



Faculdade de Tecnologia de Americana
Curso de Segurança da Informação

OUTROS TRABALHOS EM:
www.projeteredes.com.br

Gerenciamento de riscos em Cloud Computing

Alexandre Rodrigues Sonogo

Americana, SP
2011



Faculdade de Tecnologia de Americana
Curso de Segurança da Informação

Gerenciamento de riscos em Cloud Computing

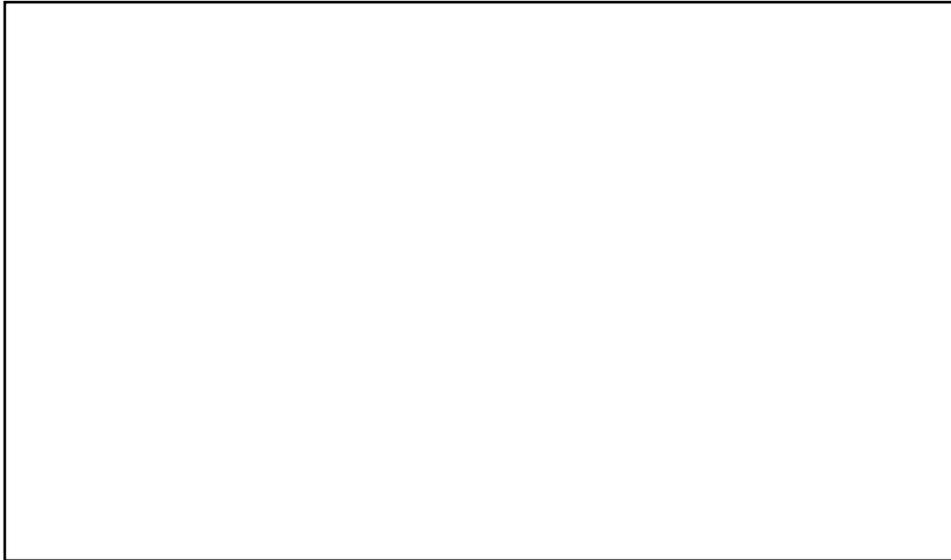
Alexandre Rodrigues Sonogo

Alexandre.rsonogo@gmail.com

**Trabalho de conclusão de curso,
desenvolvido em cumprimento à
exigência curricular do Curso de
Segurança da Informação da Faculdade
de Tecnologia de Americana, sob
orientação do Prof. Benedito Cruz.**

**Americana, SP
2011**

FICHA CATALOGRÁFICA



BANCA EXAMINADORA

Prof. Benedito Cruz (Orientador)

Prof. Rogério Nunes de Freitas (Convidado)

Prof. Antonio Alfredo Lacerda (Presidente da banca)

AGRADECIMENTOS

Primeiramente, agradeço aos meus pais, juntamente com minha namorada, que sempre me apoiaram e compreenderam as ausências resultantes no tempo dedicado ao curso e trabalhos em questão.

Aos professores e funcionários do Centro Paula Souza que direta ou indiretamente contribuíram para o crescimento pessoal e profissional alcançado.

Aos colegas de classe, a primeira turma do curso de Segurança da Informação, que mutuamente se ajudaram nessa árdua caminhada nestes três anos.

Finalmente a todos que de alguma forma contribuíram para a conclusão de mais esta etapa.

DEDICATÓRIA

Este trabalho é dedicado aos meus pais, namorada e amigos que constantemente me apoiaram em mais esta etapa.

*“..... Não importa a forma que a informação tome, ou os meios pelos quais ela é compartilhada ou armazenada, convém que ela sempre seja apropriadamente protegida.”
(ISO/IEC 27002:2007)*

RESUMO

O presente texto conceitua o que é computação em nuvem e suas principais características. Posteriormente é realizada uma análise dos principais benefícios econômicos e no âmbito de segurança. Por fim, são apresentados os principais riscos identificados pelas entidades competentes no assunto e sugestões para o adequado gerenciamento destes.

Palavras Chave: computação em nuvem, gerenciamento de risco

ABSTRACT

The present text conceptualizes what is cloud computing and the key characteristics. After that, appoint the major economic and security benefits. Finally, its brings the key risks, according the especialistas, and suggest some managing actions.

Keywords: Cloud computing, risk management

LISTA DE FIGURAS

Figura 1 – Diagrama de responsabilidade X serviço.....	21
Figura 2 – Modelo Cloud Cube Jericho.....	23

ABREVIATURAS E SIGLAS

SETI - Search for Extra-Terrestrial Intelligence

NIST - National Institute of Standards and Technology

CSA - Cloud Security Alliance

SaaS – Software as a Service

PaaS - Plataform as a Service

IaaS - Infraestructure as a Service

EC2 (Elastic Computing Cloud)

S3 (Simple Storage Service)

SPI - Software, plataform and Infraescstruture

COA - Collaboration Oriented Architectures

CAPEX - Capital expenditure

OPEX - Operational Expenditure

ISACA - System Audit and Control Association

ENISA - European Network Information Security Agencia

SLA - Service Level Agreement

VPN - Virtual Private Network

SUMÁRIO

INTRODUÇÃO.....	14
COMPUTAÇÃO EM NUVEM.....	16
2.1 Histórico.....	16
2.2 Características Essenciais de Computação em Nuvem.....	18
2.3 Modelos de Serviços de Nuvem.....	19
2.4 Modelos de Implantação de Nuvem.....	21
FORMAÇÕES DE IMPLANTAÇÃO DA NUVEM.....	23
2.5 Dimensões do cubo de cloud.....	24
BENEFÍCIOS DA COMPUTAÇÃO EM NUVEM.....	28
2.6 Benefícios comerciais em computação em nuvem.....	29
2.6.1 Contenção de despesas.....	29
2.6.2 Imediatismo.....	29
2.6.3 Dimensionamento.....	29
2.6.4 Eficiência.....	30
2.7 Benefícios de segurança em computação em nuvem.....	30
2.7.1 Benefícios da Escala.....	30
2.7.2 Segurança como diferencial.....	31
2.7.3 Padronização do gerenciamento de serviços de segurança.....	32
2.7.4 Dimensionamento rápido e inteligente dos recursos.....	32
2.7.5 Processo de aquisição de evidências para auditoria.....	33
2.7.6 Upgrades mais rápidos, efetivos e eficientes.....	33
2.7.7 Benefícios da concentração de recursos.....	34
RISCOS.....	35
2.8 Riscos organizacionais.....	36
2.8.1 Dependência do fornecedor (Vendor lock-in).....	36
2.8.2 Perda de governança corporativa e de normativas (compliance).....	37

2.8.3 Perda de reputação por ações indiretas.....	38
2.8.4 Falhas na cadeia de fornecimento.....	39
2.9 Riscos técnicos.....	39
2.9.1 Falta de recursos.....	39
2.9.2 Falha nos mecanismos de separação.....	40
2.9.3 Uso inadequado das contas privilegiadas.....	41
2.9.4 Interface de gerenciamento.....	42
2.9.5 Captura de informações em tráfego.....	42
2.9.6 Descarte dos dados de forma insegura / não eficiente.....	43
2.9.7 Ataques distribuídos de negação de serviço	44
2.10 Riscos jurídicos.....	44
2.10.1 Intimação, busca e apreensão.....	44
2.10.2 Mudança de jurisdição.....	45
RECOMENDAÇÕES FINAIS.....	46
2.11 Governança corporativa e aspectos legais.....	46
2.12 Auditoria.....	48
2.13 Portabilidade e Interoperabilidade.....	49
2.14 Continuidade de Negócios, Recuperação de Desastres e Incidentes.....	49
CONCLUSÃO.....	51
REFERÊNCIAS BIBLIOGRÁFICAS.....	52

INTRODUÇÃO

Atualmente a demanda por novas funcionalidades e informações cresce exponencialmente: a web já faz parte do dia a dia e milhares de transações ocorrem simultaneamente cada instante, resultando na geração de informações que ganham valor agregado na mesma proporção em que são criadas.

