V Congresso CONSAD de Gestão Pública
Centro de Convenções Ulysses Guimarães
Brasília/DF – 4, 5 e 6 de junho de 2012

CLOUD COMPUTING: QUESTÕES CRÍTICAS PARA A IMPLEMENTAÇÃO EM ORGANIZAÇÕES PÚBLICAS

Fernando C. G. D. Guerra
Marcelo de Alencar Veloso
Rogério Luís Massensini

CLOUD COMPUTING: QUESTÕES CRÍTICAS PARA A IMPLEMENTAÇÃO EM ORGANIZAÇÕES PÚBLICAS

Fernando C. G. D. Guerra
Marcelo de Alencar Veloso
Rogério Luís Massensini

RESUMO

O Gartner (2008) define o termo *Cloud Computing* como computação em nuvem, em que recursos relacionados de Tecnologia da Informação e Comunicação são fornecidos "como serviço" usando tecnologias de Internet para vários clientes externos. Segundo Daryl Plummer, vice-presidente do *Gartner* o uso, cada vez mais, dos recursos tecnológicos na internet *"se deve, em parte, à popularização e padronização de tecnologias, e mais importante, ao dramático crescimento da popularidade da Internet."* Portanto, o desenvolvimento explosivo das tecnologias da internet mostra-se positivo e impositivo à sua utilização. No entanto, pontos negativos também estão presentes em sua aplicabilidade. Sendo assim, partindo do princípio da inevitabilidade da adoção de soluções de *Cloud Computing,* o objetivo deste estudo é apresentar alguns pontos a serem considerados ao se fazer a sua implementação, a fim de minimizar impactos negativos nos órgãos e entidades públicas. São questões que perpassam pela governança de processos, segurança da informação, infraestrutura, legislação e interoperabilidade dos serviços públicos.

Palavras-chave: *Cloud Computing*. Computação em Nuvem. Segurança da Informação. Governança de Processos.

1 INTRODUÇÃO

As mudanças promovidas pela internet no campo dos serviços ofertados à sociedade são dinâmicas, mostrando-se cada vez mais rápidas. Os processamentos dos serviços disponíveis na internet buscam, por meio da popularização desse canal de comunicação entre os diversos atores, multiplicar as possibilidades de se atender os processos demandados.

O crescimento da popularidade da internet, na utilização de serviços privados e, nos últimos tempos, de serviços públicos, ou seja, serviços ofertados **usando novas tecnologias de internet para vários clientes externos** exige-nos atenção quanto às questões críticas para implementação de *Cloud Computing* em organizações públicas.

Essa nova tecnologia, em nuvem, é um ambiente em que a escalabilidade e a disponibilidade proporcionam e oferecem redução de custos por meio de computação otimizada, a qual se trata da utilização de serviços, aplicações, informação e infraestrutura composta por grupos de recursos computacionais como: de rede, de informação e de armazenamento. Componentes estes que são organizados, implementados, desativados ou escalonados a prover um modelo de locação ao consumo sobre demanda de recursos.

Assim, dois pontos de atenção serão abordados neste artigo: **Governança de Processos e Segurança da informação**, com a pretensão de se tratar exatamente da importância que ambos representam na implementação de computação em nuvem para ofertar serviços públicos aos cidadãos.

Para tanto, o próximo tópico: **Vantagens e desvantagens** colocará em discussão alguns apontamentos, a partir da definição do termo *Cloud Computing*, quanto às vantagens e desvantagens que se podem levantar sobre esta tecnologia, o que nos serve como suporte ao debate para sua implementação em organizações públicas.

2 VANTAGENS E DESVANTAGENS

O tema de *Cloud Computing* (computação em nuvem) é uma tendência ascendente no ambiente organizacional. Embora possua inúmeros benefícios sobre as tecnologias atuais, a sua utilização e o processo de transição devem ser avaliados com cautela. A organização não deve esquecer-se de problematizar questões sobre avaliações de riscos entre as relações de absorção de uma nova tecnologia e os seus clientes, que utilizam os serviços ofertados por ela.

Deste modo, faz-se necessário, antes de se apresentar as vantagens e desvantagens da implementação de *Cloud Computing*, discutir os conceitos do termo em questão, para melhor entendimento sobre sua utilização.

O Gartner (2008) define o termo *Cloud Computing* como computação em nuvem, em que recursos relacionados de Tecnologia da Informação e Comunicação são fornecidos "como serviço" usando tecnologias de Internet para vários clientes externos. Segundo Daryl Plummer, vice-presidente do *Gartner* o uso, cada vez mais, dos recursos tecnológicos na internet *"se deve, em parte, à popularização e padronização de tecnologias, e mais importante, ao dramático crescimento da popularidade da Internet."* Portanto, o desenvolvimento explosivo das tecnologias da internet mostra-se positivo e impositivo à sua utilização.

A ISACA (2009, p.5) fundamenta a denominação de *Cloud Computing* do Gartner ao definir que:

> 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.

Desta forma, tais definições são observadas no modelo do NIST (2011), que é uma entidade governamental americana, em que o termo computação em nuvem se define a partir de: cinco características essenciais, três modelos de serviço e quatro modelos de implementação, conforme lista a Figura 1.

Figura 1: Modelo Visual da Definição Corrente de Computação em Nuvem do NIST[i]

No contexto de computação em nuvem, o *software* é um componente de uso heterogêneo executado à distância, que desempenha a funcionalidade de serviço. Os dados e informações vão ou não estar armazenados em um provedor de serviço, ou seja, fora da organização (na nuvem).

