivo este que pode ser um computador pessoal, um telefone inteligente (*smartphone*), um *tablet*, entre outros.

O SaaS, pode ser definido, de acordo com a MSDN (*Microsoft Developer Network*), como um software implantado como serviço hospedado, acessado através da Internet.

Um mesmo software pode ser utilizado por múltiplos usuários, sejam pessoas ou empresas. Esse tipo de serviço é executado e disponibilizado por servidores em 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 parabeneficio exclusivo, disponibiliza-o a um custo baixo a uma grande quantidade de usuários .(AULBACH, 2009 aput Nogueira, 2009).

3.1.2 Plataforma como Serviço (PaaS)

Este modelo é mais flexível do ponto de vista de padronizações necessárias para a empresa. Se a empresa precisa, além do software como um serviço, de uma plataforma de desenvolvimento para as aplicações customizadas que ele pretender ter, este é o modelo ideal. Neste modelo a empresa estará utilizando o conjuntode elementos oferecidos pelo provedor de soluções para desenvolvimento de software e padr onizações dos serviços.

Esse tipo de serviço disponibiliza servidores virtu alizados nos quais os utilizadores podem executar aplicações existentes ou desenvolver novas aplicações, sem ter que se preocupar com a manutenção dos sistemas operativos, servidores, balanceamento de cargas ou capacidade de computação.

Chirigati (2009) afirma que objetivo do PaaS é facilitar o desenvolvimento de aplicações destinadas aos usuários de uma nuvem, criando uma plataforma que agiliza esse processo.

3.1.3 Infraestrutura como Serviço (IaaS)

Neste modelo o provedor de soluções para computação na nuvem vai disponibilizar para o contratante a infraestrutura computacional necessária para que ele coloque seu negócio em produção. A infraestrutura em questão inclui a disp onibilização de rede, dispositivo de armazenamento e, diferentemente dos outros modelos, neste o contratante tem acesso ao sistema operacional do ponto de vista de instalação, config uração e manutenção.

Disponibiliza *grids* ou *clusters* ou servidores virtualizados, redes, armazenamento e software de sistemas desenhados para aumentar ou substituir as funções de um centro de dados.

Para Amrhein e Quint (2009) os serviços de infraest rutura abordam o problema de equipar de forma apropriada os *datacenters*, assegurando o poder de computação quando

necessário. Além disso, devido ao fato das técnicasde virtualização serem comumente empregados nessa camada, economias de custos decorrentes da utilização mais eficiente de recursos podem ser percebidas.

4. SEGURANÇA

Na sociedade da informação, a informação é o princi pal patrimônio da empresa e está sob constante risco (DIAS, 2000). As empresas já perceberam que o domínio da tecnologia como aliado para o controle da informação é vital. Sêmola (2003) define a Segurança da Informação, como proteção existente sobre as inform ações de uma determinada empresa ou pessoa, isto é, aplica-se tanto as informações corp orativas quanto as pessoais. A segurança de uma determinada informação pode ser afetada por fat ores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificartal informação.

As principais propriedades da segurança são a Confi dencialidade, Integridade e Disponibilidade que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. (SÊMOLA, 2003).

Confidencialidade: Segundo Sêmola (2003) é a propriedade que limita acesso a informação tão somente às entidades legítimas, ou s eja, àquelas autorizadas pelo proprietário da informação. Considera-se este princípio quando u m sistema, ou ativo de informação, necessita de proteção contra a divulgação não autor izada dos seus bens de informação.

Integridade: Sêmola (2003) afirma que é a propriedade que garante que a informação manipulada mantenha todas as caracterís t icas originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição). Considera-se este princípio quando um sistema, ou ativo de informação, contém informação que deve ser protegida contra modificações não autorizadas, imprevistas ou até mesmo não intencionais, incluindo ainda mecanismos que permitam a detecção de tais tipos de alteração.

Disponibilidade: Conforme Sêmola (2003) é a propriedade que garanteque ainformação esteja sempre disponível para o uso legí timo, ou seja, por aqueles usuários autorizados pelo proprietário da informação. Considera-se este princípio quando um sistema, ou ativo de informação precisa estar disponível par a satisfazer os seus requisitos ou evitar perdas financeiras.

Na hora de migrar os dados de uma empresa para uma nuvem, todo administrador se preocupa com a segurança de suas informações, com a qualidade que estas estarão sendo guardadas. Existe o risco de alguém invadir o servidor e ter acesso aos dados das organizações que lá hospedam seus serviços, o que pode eventualmente gerar transtornos vitais, como o compartilhamento de dados por concorrentes, ou mesmo a alteração original dos dados, levando a tomada de decisões equivocadas.