Paralelamente, há uma crescente movimentação para reduzir os custos dos recursos de armazenamento e gerenciamento destas informações; além do “movimento TI Verde”, preocupação mundial para redução do consumo de energia para produção e utilização destas informações.

No passado era comum o gasto de altos valores para aquisição de super servidores, máquinas de alto desempenho para garantir que não houvesse falta de recursos computacionais quando necessários. Entretanto, não havia uma preocupação ou qualquer tipo de análise acerca do aproveitamento destes recursos em tempo integral, resultando assim em uma subutilização destes, impactando diretamente no custo de retorno do investimento realizado.

Em linha com essa necessidade, criou-se a virtualização, tornando possível otimizar a utilização dos recursos computacionais de uma máquina através do compartilhamento de uma mesmo hardware por mais de um sistema operacional, reduzindo a demanda por recursos físicos e consumo de energia.

Com o amadurecimento do conceito de virtualização aplicada aos desktops e servidores, houve uma mudança de paradigma; se armazenamento e sistemas operacionais podem ser virtualizados, por que não virtualizar aplicações, serviços, plataformas e infra-estruturas? Desta maneira, a idéia de compartilhar recursos

abstraiu os limites dos servidores produzindo um novo conceito conhecido como computação em nuvem.

Como acontece com qualquer tecnologia emergente, a computação em nuvem oferece a possibilidade de recompensa elevada em termos de contenção de custos, assim como agilidade e velocidade de fornecimento de recursos. No entanto, como uma iniciativa nova, ela também pode trazer um alto risco em potencial. A computação em nuvem apresenta um nível de abstração entre a infraestrutura física e o proprietário da informação a ser armazenada e processada. Tradicionalmente, o proprietário dos dados mantém controle direto ou indireto do ambiente físico que afeta seus dados. No sistema de nuvem, isso não ocorre mais. Devido a essa abstração, já existe uma demanda generalizada de maior transparência e garantia de abordagem robusta de segurança do ambiente de controle e de segurança do provedor de serviços de nuvem.

Este trabalho de conclusão de cursos tem como objetivo realizar um breve histórico acerca da computação em nuvem bem como das suas principais características. Posteriormente é realizado um levantamento dos principais riscos, apresentados por essa nova tecnologia e eventuais sugestões para gerenciar e mitigar estes riscos. Conclui-se o trabalho apresentando uma tese que os benefícios trazidos por essa nova tecnologia sobrepõem os riscos envolvidos, desde que estes se encontrem devidamente gerenciados.

COMPUTAÇÃO EM NUVEM

Uma das questões mais confusas em torno do sistema de nuvem e seus serviços relacionados é a falta de acordo acerca de suas definições. Tal como acontece com todas as tecnologias emergentes, a falta de clareza e de acordo muitas vezes dificulta a avaliação e a aceitação destas tecnologias.

Os dois principais grupos que têm oferecido uma base de definições são o NIST (*National Institute of Standards and Technology*) e a CSA (*Cloud Security Alliance*). Ambos definem a computação em nuvem como: *“Um modelo para permitir o acesso à rede sob demanda, de forma conveniente, a um conjunto compartilhado de recursos de computação configuráveis (por exemplo, redes, servidores, armazenamento, aplicativos e serviços) que podem ser rapidamente fornecidos e lançados com o mínimo esforço de gestão ou interação do prestador de serviço.”*

2.1 Histórico

Historicamente não há um início claro da computação em nuvem; pode-se dizer que seu conceito inicial originou-se na década de 60, onde o cientista da computação norte-americano John McCarthy afirmou que iria acontecer com a informática o mesmo que aconteceu com a eletricidade. Ao invés de as pessoas terem geradores em suas casas, elas pagariam pela quantidade de energia elétrica utilizada.

Em Maio de 1964. Martin Greenberger publicou o artigo “The computers of Tomorrow” (“Os computadores do Amanhã”) na Atlantic Monthly onde ele discorria acerca da utilização dos recursos computacionais não apenas para cálculos

científicos e pesquisas, mas com funções para atender os processos de negócio das empresas. Ele visionou o que viria a se tornar o principal negócio da IBM, a venda de capacidade de processamento computacional para atender as demandas das empresas.

Em Março de 1999, a *salesforce.com* foi inaugurada, utilizando-se do conceito de Software as Service (SaaS), oferecendo um software de CRM (*Customer Relationship Management*) diretamente em nuvem, 24h por dia, e altamente customizável e escalonável.

Em 2001 o SETI (*Search for Extra-Terrestrial Intelligence*) desenvolveu o SETI@HOME, onde os dados obtidos pelos satélites eram segregados em diversos pacotes menores e enviados a computadores pessoais cadastrados, para que estes realizassem as análises e enviassem de volta os resultados obtidos. A capacidade de processamento destes computadores voluntários supera em 5 vezes o volume de dados disponíveis para análises, além de, em conjunto constituírem a maior capacidade de processamento criada pelo homem, totalizando 23 teraflops.

De 2002 a 2006 a *Amazon.com* criou e amadureceu o conceito da EC2 (*Elastic Computing Cloud*) onde os usuários podem criar e configurar suas próprias máquinas virtuais para execução na Nuvem da Amazon. Estas máquinas virtuais ficam armazenadas no Amazon S3 (*Simple Storage Service*), permitindo que sejam iniciadas quando solicitadas pelos clientes. Todas as configurações são escalonáveis, e o usuário só paga pelos recursos que foram utilizados.

Em Abril de 2008 é lançado a *Google App Engine*, marco da entrada de uma empresa puramente voltada à tecnologia no mercado de computação em nuvem. Tal

como acontece com todos os seus outros produtos há uma prática agressiva de preços, com valores iniciais extremamente baixos e tendo os custos de armazenamento entre os mais baixos do mercado.

2.2 Características Essenciais de Computação em Nuvem

Conforme o artigo da CSA (*Cloud Security Alliance*) “*Security Guidance for Critical Areas of Focus in Cloud Computing*” os serviços na nuvem apresentam cinco características essenciais que demonstram suas relações e diferenças das abordagens tradicionais de computação:

- **Auto-atendimento sob demanda:** O provedor do sistema de nuvem deve ser capaz de fornecer automaticamente os recursos de computação, tais como armazenamento de rede e servidores, conforme forem necessários, sem exigir a interação humana com o provedor de cada serviço.
- **Ampla acesso a rede:** De acordo com o NIST, a rede de nuvem deve ser acessível em qualquer lugar, em quase todos os dispositivos (por exemplo, smartphones, laptops, PDAs, aparelhos portáteis).
- **Grupo de recursos:** O provedor de recursos de computação é agrupado para atender vários clientes usando um modelo multiciente com diferentes recursos físicos e virtuais atribuídos dinamicamente e reatribuídos de acordo com a demanda. Há um senso de independência local. Geralmente, o cliente não tem nenhum controle ou conhecimento sobre a localização exata dos recursos disponibilizados. No entanto, é possível especificar o local em um nível maior de abstração (por exemplo, país, região ou central de dados). Os

exemplos de recursos incluem o armazenamento, o processamento, a memória, a largura de banda da rede e as máquinas virtuais.