As características essenciais, adaptadas do NIST (2011), são as listadas no quadro abaixo:

Autoatendimento sob demanda. O contratante provisiona unilateralmente suas necessidades computacionais sem requerer interação humana através de automações e definição de regras tais como: armazenamento de espaço de disco (HD) e etc.
Amplo acesso a rede. Capacidades disponíveis na rede de dados e acessadas através de dispositivos de plataformas de clientes leves (*thin clients*) ou não (por exemplo, telefones celulares, laptops, e PDAs) da mesma forma que demais serviços de software tradicionais ou baseados em nuvem.
***Pool* de Recursos**. Trata-se de recursos computacionais tais como: armazenamento, processamento, memória, largura de banda, e máquinas virtuais que são utilizados por múltiplos consumidores e por este motivo possibilita a divisão dos custos destes itens comuns entre os contratantes do serviço.
Elasticidade Rápida. Facilidade em gerir elasticamente as capacidades provisionadas, aumentando-as ou diminuindo-as conforme as necessidades, em momentos de picos ou ociosidade.
Serviços mensuráveis. O contratante e o contratado conseguem mensurar e otimizar a utilização de recursos maximizando a capacidade de avaliar algum nível de abstração para tipos de serviços tais como: armazenamento, processamento, largura de banda e até contas de usuário ativas.

Há três modalidades de serviços na computação em nuvem:

1. SAAS – Software as a Service (software como serviço);
2. PAAS – Plataform as a Service (plataforma como serviço);
3. IAAS – Infrastructure as a Service (infraestrutura como serviço) disponíveis para aos modelos de implantação conhecidos como nuvem pública, nuvem privada ou nuvem híbrida (a união das duas anteriores).

Essa é uma das razões para que a computação em nuvem seja discutida de um modo mais aprofundado, uma vez que clientes internos e externos se tornam cada vez mais participantes ao utilizar ferramentas disponíveis nestes ambientes, serviços estes disponíveis conforme a figura 2 de Taxonomia da *OpenCrowd*.

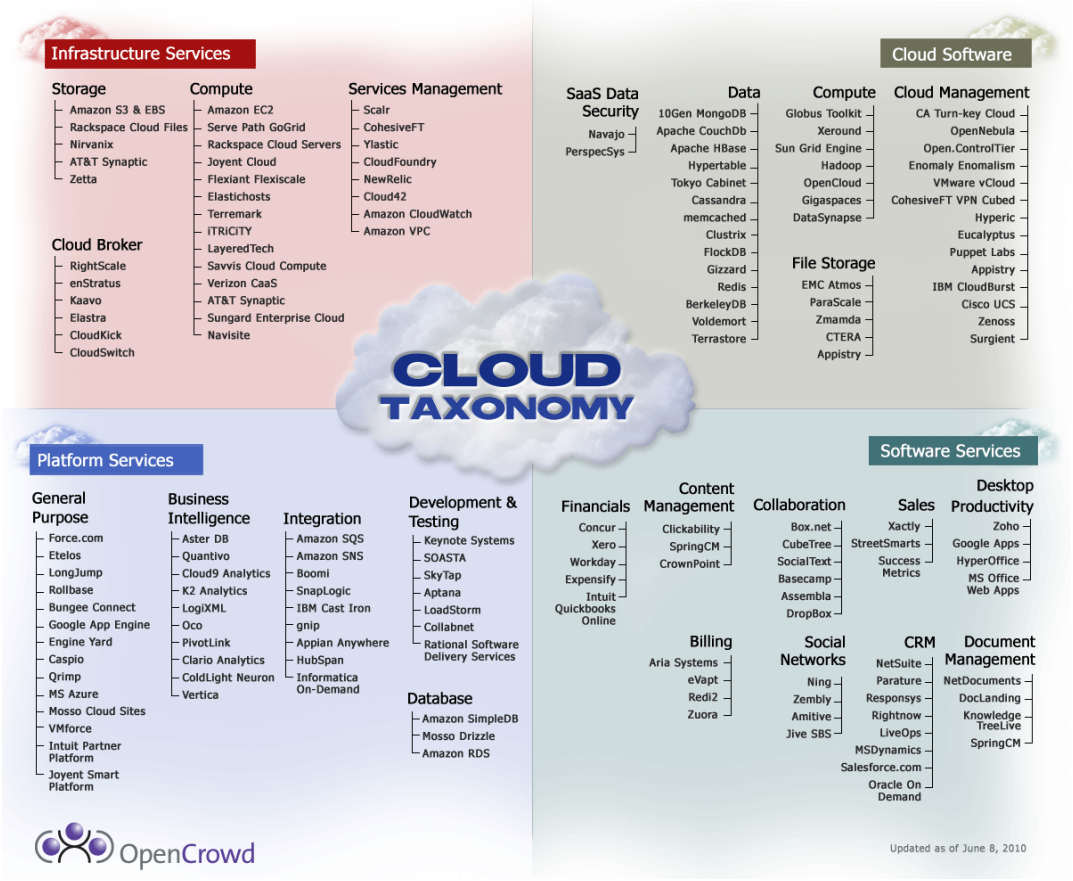
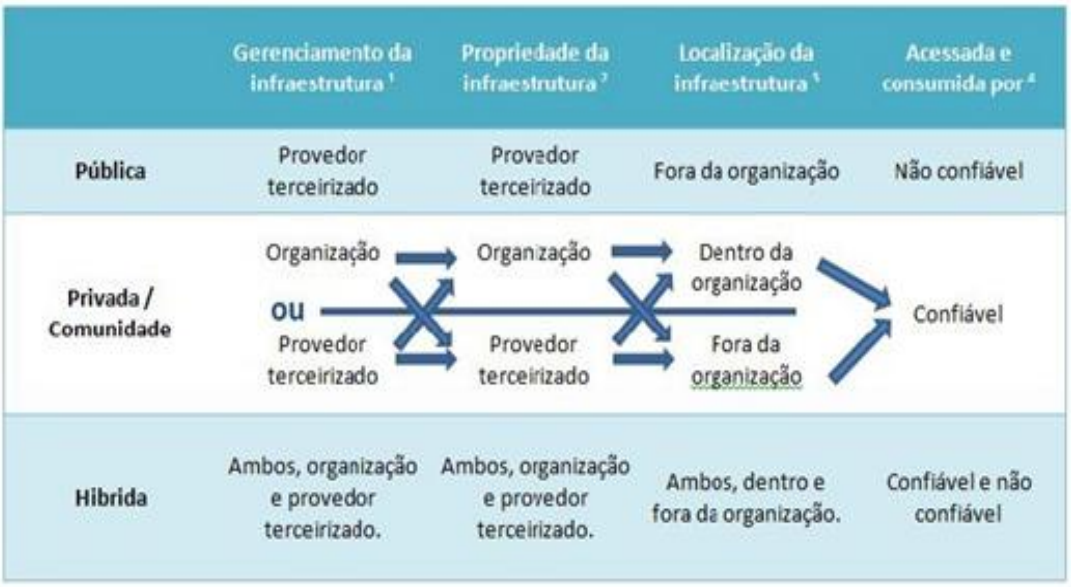