Em uma pesquisa realizada pelo IDC (*International Data Corporation*) com 244 executivos de TI, procurou-se investigar qual o aspecto mais preocupante quando do uso de serviços de computação em nuvens. Os resultados mos traram que 74,5% das pessoas entrevistadas preocupam-se com a segurança (VELTE A ., VELTE T. e ELSENPETER, 2010).

Por isso, a segurança da informação deve ser vista como uma das partes mais importantes para se começar a utilizar o serviço de computação em nuvens, pois a empresa estará lidando com dados coletadas ao longo de vários anos, inclusive dados de terceiros. Sendo assim, qualquer problema que houver no servidor, como um vazamento de informação, poderá resultar em um enorme prejuízo para seus clientes.

Tendo esse aspecto em mente, deve-se analisar qual a melhor empresa, a partir de uma análise dos níveis, técnicas e ferramentas de segurança que são utilizadas para a proteção dos dados. Ainda, avaliar as técnicas de redundância e espelhamento utilizados no *datacenter*, fatores que contribuem para que os serviços ofereci dos não deixem de funcionar em uma eventual falha recorrente da falta de energia ou problemas de hardware e software no local onde os dados são armazenados e gerenciados.

Uma preocupação crescente são os *hackers*, pois, como os dados estão sendo mantidos nos equipamentos de outras empresas, pode-se estar à mercê de quaisquer medidas de segurança das quais eles tenham conhecimento (VELTE A., VELTE T. e ELSENPETER, 2010).

Quando ocorre um ataque de *hackers*, estes utilizam de chantagens para poder devolver as informações. Ou seja, a empresa tem que pagar a eles para obterem algo que já lhes pertence.

Entretanto, não se deve ter o conceito que os seus dados estarão completamente desprotegidos. Grandes *datacenters* possuem uma infraestrutura muito preparada contra quaisquer tipos de ataques, tanto virtuais quanto físicas. Por isso deve-se analisar bem a instituição que será contratada.

Velte A., Velte T. e Elsenpeter (2010) destacam alguns pontos positivos sobre a segurança nas nuvens:

Monitoramento: maior facilidade no controle da segurança, pois a atenção está voltada para uma nuvem, e não para servidores e num erosos clientes.

Intercâmbio Instantâneo: caso ocorra algum problema com seus dados, pode-se fazer a transferência instantânea deles para outro computador, sem comprometer assim a integridade das informações.

Construções Seguras: a rede da própria empresa e se u software de segurança podem ser agrupados, desenvolvendo assim em um nível de segurança desejado.

Melhoria da Segurança de Software: como os forneced ores não querem perder vendas, eles aplicam o melhor software possível em segurança de dados.

Teste de Segurança: nos serviços de SaaS, os testes e segurança feitos não são cobrados aos clientes.

Entre os componentes básicos importantes das relações de confiança e verificação estão o controle de acesso, a segurança dos dados, a conformidade e o gerenciamento de eventos — todos os elementos da segurança que são bem compr eendidos atualmente pelos departamentos de TI, implementados com produtos e tecnologias existentes e com possibilidade de extensão para a nuvem.

A RSA em seu *White Pape* (2009) define alguns critérios de segurança:

Segurança de identidades

O gerenciamento completo de identidades, os serviço s de autenticação de terceiros e a identidade federada são elementos fundamentais para a segurança da nuvem. A segurança da identidade preserva a integridade e a confidencialidade dos dados e dos aplicativos enquanto deixa o acesso prontamente disponível para os usuários apropriados. O suporte a esses recursos de gerenciamento de identidade para usuários e componentes da infraestrutura é um requisito principal da computação em nuvem e a identidade pre cisa ser gerenciada de maneira que gere confiança. Ele exige:

- Autenticação sólida: a computação em nuvem deve ir além da fraca autenticação com nome de usuário e senha se quiser oferecer suporte a empresas. Isso significa adotar técnicas e tecnologias que já são padrão na TI corporativa, como autenticação sólida (autenticação de vários fatores com tecnologia de senha única), federação dentro de empresas e, entre elas, a autenticação com base em risco que mede o histórico de comportamento, o contexto atual e outros fatores para avaliar o nível de risco de uma solicitação de usuário.
- Autorização mais granular: a autorização pode ser e specificada dentro de uma empresa ou até de uma nuvem privada, mas para manipular dados confidenciais e requisitos de conformidade, as nuvens públicas precisarão de recursos granulares de que possam ser persistentes na infraestrutura da nuvem e ao longo de todo o ciclo de vida dos dados.