- **Elasticidade:** Os recursos podem ser provisionados rapidamente e de forma elástica, em muitos casos de forma automática, para aumentar em escala rapidamente e também reduzir de forma rápida. Para o cliente, os recursos disponíveis para o fornecimento muitas vezes parecem ser ilimitados e podem ser adquiridos em qualquer quantidade a qualquer momento.
- **Serviços mensuráveis:** Os sistemas de nuvem controlam e otimizam automaticamente a utilização de recursos, aproveitando a capacidade de medição (por exemplo, armazenamento, processamento, largura de banda e contas de usuários ativas). O uso de recursos pode ser monitorado, controlado e reportado, oferecendo transparência tanto para o provedor quanto para o cliente do serviço utilizado.

2.3 Modelos de Serviços de Nuvem

A entrega de serviços de nuvem é dividida entre três modelos de arquitetura e várias combinações derivadas. As três classificações fundamentais são geralmente referidas como “Modelo SPI”, onde “SPI” significa Software, Plataforma e Infraestrutura (como um Serviço), respectivamente – definidos, portanto como:

- **Software como Serviço (Software as a Service - SaaS):** Capacidade para utilizar os aplicativos do provedor a serem executados na infraestrutura do sistema de nuvem. Os aplicativos podem ser acessados a partir de vários dispositivos do cliente através de uma interface leve (thin client interface),

como um navegador da Web (por exemplo, um webmail). O consumidor não gerencia ou controla a infraestrutura adjacente na nuvem, incluindo rede, servidores, sistemas operacionais, armazenamento, ou nem mesmo as capacidades individuais da aplicação, com a possível exceção de parâmetros limitados de configuração da aplicação específicos para os usuários.

- **Plataforma como Serviço (*Platform as a Service - PaaS*):** Capacidade para a implantação de infraestrutura da nuvem criada pelo cliente ou aplicativos adquiridos criados com linguagens de programação e ferramentas compatíveis com as do fornecedor. O consumidor não gerencia ou controla a infraestrutura adjacente na nuvem, incluindo rede, servidores, sistemas operacionais, ou armazenamento, mas tem controle sobre as aplicações implementadas e possivelmente configurações da aplicação referentes ao ambiente do servidor.
- **Infraestrutura como Serviço (*Infrastructure as a Service - IaaS*):** A capacidade oferecida ao consumidor é de provisionar processamento, armazenamento, redes e outros recursos computacionais fundamentais onde o consumidor está apto a implementar e rodar os softwares que desejar, o que pode incluir sistemas operacionais e aplicações. O consumidor não gerencia ou controla as camadas adjacentes da infraestrutura na nuvem, mas tem controle sobre o sistema operacional, armazenamento, aplicações implementadas e possivelmente controle limitado de componentes específicos de rede. (exemplo: firewalls no servidor).

Uma visão gráfica de como cada modelo de serviço tem seus componentes gerenciados pode ser visualizado no diagrama abaixo:

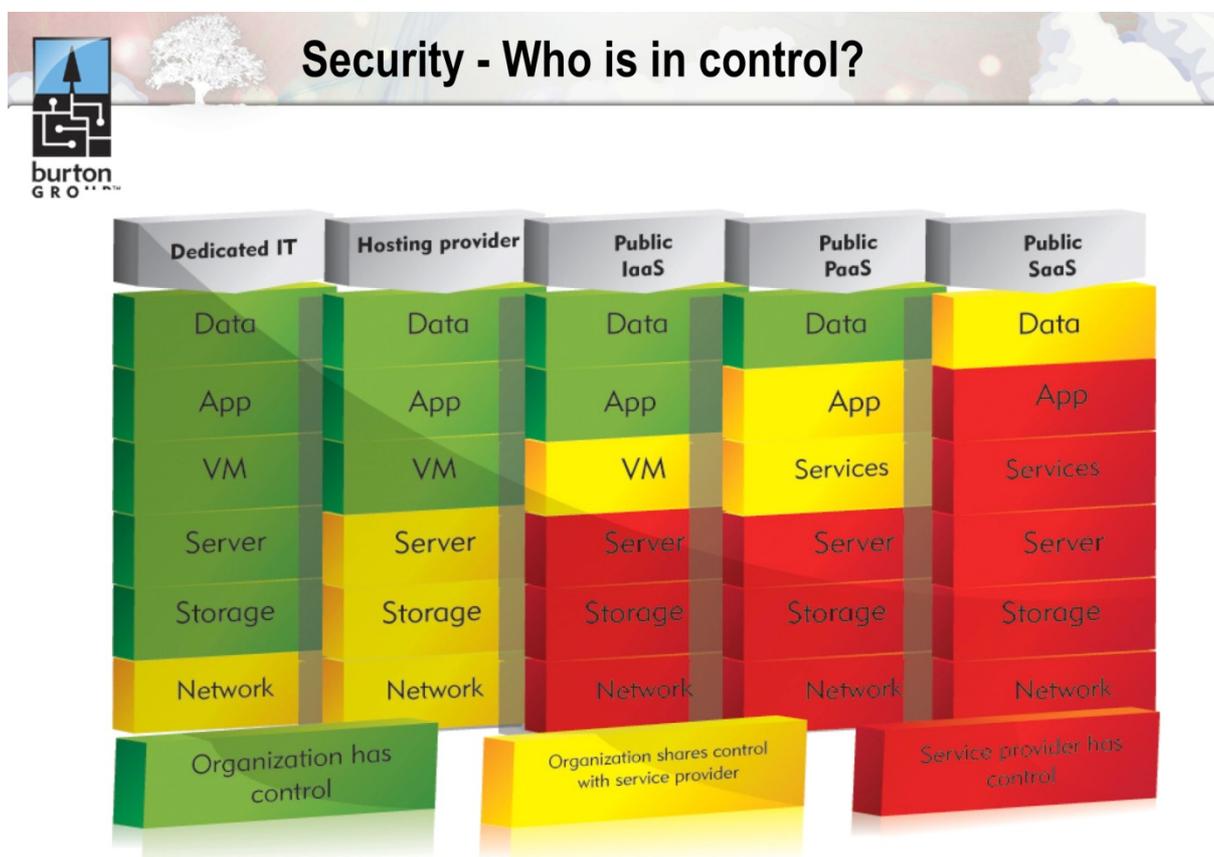


Figura 1 – Diagrama de responsabilidade X serviço

Fonte: <http://kscottmorrison.files.wordpress.com/2009/12/cloudcontrolboundaries.jpg>

2.4 Modelos de Implantação de Nuvem

Independente do modelo de serviço utilizado (SaaS, PaaS ou IaaS) existem quatro modelos de implantação de serviços de nuvem, com variações para atender a requisitos específicos:

- **Nuvem Pública:** A infraestrutura de nuvem é disponibilizada ao público em geral ou a um grande grupo industrial e é controlada por uma organização que vende os serviços de nuvem.
- **Nuvem Privada:** A infraestrutura da nuvem é operada exclusivamente por uma única organização. Ela pode ser gerida pela organização ou por terceiros, e pode existir no local ou fora do ambiente da empresa.
- **Nuvem Comunitária:** A infraestrutura da nuvem é compartilhada por diversas organizações e suporta uma determinada comunidade que partilha interesses (por exemplo, a missão, os requisitos de segurança, política ou considerações de conformidade). Ela pode ser administrada pelas organizações ou por um terceiro e pode existir no local ou fora do ambiente da empresa.
- **Nuvem Híbrida:** A infraestrutura da nuvem é uma composição de duas ou mais nuvens (privada, comunitária ou pública) que permanecem como entidades únicas, mas estão unidas pela tecnologia padronizada ou proprietária que permite a portabilidade de dados e aplicativos (por exemplo, “*cloud bursting*” para balanceamento de carga entre as nuvens).

FORMAÇÕES DE IMPLANTAÇÃO DA NUVEM

Antes de abordar os principais riscos de TI envolvidos na computação em nuvem, é preciso demonstrar como as diversas “formações de nuvem” – combinações entre as diferentes maneiras de implantação- apresentam diferentes características, diferentes graus de flexibilidade, diferentes oportunidade de colaboração, e diferentes riscos.

Atualmente, não há um padrão estabelecido para abordagem destes riscos de formações, entretanto, o *Jericho Fórum* (<http://www.opengroup.org/jericho>) desenvolveu um framework experimental e este vem sendo utilizado como pioneiro nas documentações atuais.

Este modelo apresenta quatro critérios para diferenciar as formações de nuvem, denominado “*The Cloud Cube Model*”, como pode ser visto abaixo e explanado na seqüência:

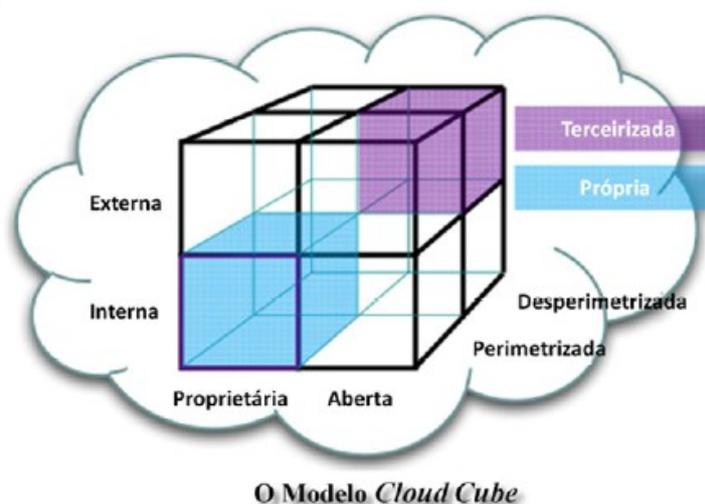


Figura 2 – Modelo Cloud Cube Jericho

Fonte: http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

2.5 Dimensões do cubo de cloud

1ª Dimensão: Interno (I) / Externo (E)

Esta dimensão determina a localização física dos dados: onde está a nuvem utilizada; dentro ou fora dos limites da sua organização:

- Se encontra dentro dos seus limites físicos, é interno
- Se não se encontra dentro dos seus limites físicos, é externo

Por exemplo, um disco rígido virtualizado no data center da organização será interno, enquanto o *Amazon S3* é considerado externo. Não se deve assumir que o modelo interno é mais seguro que o externo, a utilização adequada de ambos é responsável pelo seu grau de segurança.

2ª Dimensão: Proprietário(P) / Aberta (O)

Esta é a dimensão que define o estado de propriedade da tecnologia da nuvem, dos serviços, interfaces, etc. Ela indica o grau de interoperabilidade da nuvem, como a capacidade para retirar os dados de uma forma nuvem ou movê-la para outro sem restrição, além da possibilidade de compartilhar aplicativos.

Uma nuvem proprietária significa que a organização que presta o serviço é quem provisiona os recursos. Como resultado, quando se opera em nuvens proprietárias, pode-se não ser capaz de mudar para outro fornecedor de nuvem sem demandar grande esforço ou investimento. Muitas vezes os avanços da tecnologia inovadora ocorrem no domínio do proprietário. Como tal, o titular pode optar por impor

restrições através de patentes e, mantendo a tecnologia envolvida um segredo comercial.

Uma nuvem aberta caracteriza-se por utilizar tecnologias não proprietárias e de código aberto (open source), por consequência, tal forma possui maior número de fornecedores e grande facilidade em migrar os dados e aplicações entre nuvem que se utilizem da mesma tecnologia.

3ª Dimensão: Perimetrizado (Per) / Desperimetrizada (D-P)

A terceira dimensão representa a "mentalidade arquitetônica" - você está operando dentro do perímetro tradicional de TI ou fora dele? Desperimetrizadas estão relacionados à falha gradual / remoção / redução / colapso do perímetro tradicional de TI.

Perimetrizado constitui a operação dentro dos perímetros tradicionais de TI, muitas vezes sinalizados por "*firewalls*". Quando se opera em áreas perimetrizadas, você pode estender o perímetro da sua organização para o domínio externo de computação em nuvem usando uma conexão *Virtual Private Network* (VPN) e incluindo o servidor virtual no seu próprio domínio IP. Desta forma, apesar de virtual, o encontra-se em seu perímetro em quanto em uso.

Desperimetrizado é um termo criado por Paul Simmonds do Jericho Fórum e segundo sua própria explicação:

“(..)*Finalmente, em uma rede totalmente desperimetrizada cada componente torna-se independentemente seguro exigindo sistemas de proteção de dados em múltiplos níveis, como:*

- Criptografia;
- comunicações inerentemente seguras;
- dados de nível de autenticação”

Por exemplo, em um cenário desperimetrizado os dados serão encapsulados em meta-data e possuirá mecanismos que irão protegê-los de um uso inapropriado. O próprio *Jericho Fórum* desenvolveu um modelo denominado Arquiteturas Orientadas a Colaboração (*Collaboration Oriented Architectures – COA*) voltada a suprir as necessidades de desperimetrização.

Desta maneira:

Pode-se operar em qualquer das quatro formações de nuvem descritas (I/P,I/O,E/P,E/O) juntamente com a mentalidade arquitetônica Perimetrizada ou desperimetrizada.

O quadrante superior direito E/O/D-p representa a formação de nuvem denominada o ponto ideal, onde a flexibilidade ideal e colaboração podem ser alcançadas.

Um provedor de cloud privado irá permanecer no canto inferior esquerdo do cubo, acumulando continuamente inovação e agregando valor.

A capacidade de mover-se do canto inferior esquerdo para o “ponto ideal” vai exigir uma interface conceitual e rara, pois facilitar essa transição vai contra os interesses dos provedores de computação em nuvem.