Figura 2: Taxonomia OpenCrowd[ii]

Devido a essa diversidade de possibilidades, deve haver um entendimento do contratante para cada uma das modalidades de serviço para que não haja desperdícios dos recursos financeiros. Em cada uma das modalidades de serviço deve existir ponderação e cautela, pois todas possuem prós e contras que devem ser avaliados.

Se por um lado ocorre a economia e ganhos ao contratar os serviços por escala, comparando uma modalidade para com a outra, surge o risco negativo ao observar que o contratante pode se tornar dependente do fornecedor, ou seja, perder o controle total do ambiente. Por isso se faz necessário ao contratante avaliar qual o melhor modelo para seu negócio.

Para cada ambiente de C*loud Computing* devem ser avaliados os seus riscos, conforme listados na figura 3 de modelos de implantação de nuvem da CSA (*Cloud Security Alliance*, 2010 p.25).



[1] Gerenciamento inclui: Governança, Operação, Segurança, Conformidade, etc...
[2] A infraestrutura implica em infraestrutura física bem como facilidades, computação, rede e equipamentos de armazenamento
[3] A localização da infraestrutura é tanto física e relativa para o gerenciamento organizacional quanto a conversa entre proprietário e controle.
[4] Clientes confiáveis de serviço são aqueles considerados parte legal/contratual/politica de uma organização, incluindo empregados, contratados e parceiros de negócios. Clientes não confiáveis são aqueles que podem ser autorizados para consumir alguns/todos os serviços, mas não tem extensão logica com a organização.

Figura 3: Modelos de Implantação da Nuvem

Da mesma forma, cada modelo deve ser compreendido conforme listado na tabela abaixo.

MODELOS DE SERVIÇOS	VANTAGENS	DESVANTAGENS
Infraestrutura como serviço (IaaS)	O provedor da nuvem entrega o ambiente que a TIC da contratante julgar necessária. Este serviço é a modalidade mais completa, pois envolve todo o hardware, processamento, armazenamento, infra e que podem ser compartilhados entre os clientes dos provedores de nuvem. Desta forma há uma distribuição de custos fixos que são distribuídos entre o provedor e seus clientes, gerando economia.	É bem semelhante às tarefas de integração tradicionais.
Plataforma como serviço (PaaS)	Geralmente o provedor da nuvem entrega os servidores virtuais pré-carregados com sistemas operacionais instalados e prontos para serem utilizados. Estes podem conter banco de dados para ambiente de produção e desenvolvimento, o que reduz os esforços das áreas tradicionais de TI.	A integração dos sistemas envolve novos desafios ligados às transformações entre o ambiente local e de nuvem, além dos tradicionais.
Software como serviço (SaaS)	Geralmente se torna indicado para aqueles que necessitam somente de soluções em programas e aplicativos tecnológicos. Os fornecedores entregam aplicativos totalmente funcionais acessados pelos usuários através dos navegadores da Web. As economias de escala para essas soluções podem ser enormes, chegando a representar um custo 10 vezes menor.	O fornecedor do serviço de nuvem controla totalmente cada um dos sistemas. Ainda há muitos casos dos sistemas não poderem ser integrados a outros de forma alguma,embora atualmente os fornecedores começarem a ofertar opções de APIs para habilitar a integração entre os sistemas. Deve haver uma preocupação do contratante para ter o recurso da integração de identidades.