Segurança das informações

No *data center* tradicional, os controles sobre o acesso físico, o acesso a hardware e software e os controles de identidade se combinam para proteger os dados. Na nuvem, a barreira protetora que protege a infraestrutura é diluída. Para compensar, a segurança passará a ser centrada nas informações. Os dados precisam de segu rança própria que os acompanhe e os proteja. Isso exigirá:

Isolamento de dados: em situações de multilocação, os dados precisam ser mantidos em segurança para que fiquem protegidos quando vários clientes usarem recursos compartilhados. A virtualização, a criptografia e o controle de ace sso serão robustos para permitir níveis variáveis de separação entre corporações, comunidad es de interesse e usuários.

Segurança de dados mais granular: à medida que aume nta a confidencialidade das informações, a granularidade da aplicação da classi ficação de dados precisa aumentar. Nos atuais ambientes de *data center*, a granularidade do controle de acesso com base em funções no nível dos grupos de usuários ou das unidades denegócios é aceitável na maioria dos casos porque as informações continuam sendo controladas p ela empresa. Para as informações na nuvem, os dados confidenciais exigem segurança no n ível do arquivo, do campo ou até do bloco para atender às demandas de garantia e conformidade .

Segurança consistente dos dados: há uma necessidadeóbvia de proteção de conteúdo com base em políticas para atender às necessidades da empresa e às determinações das políticas normativas. Para algumas categorias de dados, a segurança centrada nas informações precisada criptografia em trânsito e em repouso, al ém do gerenciamento em toda a nuvem e ao longo de todo o ciclo de vida dos dados.

Classificação eficiente de dados: a computação em n uvem impõe uma troca de recursos entre alto desempenho e os requisitos de segurança, cada vez mais robustos. A classificação de dados é uma ferramenta essencial para equilibrar essa equação. As empresas devem saber quais dados são importantes e onde eles estão local izados como pré-requisitos para tomar decisões sobre o custo/benefício do desempenho, além de garantir o foco nas áreas mais essenciais dos procedimentos de prevenção contra a perda de dados.

Information Rights Management: o IRM (*Information Rights Management*,gerenciamento dos direitos às informações) é, muita s vezes, tratado como um componente deidentidade, um meio de configurar controles gerais que definem que usuários têm acesso a quais dados. Mas uma maior segurança granular centr ada nos dados exige que as políticas e os mecanismos de controle no armazenamento e o uso das informações sejam diretamente associados às informações.

Controle e conformidade: um requisito importante do controle e da conformidade das informações corporativas é a criação de informações de gerenciamento e validação — monitorando e fazendo a auditoria do estado de segurança das informações com recursos de registro. Nesse caso, isso não é importante apenas para o acesso a documentos e para recusas de dados, mas para garantir que os sistemas de TI estejam configurados para atender às especificações de segurança e não tenham sido alter ados. A expansão de políticas de retenção para a conformidade da política de dados também será um recurso essencial da nuvem.

Em suma, as infraestruturas da computação em nuvem devem ser capazes de verificar se os dados estão sendo gerenciados de acordo com a s regulamentações locais e internacionais aplicáveis (como PCI e HIPAA), com controles apropriados, coleta de registros e emissão de relatórios.

Dados confidenciais na nuvem precisarão de seguranç a granular, mantida de modo consistente durante todo o ciclo de vida dos dados.

Segurança da infraestrutura

A infraestrutura de base de uma nuvem deve ser inerentemente segura, independentemente de a nuvem ser privada ou pública ou de o serviço ser SAAS, PAAS ou IAAS. Isso exige:

Segurança inerente no nível do componente: a nuvem precisa ser projetada para ser segura, montada com componentes inerentemente seguros, implementada e provisionada de maneira segura com interfaces sólidas para outros c omponentes e, finalmente, sustentada de modo seguro, com processos de avaliação de vulnerab ilidades e gerenciamento de alterações que produzem informações de gerenciamento e garanti as de nível de serviço que geram confiança. Para esses componentes implementados com flexibilidade, a definição de impressão digital de dispositivos para garantir a configuraçã o e o estado seguros também será um elemento importante de segurança, assim como é para os dados e as identidades.

Segurança de interface mais granular: os pontos do sistema nos quais ocorrem transferências — do usuário para a rede, do servidor para o aplicativo — exigem políticas e controles de segurança granulares que garantam a co nsistência e a responsabilidade. Nesse caso, o sistema completo precisa ser exclusivo, um padrão verdadeiro ou uma federação de fornecedores que oferecem políticas de segurança im plementadas consistentemente.

Gerenciamento do ciclo de vida de recursos: a economia da computação em nuvem é baseada em multilocação em compartilhamento de recu rsos. À medida que as necessidades e os requisitos de um cliente mudam, um provedor de serviços precisa fornecer ou desativar esses recursos — largura de banda, servidores, armazename nto e segurança — adequadamente. Esse

processo de ciclo de vida deve ser gerenciado para fins de responsabilidade, de modo a gerar confiança.