4ª Dimensão: Terceirizada / Privada

Define-se a 4ª dimensão como sendo dois estados das quatro formações de nuvem: Per(IP,IO,EP,EO) e D-P (IP,IO,EP,EO):

- Terceirizada: Todos serviços são provenientes de fontes terceirizadas
- Privada: Os serviços são providos com seus recursos e estão sob responsabilidade da sua equipe

Desta forma, conceituado as formações de nuvem, passamos a tratar acerca dos principais benefícios, riscos e sugestões de ações a serem tomadas.

BENEFÍCIOS DA COMPUTAÇÃO EM NUVEM

Definitivamente a vantagem mais significativa, e que vem impulsionando o crescimento da computação em nuvem, encontra-se no âmbito econômico.

A computação em nuvem permite uma padronização dos recursos de TI e automatiza muitas das tarefas de manutenção realizadas manualmente. Apresenta benefícios como o consumo elástico, eliminação (ou pelo menos uma redução drástica) das despesas de capital, de auto-atendimento, além dos pagamentos “pague-o-que-usar” (*pay-as-you-go*).

Na maioria dos casos, migrar para computação em nuvem elimina os investimentos em bens de capital (*capital expenditure – CAPEX*), permitindo que estes valores sejam investidos em custos operacionais (*Operational Expenditure – OPEX*) negociáveis e gerenciáveis.

Além dos benefícios econômicos, a Associação dos auditores de controle e sistemas (*System Audit and Control Association - ISACA*) e a Agência Europeia de Segurança da informação (*European Network Information Security Agencia - ENISA*) relacionaram outras vantagens da computação em nuvem, no âmbito comercial e de segurança.

2.6 Benefícios comerciais em computação em nuvem

Segundo o artigo; “*Computação em nuvem: benefícios para o negócio com perspectivas de segurança, governança e qualidade*” (ISACA 2009) os principais benefícios comerciais da computação em nuvem são:

2.6.1 Contenção de despesas

O sistema de nuvem oferece às empresas a opção de dimensionamento sem sérios compromissos financeiros necessários para aquisição e manutenção de infraestrutura. Os serviços de nuvem exigem pouca ou nenhuma despesa de capital inicial. A economia de espaço não utilizado nos servidores permite que as empresas reduzam seus gastos com relação às exigências de tecnologia existentes e experimentem novas tecnologias e serviços sem precisar de grandes investimentos.

2.6.2 Imediatismo

Muitos pioneiros da computação em nuvem citaram a capacidade de fornecimento e utilização de um serviço em um único dia. Isso se compara aos tradicionais projetos de TI que podem exigir semanas ou meses para serem desenvolvidos, configurados e aplicados aos recursos necessários. Esse processo tem um impacto fundamental sobre a agilidade de um negócio e a redução dos custos associados aos atrasos.

2.6.3 Dimensionamento

Com capacidade irrestrita, os serviços de nuvem oferecem mais flexibilidade e dimensionamento envolvendo as necessidades de TI. O fornecimento e a

implementação são realizados sob demanda, permitindo aumento de tráfego e reduzindo o tempo para implementar novos serviços.

2.6.4 Eficiência

A realocação das atividades operacionais de gestão de informações sobre realocação da nuvem oferece às empresas uma oportunidade única para concentrar esforços na inovação e pesquisa e desenvolvimento. Esse processo abre as portas para o crescimento comercial, bem como o crescimento do produto, e ainda pode ser mais benéfico do que as vantagens financeiras oferecidas pelo sistema de nuvem.

2.7 Benefícios de segurança em computação em nuvem.

Antes de apresentar os riscos trazidos por esta nova tecnologia, é interessante demonstrar como especialistas acreditam que há vários aspectos de vantagens em se tratando de segurança.

Segundo o artigo; *“Computação em nuvem: Benefícios, riscos e recomendações para segurança da informação”* (ENISA 2010) os principais benefícios no âmbito de segurança da informação da computação em nuvem são:

2.7.1 Benefícios da Escala

Naturalmente, todos os tipos de soluções de segurança tornam-se mais baratas quando implementadas em grande escala. E quanto maior o investimento melhor a qualidade de proteção adquirida.

Isso inclui todos os tipos de medidas defensivas, tais como filtragem, gerenciamento de atualizações, o blindagens de máquinas virtuais e hypervisors,

recursos humanos, redundância de hardware e software, autenticação segura, controle de acesso eficiente, soluções de gerenciamento de identidade federada, o que também melhora os efeitos de colaboração entre os vários parceiros envolvidos na nuvem. Outros benefícios incluem:

- **Múltiplas localizações:** Os provedores de computação em nuvem possuem recursos econômicos para replicar os conteúdos em múltiplos locais. Isto aumenta a redundância e independência em caso de falha e proporciona um nível de recuperação de desastres inimaginável.
- **Bordas da rede:** Armazenamento, processamento e entregas realizadas próximas as bordas da rede significam serviços mais confiáveis e com maior qualidade, onde problemas na rede local dificilmente impactarão no âmbito global.
- **Gerenciamento de ameaças:** Provedores de computação em nuvem possuem recursos para contratarem profissionais capacitados e especializados em determinadas ameaças de segurança, enquanto uma empresa menor poderia apenas contratar um generalista.

2.7.2 Segurança como diferencial

A escolha de um provedor de computação em nuvem será realizada baseando-se na reputação do mesmo no âmbito de confidencialidade, integridade e disponibilidade oferecida por esse provedor. Esse fator tende a ser mais relevante do que em um ambiente tradicional, desta forma, haverá um impulso para direcionar

os provedores a melhorarem as práticas de segurança, tornando-se mais competitivos.

2.7.3 Padronização do gerenciamento de serviços de segurança

Grandes provedores de computação em nuvem pode oferecer uma interface aberta e padronizada para gerenciamento de serviços de segurança (MSS). Isso potencialmente cria um mercado mais aberto e disponível para serviços de segurança, onde os clientes podem mudar de fornecedor com mais facilidade e menor custo de implementação.

2.7.4 Dimensionamento rápido e inteligente dos recursos

Um provedor de computação em nuvem tem potencial para dinamicamente alocar recursos adicionais para filtragem, *traffic shaping*, encriptação, etc. com o intuito de ampliar a “potência” destes dispositivos de segurança (como por exemplo, para prevenir um ataque de negação de serviço (*Denial of Service* – DDoS)).

Quando essa capacidade de dimensionamento dinâmico de recursos é combinada com os métodos de otimização adequados, o provedor de cloud computing estará apto a minimizar ou até mesmo anular os efeitos de alguns ataques.

A capacidade de escalonar dinamicamente recursos defensivos sob demanda possuem vantagens óbvias para a resiliência. Além disso, todos os tipos de recursos individuais podem ser dimensionados de forma granular, sem dimensionar

o sistema como um todo. Naturalmente, isso se torna extremamente mais barato para responder a estes picos de demanda.

2.7.5 Processo de aquisição de evidências para auditoria

Provedores de computação em nuvem possuem recursos para clonagem de máquinas virtuais sob demanda. Em um incidente em que se acredite haver uma quebra de segurança, o cliente pode solicitar uma imagem ‘viva’ da máquina virtual – enquanto a máquina original continua operando normalmente – para realizar uma análise forense paralelamente. Isto reduz drasticamente o tempo de obtenção desta evidência para análise, contribuindo para identificação do ocorrido.