Existem vantagens e desvantagens a serem consideradas ao adotar soluções de *Cloud*., conforme tabela adaptada de Veras (2011, p.33-34):

VANTAGENS	CONCEITO	EXEMPLOS NA ADM. PÚBLICA
Menores custos de infraestrutura	A ideia de se pagar somente pelo que consome sem ter que investir capital aos recursos de infraestrutura interna;	Armazenar arquivos em discos (HD); Diminuir a necessidade de fornecer manutenção da infraestrutura física de redes locais cliente/servidor;
Aumento da utilização da infraestrutura	Custos divididos entre contratantes que utilizam de recursos de TI comuns utilizado em apoio ao provedor;	Reduzir custos de compras ou utilização de *software* e *hardware* coletivo, como: *Firewalls*, Discos (HD), módulos de memórias, *Switch*, computadores, etc.;
Aumento da segurança	Uma infraestrutura centralizada pode ajudar a melhorar rotinas de *backup*, otimizá-las e testa-las, embora exista controvérsias;	Todos os dados dos sistemas podem estar alocados na estrutura contratada em um único local;
Acesso a aplicações sofisticadas	Aplicações com alto custo podem ser utilizadas com recursos sob demanda;	Permite acesso a aplicações conforme as necessidades, reduzindo investimentos e alocação de recursos;
Economia de energia	Redução de custo de energia e refrigeração;	Os servidores se tornam virtuais e não ficam mais no ambiente do contratante;
Aumento da produtividade por usuário	Como o usuário pode acessar as aplicações disponíveis de qualquer lugar tende a ter um aumento de produtividade em sua rotina de trabalho;	Qualquer aplicação (sistema) torna-se disponível 24x7, independente da localização do usuário;
Aumento da confiabilidade	Com a existência de contingência quase que obrigatória, tende a melhorar a confiabilidade das aplicações disponíveis aos clientes;	Geralmente as empresas contratadas possuem *links* de dados redundantes, geradores de energia, etc.;
Escalabilidade sob demanda	Facilidade em alocar recursos sob demanda.	Aumento de memória, discos (HD), processadores, capacidade dos computadores conforme as necessidades.

DESAFIOS	CONCEITO	EXEMPLOS NA ADM. PÚBLICA
Falta de interoperabilidade	A maioria dos modelos disponíveis ainda é realizada de forma integrada verticalmente e limita a escolha da plataforma;	Falta definir um padrão comum entre as distribuições dos serviços. Seria como no passado comprar um banco de dados que não se comunicava com outro;
Compatibilidade entre operações	Muitas das aplicações disponibilizadas para nuvem ainda são incompatíveis com as aplicações legadas;	Nem todo o ambiente possibilita realizar a integração de um sistema local com uma aplicação na nuvem;
Dificuldades em obedecer a normas regulatórias	Ainda se faz necessário definir ou estabelecer critérios legais de uma forma melhor estruturada;	Não existem leis ou regulamentações sobre a proteção de dados armazenados nos servidores, etc.;
Segurança inadequada	O compartilhamento de estrutura e base de códigos por serem centralizados pode se tornar prejudicial em alguns casos para o negócio dos contratantes.	Riscos para as informações da organização, ao ter seus dados em ambientes utilizados também por outros clientes desconhecidos.

Percebe-se no mercado a utilização dos serviços de *Cloud Computing* em organizações que necessitam de elasticidade nas suas aplicações rapidamente, ou que não tem recursos físicos, tecnológicos e humanos disponíveis ou não desejam realizar estes investimentos, focando somente no seu negócio. Esta é uma opção para a utilização de soluções de nuvem, mas cabe ao tomador de decisão avaliar os custos e riscos a cada nova situação de contratação, uma vez que os custos com a tecnologia tendem a cair com a sua proliferação e utilização em massa por entidades públicas e privadas.

A utilização de *Cloud Computing* não é apenas para os que não têm recursos físicos, tecnológicos e humanos, mas sim para todos que desejam maximizar suas aplicações (sistemas) ou tarefas com a utilização da nova tecnologia da informação e comunicação emergente no mercado. Um bom exemplo de utilização de *Cloud Computing* seria para um ambiente de desenvolvimento e homologação, utilizando-o apenas quando necessário, reduzindo custos ao contratar um pool de recursos no provedor de nuvem.

Mas toda nova tecnologia gera reflexões. Em fevereiro de 2012 foi publicado um *ranking* comparativo sobre a utilização da tecnologia *Cloud Computing* em alguns países. Uma vez que o Brasil está em 24º (vigésimo quarto) lugar comparando-o a outros países mais desenvolvidos sobre o uso da nova tecnologia, faz-se necessário avaliar os riscos dos itens considerados no trabalho de pesquisa do BSA aos interessados em utilizar a nova tecnologia.

> A Pontuação Global de Computação em Nuvem, da BSA, oferece um roteiro para iniciativas e políticas que os países podem – e devem – adotar para que se materialize todo o potencial de crescimento econômico. (BSA, 2012, p.1).

No entanto, pontos negativos também estão presentes em sua aplicabilidade. Sendo assim, é importante ponderar caminhos para minimizar impactos negativos com a decisão de se implementar *Cloud Computing* nos órgãos e entidades públicas.