5. CONSIDERAÇÕES FINAIS

Este artigo apresentou a computação em nuvens como a forma de armazenamento moderna, em que se eliminam os riscos com perdas de dados físicos e as informações passam a ser disponibilizadas a qualquer momento e em qualquer lugar.

Não há duvidas de que a computação em nuvens é uma das formas mais transformadoras que vimos em TI nos últimos tempos e ela tem um impacto gigante nas possibilidades que se abrem e em como trabalhamos. Porém somente quem compreender bem sua natureza conseguirá utilizar e desenvolver produtos e serviços que usem todo o seu potencial. E isso será uma grande fonte de diferenciação e de vantagem com petitiva.

A computação em nuvem promete mudar a economia do d atacenter, mas antes que dados confidenciais e regulamentados sejam migrados para a nuvem pública, é necessário tratar de questões relativas aos padrões de segurança e co mpatibilidade que abrangem autenticação sólida, autorização delegada, gerenciamento de chav es para dados criptografados, proteções contra a perda de dados e emissão de relatórios nor mativos.

6. REFERÊNCIAS

ALECRIM, Emerson. **O que é CloudComputing (Computação nas Nuvens)?**.Disponível em: <http://www.infowester.com/cloudcomputing.php>. Acesso em: 06 de maio de 2012.

AMRHEIN, Dustin; QUINT, Scott. **Computação em Nuvem para a Empresa.** Disponível em: <http://www.ibm.com/developerworks/br/websphere/techjournal/0904_amrhein/0904_amrhein.html.> Acesso em: 15 de maio de 2012.

CHIRIGATI, Fernando Seabra. **Computação em Nuvem.** Disponível em: <http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2009_2/seabra/index.html.> Acesso em 05 de maio de 2012.

CUNHA, Meire Jane Marcelo (2005). **Proposta de documentação para subsidiar as atividades de implantação da Segurança da Informaçã o**. Disponível em: <http://www.acso.uneb.br/marcosimoes/TrabalhosOrientados/CUNHA2005.pdf.> Acesso em: 07 de maio de 2012.

DIAS, Cláudia.**Segurança e Auditoria da Tecnologia da Informação.** São Paulo: Axcel Books, 2000.

HURWITZ, Judith; BLOOR, Robin; KAUFMAN, Marcia; HALPER, Fern. **Cloud Computingfor Dummies;** 1. ed Indiana, U.S. : WileyPublishing, Inc; 2010. 336 p. ISBN:978-0-470-48470-8

NOGUEIRA, Matheus Cadori; PEZZI, Daniel da Cunha. **A computação agora é nas nuvens.** Disponível em:< http://under-linux.org/blogs/mcadori/attachments/64d1257953490-artigo-sobre-cloud-computingcloud- computing.pdf>. Acesso em: 20 de maio de 2012.

SANTOS, Bruno Carvalho dos; MENESES, Francisco Gerson Amorim de. **Cloud Computing: conceitos, oportunidades e desafios da nova computação.** Disponível em:<http://www.cefetparnaiba.edu.br/index.php?option=com_docman&task=doc_download&gi

d=277&Itemid =79>. Acesso em: 02 dez 2009.

SÊMOLA, M. Gestão da Segurança da Informação. Rio d e Janeiro: Campus, 2003. SILVA, F. H. R. **Um estudo sobre os benefícios e os riscos de segurança na utilização de Cloud Computing;** 2010. 15f. Artigo científico de conclusão de curso apresentado no CentroUniversitário Augusto Motta, UNISUAM-RJ.

SOROR, A.A; MINHAS, U.F.; ABOULNAGE, A. SALEM, K;KAMATH, S**. AutomaticVirtual Machine Configuration for Database Workloads**. ACM. Trans. Database Syst.2010.

SOUZA, Flávio R. C.; MOREIRA, Leandro O.; MACHADO,Javam C. **Computação em Nuvem: Conceitos, Tecnologias, Aplicações e Desafio s.** Disponível em: <www.ufpi.br/ercemapi/arquivos/file/minicurso/mc7.pdf.> Acesso em: 19 de maio de 2012

TAURION, Cezar**. Cloud Computing: Computação em Nuvem: Transforman do o mundo da tecnologia da informação** . Rio de Janeiro: Brasport, 2009.

TEIXEIRA, Gilberto. **As ambiguidades do conceito de Informação.** Disponível em: <http://www.serprofessoruniversitario.pro.br/ler.php?modulo=22&texto=1385>. Acesso em: 04 dez 2009.