A computação em nuvem ainda pode oferecer uma solução mais eficiente para o armazenamento das trilhas de auditoria (*logs*), pois permite o armazenamento de *logs* mais detalhados sem que haja comprometimento da performance. Seguindo o conceito de “pague o que você utilizar”, torna-se mais fácil mensurar o custo envolvido neste armazenamento e realizar ajustes para se adequar as necessidades da auditoria.

2.7.6 Upgrades mais rápidos, efetivos e eficientes

Upgrades podem ser replicados varias vezes e de forma mais rápida e homogênea do que em plataformas convencionais. É possível obter copias do estado das máquinas antes e depois de um upgrade para comparação (Por exemplo, para garantir que as regras de configuração de um firewall não deixaram de funcionar)

2.7.7 Benefícios da concentração de recursos

Embora a concentração de recursos sem dúvida possua desvantagem para segurança, fica evidente as vantagens econômicas nos campos de controle de acesso físico, implantação de uma política de segurança da informação, gerenciamento das informações, gerenciamento de atualizações, gerenciamento de incidentes além do processo de manutenção.

RISCOS

De acordo com uma pesquisa realizada pela ISACA em julho de 2010 (*ISACA IT Risk/Reward Barometer—China/Hong Kong*) com profissionais de TI das empresas da China/Hong Kong, 42% disseram que os riscos envolvidos na computação em nuvem sobrepõem os benefícios por ela apresentados.

Na contramão destes temores, em uma nova pesquisa realizada em janeiro de 2011 pela CIO Magazine, 70% dos entrevistados entendem a computação em nuvem como parte do plano estratégico da empresa, e pretendem investir U\$1.2 milhões nos próximos 12 meses nessa tecnologia.

A seguir, apresenta-se os principais riscos listados no artigo “*Computação em nuvem: Benefícios, riscos e recomendações para segurança da informação*” (ENISA 2010) as recomendações de gerenciamento são parte integrantes deste artigo e de outros que foram utilizados no processos de pesquisa, podendo ser encontrados nas referencias bibliográficas.

As principais premissas relacionadas a estes riscos são:

- Riscos devem sempre ser analisados como uma relação custo-benefício
- O nível de risco apresentado considera apenas a visão do cliente, e não a do provedor de computação em nuvem.

Os riscos são classificados em três categorias:

- Riscos organizacionais
- Riscos técnicos
- Riscos jurídicos
-

2.8 Riscos organizacionais

2.8.1 Dependência do fornecedor (*Vendor lock-in*)

Por se tratar de uma tecnologia recente, ainda não a ferramentas, procedimentos ou padrões de dados ou interfaces que garantam a portabilidade dos mesmos. Isto torna extremamente difícil para que um cliente realize a migração dos seus dados ou serviços de um provedor ao outro, ou até mesmo de volta a um ambiente interno.

Esta dependência em potencial do serviço provisionado ou de um provedor de nuvem em particular, pode acarretar em uma falha catastrófica para os negócios caso o provedor venha a falir.

Gerenciando o risco: Deve-se optar por um provedor de computação em nuvem que possua uma tecnologia aberta (*Jericho cube*), ou que, caso seja privada, possua interfaces para migração as principais tecnologias do mercado. Tais questões devem figurar em contrato.

Deve-se estudar a reputação do provedor antes de contratar um *software* como serviço; além de avaliar o grau de dependência que a empresa terá com relação a este *software* em questão.

Caso o serviço utilizado seja um SaaS, recomenda-se periodicamente realizar uma cópia dos dados considerados sensíveis pela empresa e armazená-los em formato universal (como o XML), facilitando assim seu acesso caso necessário.

2.8.2 Perda de governança corporativa e de normativas (*compliance*)

Ao utilizar uma solução de computação em nuvem, o cliente transfere uma série de controles para o provedor de nuvem, que eventualmente pode vir a não permitir testes de penetração, mapeamento de vulnerabilidades, dentre outras atividades que impactarão nas práticas de governança.

A perda da governança e dos controles podem impactar diretamente na estratégia da empresa e na sua capacidade de cumprir suas metas e objetivos. Tal condição pode impossibilitar a companhia de cumprir com os requisitos de segurança, confidencialidade, integridade e disponibilidade.

Outro importante fator são as empresas que realizaram investimentos na obtenção de certificações para criarem vantagens competitivas, atendendo a padrões de mercado e requerimento de regulamentações. Eventualmente um provedor de nuvem pode não prover evidências que comprovem essa adequação, ou podem não permitir auditoria externa.

Gerenciando o risco: Novamente reforça-se a importância em contratar um provedor em linha com as necessidades da organização e que permitam procedimentos para atender os requisitos de governança corporativa, *compliance*, auditoria, regulamentações, etc. Uma escolha inadequada impactará diretamente nos negócios da organização.

Deve-se estabelecer Acordos de Nível de Serviço (*Service Level Agreement* – SLA) bem como métricas ou procedimentos (por exemplo, a auditoria interna da organização realizar alguns testes no provedor de nuvem) para garantir que todos procedimentos contratados vem sendo adequadamente realizados

2.8.3 Perda de reputação por ações indiretas

Em ambiente de recursos compartilhados, caso um organização utilize o provedor de computação em nuvem para realizar atividades ilícitas (Por exemplo, envio de spam, exploração de rede (*port scan*), armazenamento de conteúdo inadequado, etc), todos os clientes deste provedor podem ser impactados, seja por um simples bloqueio de IP, ou ate mesmo uma paralisação das atividades.

Gerenciando o risco: No processo de aquisição de um provedor de computação em nuvem, deve-se verificar quem são seus clientes e bem como seu histórico de reputação e incidentes. De forma conservadora, optar por um provedor que só atenda empresas apresenta maior confiabilidade. Este risco é minimizado em nuvens privadas.

2.8.4 Falhas na cadeia de fornecimento

Um provedor de computação em nuvem pode terceirizar algumas tarefas para fornecedores externos. Neste cenário, o nível de segurança do provedor dependerá do nível de seguranças de todos os componentes que fazem parte da cadeia de fornecimento. Uma falha em algum ponto desta estrutura, pode culminar em indisponibilidade dos serviços, perda de dados confidenciais, perda de integridade, quebra de SLA, etc

Gerenciando o risco: O provedor de nuvem necessita ser transparente em seus contratos, explicitando quais serviços encontram-se terceirizados. Cabe então ao consumidor julgar a importância destes serviços, a confiabilidade do provedor, histórico de problemas, etc.

2.9 Riscos técnicos

2.9.1 Falta de recursos

Serviços em nuvem são sob demanda, portanto, é necessário que o provedor estime o poder computacional através de projeções estatísticas antes de vender as soluções. Caso haja uma modelagem inadequada, corre-se o risco de:

- Indisponibilidade dos serviços: Falha na entrega dos serviços, paralisando as operações.

- Falha dos controles de acesso: comprometendo diretamente a confidencialidade e integridade das informações

Recentemente a *Amazon* passou por este problema:

“Servidores da Amazon falham e prejudicam New York Times - IT web – 25/04/2011

Os servidores da Amazon falharam no final da última semana e deixaram mais de 70 sites fora do ar, entre eles o do jornal New York Times e do serviço de localização Foursquare, reportou a Folha.com.