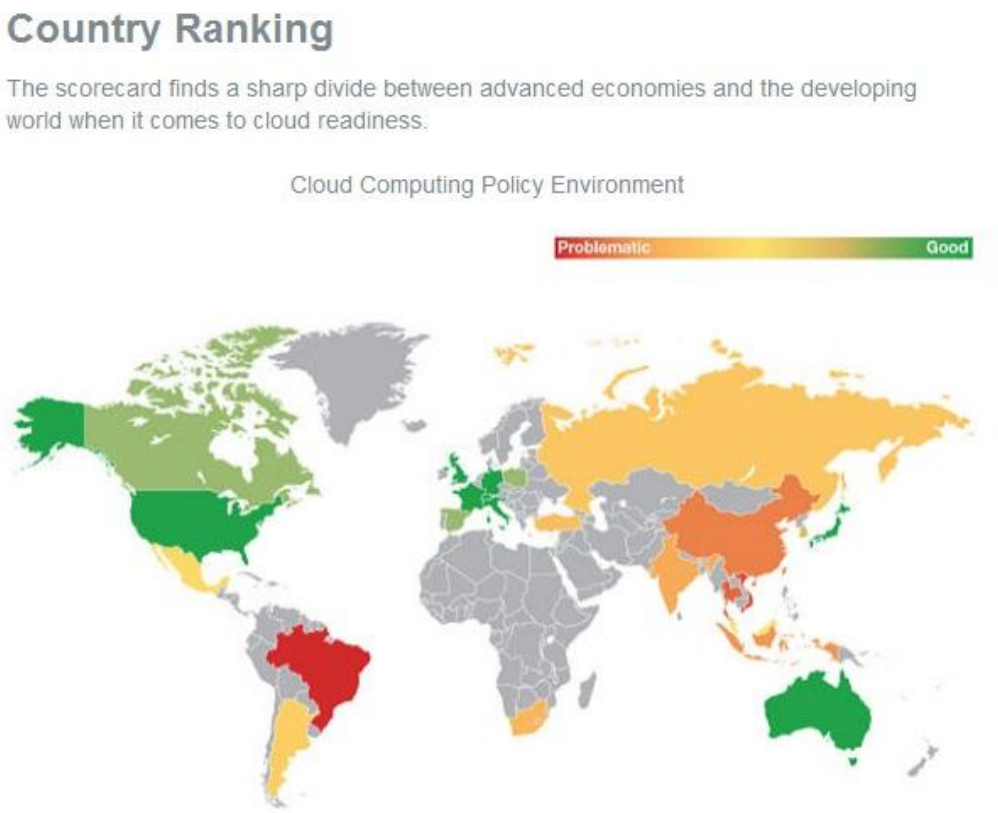


Figura 4: Ranking dos países[iii]

Se avaliarmos visualmente a figura acima, o Brasil é listado no *ranking* entre os demais países com a cor vermelha, que tende a ser problemática.

2.1 Reflexões sobre o negócio na implantação de *Cloud Computing*

Faz-se necessário ter um catálogo de serviços de TI da instituição para que os gestores da alta cúpula reflitam em conjunto sobre o que deve ser migrado para a tecnologia *Cloud Computing*, sempre avaliando e mitigando os riscos do negócio em cada uma das aplicações de TI (sistemas) ao ser transferida a responsabilidade a terceiros.

Se os gestores pelas áreas de TI demorarem a se posicionar, corre-se o risco dos responsáveis pelas unidades de negócios contratarem soluções na nuvem até mesmo sem avisar o departamento de tecnologia, com falta de alinhamento entre as estratégias do negócio e as estratégias de TI, desconsiderando avaliar parâmetros como segurança da informação e outros custos ocultos como *link* de dados (circuito).

Afinal, não basta apenas transferir problemas de processos de negócio e de segurança da informação que muitas vezes não estão definidos dentro de casa a terceiros, pensando que estes riscos estão sendo geridos de uma forma melhor. Cabe a ambos, contratante e contratado monitorar as informações e processos, avaliando os serviços na nuvem.

O contratante não pode pensar que somente ter um contrato bem redigido é o suficiente para acompanhar seus serviços, e que SLAs (*Service Level Agreement)* definidos sejam o suficiente para se atingir a segurança ou a escalabilidade dos dados na nuvem.

A contratação de um serviço de *e-mail* na nuvem poderá ficar fora do ar durante horas ou dias e o contratante terá que aguardar a resposta do contratado para solucionar o seu problema, uma vez que os gestores da organização transferiram essa responsabilidade e parte do seu negócio para o ambiente da nuvem.

Outro exemplo simples, seria a não definição sobre ações de compra, descarte e volume de contas de *e-mail* contratadas, uma vez que uma contração sem a existência de regras definidas sobre o gerenciamento das contas pode onerar os cofres da organização contratante.


Neste exemplo, é preciso definição do que será feito com os dados de uma conta de *e-mail* quando seu proprietário (funcionário) é desligado da organização. Se ninguém sabe, a conta continuará sendo paga pela instituição, seja no valor da conta de *e-mail,* no espaço em disco que está sendo utilizado, no tempo na realização de *backup* e restauração de dados, etc. Porém, se as áreas de TI deletarem ou destruirem os dados armazenados na conta de *e-mail* quando o funcionário for desligado da instituição, é preciso garantir que as informações ali armazenadas não serão mais importantes para a organização.

Então, caso não existam regras ou definições de processos sobre como tratar as informações de um serviço simples como *e-mail*, poderá ocorrer um ônus para a organização ao manter esta estrutura, uma vez que o consumo dos serviços de TI tende a aumentar.

Comprar uma conta de *e-mail* é fácil, mas não se ter o controle sobre o que consome os recursos financeiros da organização pode inviabilizar o negócio a longo prazo, ao imaginar que a falta de gestão de 20.000 contas de *e-mail* ao ano pode onerar os cofres da administração pública.

Um ponto a favor sobre utilização da nova tecnologia são os custos, que são uma preocupação de todas as entidades, sejam públicas ou privadas. Por esta razão, há necessidade de se ter processos internos e externos bem monitorados, para que os gastos não estejam apenas sendo transferidos de um recurso para outro, pois pode ocorrer de não se considerar o valor por exemplo do acesso ao *link* de dados (circuito), uma vez que sua utilização tende a subir.

Enquanto o serviço de *e-mail* se encontra localmente na organização o recurso de banda utilizado é o local, mas migrar para a nuvem, o *link* de dados utilizado passa a ser o de saída para a internet. Conforme pode ser observado pela citação do analista da Forrester que “para cada grupo de 100 utilizadores bastante activos no Outlook instalado localmente, são necessários 37 KB/s. Já o mesmo grupo de 100 utilizadores ligados ao servidor de e-mail Outlook alojado numa plataforma de e-mail requer mais do dobro, 85KB/s” (COMPUTERWORLD, 2011).

Não considerar o *link* a curto, médio e longo prazo pode se tornar oneroso, uma vez que ao menos que se forneça internamente um serviço idêntico ao que estava contratado, alterá-lo se tornará traumático tanto para o gestor quanto para a instituição.

Como a tecnologia da informação se encontra presente em todo serviço do negócio, se torna imprescindível avaliar questões relacionados aos processos mapeados, para não haver desperdício dos recursos utilizados pela instituição, sendo esta uma ação conjunta de seus gestores, uma vez que o gestor de TI não pode e não deve julgar ou priorizar sozinho as ações de mitigação de risco da organização.

Outro ponto a considerar é que embora o Brasil receba uma boa avaliação na área da "Estrutura Tecnológica e Banda-larga", conforme o estudo da BSA, o mesmo também demonstra que há questões que merecem atenção, como a possibilidade de realizar mudanças em sua legislação para enfrentar ações contra "Crimes Digitais" e outros pontos avaliados como: “Privacidade de Dados", "Segurança", "Propriedade Intelectual", "Apoio a Normas da Indústria e Harmonia Internacional de Regras" e "Promoção de Livre-Comércio" conforme mostra a figura 5 (BSA, 2012, p.12).

Tabela Global de Computação em Nuvem por País

✔ Sim ✖ Não ◑ Parcial

# QUESTÃO	Argentina	Austrália	Brasil
PRIVACIDADE DE DADOS			
1. Existem leis ou regulamentações governando a coleta, o uso ou outro processamento de informações pessoais?	✔	✔	◑
2. Qual é a abrangência e a cobertura da lei de privacidade?	Abrangente	Abrangente	Não se aplica
3. A lei de privacidade é compatível com os Princípios de Privacidade da Diretiva da UE de Proteção de Dados?	✔	◑	✖
4. A lei de privacidade é compatível com os Princípios de Privacidade da Plataforma de Privacidade da APEC?	✔	✔	✖
5. Há a disponibilidade de direito privado de ação contra violações de privacidade de dados?	Disponível	Não disponível	Disponível
6. Existe uma agência (ou regulador) efetivo encarregado de fiscalizar o cumprimento de leis de privacidade?	Regulador nacional	Regulador nacional	Nenhum
7. Qual é a natureza do regulador de privacidade?	Nomeado único	Nomeado único	Não se aplica
8. Controladores de dados são livres de exigências de registro?	✖	✔	✔
9. As transferências por fronteira são livres de exigências de registro?	◑	✔	✔
10. Existe uma lei de notificação de violação de dados?	✖	✖	✖
SEGURANÇA			
1. Existe uma lei ou regulamentação que garanta validade legal para assinaturas eletrônicas?	✔	✔	✔
2. Provedores de acesso e de conteúdo são livres de filtragem e/ou censura obrigatória?	✔	✔	✔
3. Existem leis ou códigos viáveis contendo exigências gerais de segurança para hospedagem de dados digitais e provedores de serviços de nuvem?	Cobertura limitada na legislação	Cobertura limitada na legislação	Nenhuma
4. Existem leis ou códigos viáveis contendo requisitos de auditoria específicos para hospedagem de dados digitais e provedores de serviços de nuvem?	Cobertura limitada na legislação	Nenhuma	Nenhuma
5. Existem leis e regulamentações de segurança exigindo certificações específicas para produtos tecnológicos?	Sem exigências	Exigências limitadas	Sem exigências
CRIME DIGITAL			
1. Existem leis de crime digital em aplicação?	✔	✔	✖
2. As leis de crime digital são consistentes com a Convenção de Budapeste sobre crimes digitais?	✔	✔	✖
3. Que acesso as autoridades de fiscalização têm os dados encriptados mantidos ou transmitidos por provedores de hospedagem de dados, operadoras ou outros provedores de serviços?	Acesso com mandado	Acesso com mandado	Acesso com mandado
4. Como a lei trata ofensas extraterritoriais?	Cobertura limitada	Cobertura abrangente	Cobertura abrangente
DIREITOS DE PROPRIEDADE INTELECTUAL			
1. O país é membro do Acordo TRIPS?	✔	✔	✔
2. Existem leis de propriedade intelectual implementando o TRIPS?	✔	✔	✔
3. O país é membro do Tratado de Direitos Autorais da OMPI?	✔	✔	✖
4. Existem leis implementando o Tratado de Direitos Autorais da OMPI?	◑	✔	◑
5. Existem sanções civis aplicáveis por publicação não autorizada na internet de trabalhos protegidos por direitos autorais?	◑	✔	◑
6. Existem sanções criminais aplicáveis por publicação não autorizada na internet de trabalhos protegidos por direitos autorais?	◑	✔	◑
7. Existem leis governando a responsabilidade de ISPs para conteúdo infringindo direitos autorais?	✖	Indeciso	✖
8. Existe base para responsabilizar ISPs por conteúdo infringindo copyright em seus sites ou sistemas?	✖	✔	✖
9. Que sanções estão disponíveis para responsabilização de ISPs por conteúdo infringindo copyright encontrado em seus sites ou sistemas?	Não se aplica	Civis e criminais	Não se aplica
10. ISPs têm obrigação de remover conteúdo infringindo copyright após notificação pelo titular?	◑	✔	✖
11. ISPs são obrigados a informar assinantes ao receber notificações de que o assinante está utilizando os serviços do ISP para distribuir conteúdo que infringe copyright?	✖	✔	✖
12. Existe alguma proteção legal clara contra apropriação indevida de serviços de computação em nuvem? Se sim, conta com fiscalização efetiva?	Proteção limitada (só atividade criminal)	Proteção abrangente	Sem proteção
APOIO À PADRÕES DA INDÚSTRIA & HARMONIA INTERNACIONAL DE REGRAS			
1. Existem leis, regulamentações ou políticas que estabeleçam uma plataforma de definição de padrões para interoperabilidade e portabilidade de dados?	✖	✔	✖
2. Existe uma agência regulatória responsável pelo desenvolvimento de padrões no país?	✔	✔	✔
3. Existem leis de comércio eletrônico em aplicação?	◑	✔	✖
4. Em que instrumentos internacionais são baseadas as leis de comércio eletrônico?	Não se aplica	Modelo UNCITRAL de Lei de Comércio Eletrônico	Não se aplica
5. A obtenção de aplicações ou dados digitais a partir de provedores de serviços de nuvem no exterior é livre de taxas ou outras barreiras de comércio?	✔	✔	✖
6. Padrões internacionais têm prioridade sobre padrões nacionais?	◑	✔	✔
7. O governo participa em processos de definição de padrões internacionais?	✔	✔	✔