A falha aconteceu com os serviços de nuvem da companhia, que já foi parcialmente restabelecido nesta segunda-feira (25/04).

A companhia ainda informou que alguns dados de consumidores podem não ser reparados.”

Gerenciando o Risco: No ato de contratação de um provedor de computação em nuvem, deve-se verificar quais são as garantias de elasticidades por este oferecida, caso haja uma sobrecarga, o servidor não deve derrubar os serviços, e deve constar no contrato como qual o tempo máximo em que a entrega de serviço perderá capacidade de crescimento.

2.9.2 Falha nos mecanismos de separação

Em um ambiente de computação em nuvem, capacidade de processamento, armazenamento e rede são compartilhados entre vários usuários. Este risco ocorre quando a alguma falha no mecanismo de separação do banco de dados, memória, ou da tabela roteamento. Informações sensíveis podem se misturar ou serem

enviada a destinos errados. Lembrando que seus próprios concorrentes podem estar no mesmo provedor, isto impactaria diretamente nas estratégias competitivas.

Gerenciando o Risco: É necessário conhecer quais mecanismos utilizados pelo provedor de computação em nuvem para impedir que isto aconteça. Verificar se são realizados testes de penetração (por exemplo, verificar se o Cliente1, consegue de alguma forma montar o banco de dados do Cliente2). Recomenda-se que os dados sejam mantidos sob criptografia e esta possuía verificação de hash, caso o risco se materialize, seja o hash será distorcido.

2.9.3 Uso inadequado das contas privilegiadas

As contas com acesso privilegiado (administrados, root, etc), são consideradas de risco pois possuem privilégios para sobrepor os controles existentes. Dependendo da solução contratada em um ambiente de computação em nuvem, a custódia destas contas fica em poder do provedor. Um acesso inadequado, seja por erro ou por atividade criminosa, comprometerá os clientes deste provedor.

Gerenciando o Risco: Deve-se verificar como o provedor gerencia as conta com privilegio administrativos, como por exemplo:

- Há uma conta com privilégios administrativos ativa?
- Quem é responsável por esta conta, há dupla custódia?
- Há registros da utilização desta conta?

- Há um administrador para cada conta privilegiada? (segregação de funções)

2.9.4 Interface de gerenciamento

Há riscos inerentes nas interfaces de gerenciamentos via internet, devido a vulnerabilidades existentes em acessos remotos e navegadores de internet. A situação torna-se mais crítica quando o gerenciamento de toda a nuvem, por parte do provedor, também é realizado via estas interfaces.

Gerenciando o Risco: Este risco pode ser mitigado através de investimentos em questões de segurança por parte do provedor de computação em nuvem.

2.9.5 Captura de informações em tráfego

Devido a características da computação em nuvem, há maior tráfego de informações do que em uma estrutura tradicional. Por exemplo, dados precisam ser transferidos para sincronizar máquinas virtuais, para realização de acesso remoto, etc. Desta forma, esta tecnologia está mais propensa a ser alvo de ataques de Análise de tráfego (Sniffing), spoofing (técnica em que se “falsifica” um endereço IP), interceptação de pacotes (man-in-the-middle), side channel e replay attacks.

Gerenciando o Risco: Nas cláusulas de contrato, o provedor de computação em nuvem deve explicitar quais informações trafegam na nuvem. Estes dados em trânsito necessitam ser criptografados, pois, embora as redes de provedores de nuvem possam ser mais seguras que a Internet aberta, compostas de muitos elementos diferentes e diferentes organizações compartilham a nuvem. Por isso, é

importante proteger essas informações sensíveis e regulamentadas em trânsito até mesmo dentro da rede dos provedores de nuvem.

É necessário haver controles sobre o gerenciamento das chaves criptográficas, bem como quem podem ter acesso às mesmas.

2.9.6 Descarte dos dados de forma insegura / não eficiente

Em caso de uma troca de provedor de computação em nuvem, pode-se ocorrer o risco dos dados ficarem ativos por um tempo fora do especificado na política de segurança da informação. Em se tratando de computação em nuvem, alguns procedimentos são impossíveis de serem realizados (como por exemplo, destruir o disco contendo informações).

Quando um pedido de exclusão é realizado, isso pode não resultar numa exclusão completa dos dados (situação que ocorre na maioria dos Sistemas Operacionais). Eventualmente uma exclusão completa pode não ser possível devido a limitações nas API's utilizadas pelo provedor.

Gerenciando o Risco: Este risco pode ser minimizado através de uma criptografia adequada, entretanto, deve-se mesmo após a exclusão dos dados, deve-se realizar teste de recuperação de dados a fim de identificar eventuais resíduos.

2.9.7 Ataques distribuídos de negação de serviço

Devido a grande concentração de informações contidas em um servidor em nuvem e sua visibilidade, estes estarão mais suscetíveis a serem alvos de grupos que praticam ataques de negação de serviço.

Adicionalmente, no conceito de “pague o que utilizar”, surge um nome tipo de ataque, denominado ataque de negação de serviço com impactos financeiros (*Economic Denial of Service* - EDOS). Esta pratica visa prejudicar financeiramente uma organização que possua serviços na rede, sobrecarregando seu uso de recursos e impactando diretamente no custo desta contratação.

Gerenciando o risco: Deve-se estabelecer no ato do contrato quais os recursos utilizados pelo provedor para mitigar um ataque de negação de serviço , como por exemplo: inspeção de pacotes (*deep packet analysis*), estrangulamento de pacotes (*traffic throttling*), descarte de pacotes (*blackholing*), etc. Bem como, de quem é a responsabilidade de monitorar a utilização dos recursos.

2.10 Riscos jurídicos

2.10.1 Intimação, busca e apreensão

No caso de uma confiscação física do hardware devido a uma intimação por órgãos de segurança ou ações cíveis, a centralização do armazenamento, bem como locação compartilhada significa que muitos clientes correm o risco de a

exposição de seus dados. Por outro lado, pode ser impossível de confiscar um nuvem completa.

Gerenciando o risco: Como todos aspectos legais envolvendo tecnologia da informação, este ponto ainda é confuso em todo o mundo. A utilização de criptografia pode minimizar os danos desta situação, entretanto, com o crescimento da computação em nuvem, deve-se criar padrões para estes tipos de investigações, levando em conta a privacidade de outros usuários. Adicionalmente, a adoção de uma nuvem privada minimiza os riscos.

2.10.2 Mudança de jurisdição

Em uma estrutura de computação em nuvem, os dados podem mudar constantemente de jurisdição, onde algumas destas podem apresentar certos riscos. Por exemplo, se servidores estiverem localizados em países de alto risco (países que não respeitam acordos internacionais, autocracias, etc) No caso de alguma disputa diplomática, ou situação imprevisível, os dados destes servidores podem ser confiscados.

Gerenciando o risco: O provedor de computação em nuvem deve ter transparência ao informar em quais localidades tem atuação. Caso a organização contratante julgue necessário, pode incluir cláusulas em contrato que especifique quais localidades seus dados irão transitar.