Figura 5: Tabela Global de Computação em Nuvem por País

Estes são alguns dos desafios a serem superados, cabendo a cada contratante avaliarem, de acordo com o seu grau de maturidade, o tipo de risco e modelo de serviço que melhor lhe convém aderir.

3 GOVERNANÇA DE PROCESSOS

A governança de processos pode ser vista como uma metodologia capaz de contribuir para uma melhor efetivação da legislação e uma melhor interoperabilidade dos serviços públicos.

São caminhos que apresentam ênfase para a gestão de processos integrada aos requisitos das organizações, a segurança da informação, infraestrutura, virtualização, e interoperabilidade dos serviços públicos.

A governança de processos perpassa todos os caminhos a serem realizados para se estruturar uma organização por processos de negócio, desde a identificação do nível de maturidade até a gestão do dia a dia, com a manutenção dos processos que, de alguma forma, já sofreram intervenção de um projeto de melhoria de processo, onde tais ações são distribuidas em forma de papéis e responsabilidades.

O gerenciamento da organização por meio de processos apresenta-se nos papeis e responsabilidades atribuidas a cada agente organizacional, para que haja certo controle sobre os processos. No entanto, de quem seria o controle dos processos na nuvem? Tal pergunta pode ser tranquila de ser respondida, mas talvez não o seja de ser praticada.

Deste modo, armazenar os dados e informações públicas em provedores fora da ornganização, sendo estes acessados pelos clientes internos e externos, cada vez mais e mais, exige que os serviços disponibilizados estejam bem estruturados e seus procedimentos padronizados de maneira eficientes e eficazes.

O cuidado que se precisa despender neste momento está na padronização em seu nível mais detalhado das informações que conjuntamete estruturam as tarefas que formatam a realização dos processos de negócio. Seria pensar em processos otimizados primeiro para depois se pensar em disponibilizá-los na internet.

Para David Linthicum (2009, p.128), o *Business Process Management* (BPM) e as ferramentas que suportam tal metodologia podem tornar possível a integração entre processos de negócio e tecnologia, potencializando tal noção de processo em nuvem, o que fortalece a ideia de se praticar a otimização dos processos e depois “transportá-los” para a *cloud*. Seria pensar camadas em cima de processos e serviços existentes, conforme a figura 6.

Neste contexto de debate utilizar-se-á do conceito de BPM de Linthicum (2009, p.141):

> BPM é uma agregação de modelagem de negócios e processos, automatização de processos de negócios e fluxo de trabalho. Esta abordagem implementa e gerencia transações e processos em tempo real de negócios que se estendem por várias aplicações, proporcionando uma camada para criar processos comuns que se estendem por muitos processos em sistemas integrados[iv].

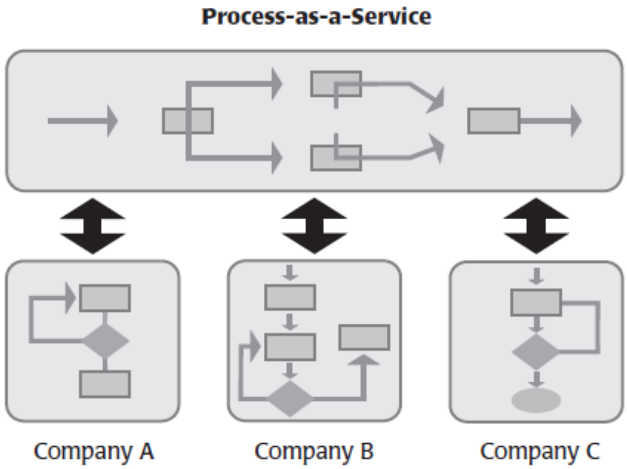


Figure 7.1 Business process management means placing meta-application layers on top of existing processes and services. This figure depicts a process that spans many companies using processes that exist within a cloud-delivered platform.

Figura 6: Gestão de Processos de Negócio[v]

A possibilidade de se usar da metodologia BPM e as linguagens a ela associadas, como por exemplo, *Web Services Business Process Execution Language* (WS-BPEL), torna menos complexo a integração entre processos e tecnologia.

Deste modo, o BPM permite que sua organização vincule serviços, baseados em nuvem, para criar processos centrais de negócios, prestando serviços para vários clientes, conforme figura 7.