RECOMENDAÇÕES FINAIS

Adicionalmente aos principais riscos, a *Cloud Security Alliance* elaborou uma série de recomendações/pontos de atenção no processo de adoção e utilização da computação em nuvem. Na seqüência encontram-se os julgados mais relevantes a questão da computação em nuvem:

2.11 Governança corporativa e aspectos legais

- É necessário ter em mente que uma parte da redução de custos decorrente da adoção de Computação em nuvem deve ser direcionada para o processo de migração para computação em nuvem, bem como o de escolha do provedor;
- O ponto inicial do processo de migração para computação em nuvem deve ser classificando as informações, serviços, aplicações, etc.

- Para as classificações críticas da organização, a abordagem de gerenciamento de riscos deve incluir a identificação e avaliação de ativos, identificação e análise de ameaças e vulnerabilidades e seu potencial impacto nos ativos (cenários de riscos e incidentes).
- Os departamentos de segurança devem ser envolvidos no desenvolvimento de planos de tratamento de riscos (controle, prevenção, transferência, aceitação). Posteriormente, o departamento jurídico deve ser envolvido para elaborar os termos contratuais dos planos de tratamento de riscos e acordos de serviço (*SLA*).
- Métricas e padrões de segurança (particularmente aquelas relacionadas a requisitos legais e de conformidade) devem ser incluídas em qualquer acordo de nível de serviço (*SLA*) e contratos. Estas métricas e padrões devem ser documentadas e ser demonstráveis (auditáveis).
- Deve-se estabelecer requisitos contratuais apropriados e controles tecnológicos para coletar dados necessários para informar as decisões sobre os riscos à informação (ex. uso da informação, controle de acesso, controles de segurança, localização, etc.).
- Assegure sua habilidade de conhecimento sobre a localização geográfica de armazenamento. Estipule isto em seus acordos em nível de serviço (*SLA*) e contratos. Garanta que controles apropriados relativos às restrições de cada país envolvido no serviço estejam definidos e reforçados.

- O contrato de serviços de nuvem deve permitir que o cliente ou terceiro designado monitore o desempenho do provedor de serviços e teste as vulnerabilidades no sistema.

2.12 Auditoria

- Deve-se analisar o impacto de mover dados e aplicações para serviços de computação em nuvem sobre as políticas e procedimentos da organização. Os clientes devem avaliar quais políticas e procedimentos relacionados com normas terão de ser alterados. Exemplos de políticas e procedimentos impactados incluem relatórios de atividades, logs, retenção de dados, resposta a incidentes, controles de testes e políticas de privacidade.
- Preparar evidências de como cada exigência está sendo cumprida. Coletar evidências de conformidade através da multiplicidade de regulamentos e de requisitos é um desafio. Clientes dos serviços de computação em nuvem devem desenvolver processos para coletar e armazenar evidências de conformidade, incluindo logs de auditoria e relatórios de atividades, cópias das configurações dos sistemas, relatórios de gestão de mudanças e resultados de outros procedimentos de teste. Dependendo do modelo de serviço o provedor pode precisar fornecer muitas dessas informações
- Opte por provedores de computação em nuvem com certificação (Por exemplo SAS 70 Tipo II, ou novas certificações que virão a surgir) . Os provedores devem ter, no mínimo, estas homologações, pois ela

proporcionará um ponto de referência reconhecido para auditores e avaliadores.

2.13 Portabilidade e Interoperabilidade

- As organizações devem considerar na adoção de um provedor de computação em nuvem, que eventualmente haja a necessidade de mudar de provedor. Por este motivo deve-se optar por provedores que ofereçam essa possibilidade. (vide os riscos de dependência de um fornecedor)

2.14 Continuidade de Negócios, Recuperação de Desastres e Incidentes

- Clientes precisam confirmar que o provedor possui uma política de plano de continuidade de negócios aprovada pelo conselho de administração do provedor. Bem como obter evidências do apoio efetivo da gestão e revisão periódica do programa de continuidade de negócios para garantir que este esteja ativo.
- O plano de recuperação de desastres do cliente deve considerar uma falha catastrófica no ambiente em nuvem e ter alternativas para essa situação.
- Clientes de computação em nuvem precisam definir claramente e comunicar aos provedores o que eles consideram incidentes (tais como roubo de dados) versus meros eventos (tais como alertas de suspeita de intrusão) antes de implementar o serviço.

- Clientes de computação em nuvem devem investigar quais ferramentas de detecção e análise de incidentes o provedor utiliza para garantir que eles sejam compatíveis com seus próprios sistemas. Um formato de *log* proprietário ou incomum poderia ser um grande problema em investigações conjuntas, particularmente aqueles que envolvam questões legais ou intervenção governamental.

CONCLUSÃO

A computação em nuvem irá continuar em crescimento e impactando a tecnologia e as organizações. Como demonstrado no presente trabalho de conclusão de curso, muitos são os benefícios oferecidos por essa nova e poderosa tecnologia, entretanto, mostra-se necessário um adequado planejamento do que será migrado para “nuvem”, dos riscos envolvidos e de estratégias para gerenciá-los, garantindo que todo o processo permaneça em linha com os planos da organização.

REFERÊNCIAS BIBLIOGRÁFICAS

ARMBRUST, M, Fox, A., Griffith, R., Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia - "Above the Clouds: A Berkeley View of Cloud Computing" – UC Berkeley Reliable Adaptive Distributed Systems Laboratory - February 10, 2009, disponível em: <<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.149.7163&rep=rep1&type=pdf>>, acessado em 01/maio/2011 às 16h06.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Citação: NBR-10520/ago - 2002. Rio de Janeiro: ABNT, 2002.

Referências: NBR-6023/ago. 2002. Rio de Janeiro: ABNT, 2002.

CASTRO, Rita de C. C; Sousa, Verônica L. Pimentel, Segurança em Cloud Computing: Governança e Gerenciamento de Riscos de Segurança, disponível em <<http://www.infobrasil.inf.br/userfiles/26-05-S5-1-68740Seguranca%20em%20Cloud.pdf>>, acessado em 01/maio/2011 às 17h32.

Cloud Security Alliance (CSA), Security Guidance for Critical Areas of Focus in Cloud Computing, Dezembro 2009, Disponível em: <www.cloudsecurityalliance.org/guidance/csaguide.pdf >, acesso em 08/ março/2011 às 22h30.

European Network and Information Security Agency (ENISA), Cloud Computing Risk Assesements, Novembro 2010, Disponível em: <<http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment>> acesso em 08/março/2011 às 21h35.

Information System Audit and Control Association (ISACA), Computação em nuvem: benefícios para o negócio com perspectivas de segurança, governança e qualidade, 2009, Disponível em < <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Business-Benefits-With-Security-Governance-and-Assurance-Perspective.aspx>> acesso em 08/ março/2011 às 21h00.

Information System Audit and Control Association (ISACA), 2010 ISACA IT Risk/Reward Barometer—China/Hong Kong, Disponível em <<http://www.isaca.org/About-ISACA/Press-room/News-Releases/2010/Pages/ISACA-US-IT-Risk-Reward-Barometer-Survey.aspx>> acesso em 01/abril/2011 às 10h15.

Jericho Fórum, Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration, disponível em: http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf, acesso em 01/abril/2011 às 10h15.

National Institute of Standard and Technology (NIST), The NIST definition of cloud computing (draft), Disponível em: http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf, acesso em 05/abril/2011 às 20h15.