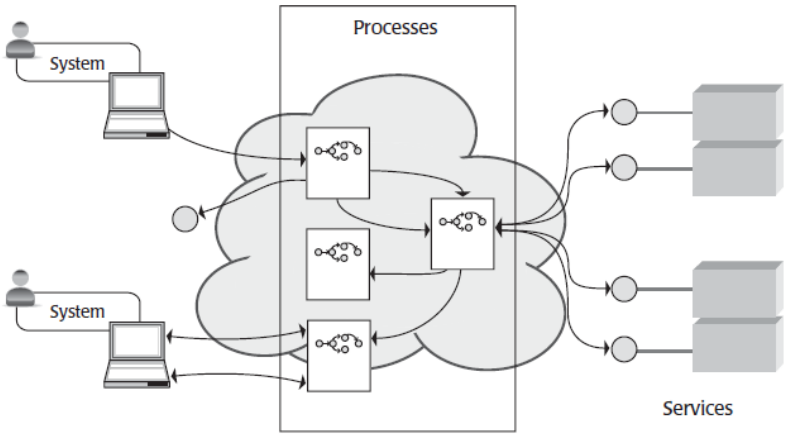


Figure 7.2 BPM allows you to bind services, cloud-based or on-premise, to create core business processes for your business.

Figura 7: Gestão de Processos de Negócio[vi]

Cabe ressaltar que se utilizar dos serviços em nuvem, projetando nessa tecnologia processos não estruturados é um risco que se corre de replicação de erros de procedimentos que podem custar alto para a organização. E, ainda, impactar forte na qualidade do serviço ofertado.

Outro cuidado, atrelado tanto à governança de processos quanto a segurança da informação, diz respeito ao controle que se deve manter sobre os dados e as informações disponibilizadas aos clientes, primeiro devido ao nível de privacidade a que se refere cada informação e, segundo devido à utilização dada a informação disponbilizada.

Deve-se ter cautela com a implementação de *cloud computing* no que tange processos críticos, uma vez que se precisa assegurar a continuidade dos serviços que passam a ir além do *data center*, podendo refletir na qualidade dos serviços públicos prestados a sociedade.

Segundo a Isaca, quando uma empresa decide adotar computação em nuvem para serviços de TI, os seus processos de negócios são impactados e a governança se torna crítica para o gerenciamento efetivo de controle de riscos, bem como para comunicar internamente e para terceiros com clareza os objetivos da companhia (Convergência Digital, 2011).

Assim, o que se percebe é a necessidade de se trabalhar a maturidade interna da organização no que diz respeito a vários pontos críticos, dentre eles a governança de processos, para depois estruturar as informações organizacionais em nuvem.

Faz-se necessário pensar em uma organização com serviços otimizados, pois ter um **catálogo dos serviços de TI** fornecidos a seus clientes exige reflexão do que deve ser migrado para nuvem, avaliando e mitigando os riscos envolvidos em cada um dos serviços a ser transferido, conforme figura 8. E, uma vez estando com os serviços otimizados é preciso monitorá-los na nuvem para que não se corra o risco com processos desatualizados e disponibilizados na nuvem contraditórios ao procedimento padrão de realização.

Geralmente as organizações realizam projetos com preocupação no prazo, no custo e na qualidade. Este tripé se torna a preocupação de todas as entidades, seja pública ou privada.

No entanto, a preocupação perpassa pela priorização do custo em detrimento, por vezes, da qualidade do serviço prestado e por esta razão há necessidade de se ter processos internos e externos bem monitorados, para que os gastos não estejam apenas sendo transferidos de um recurso para outro, pois pode ocorrer de não considerar, por exemplo, o acesso ao *link* de dados (circuito) que tende a ter um aumento do uso da banda e, para se sustentar o custo inicial, perde-se na qualidade da banda e do serviço.

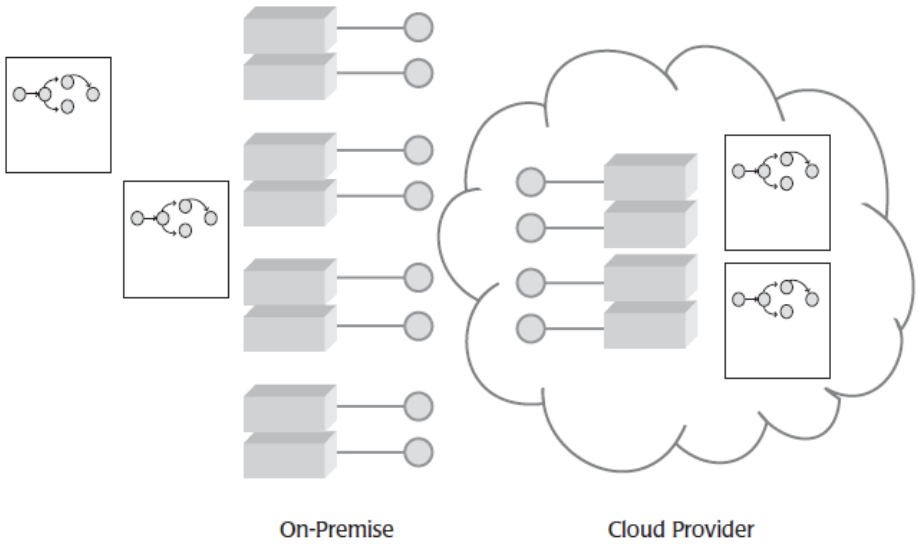


Figure 7.5 The general idea. Processes leverage services for behavior and information, and these processes and services can reside on on-premise and cloud-based systems as needed to support the architecture.

Figura 8: Serviços de Processos[vii]

Para Linthicum (2009, p.138), preocupar-se com o nível de mudança provocado na organização torna-se imprescindível, uma vez que “[...] uma solução de configuração do processo permite que você faça muitas mudanças para os processos de negócio, normalmente sem impulsionar a mudança para os serviços básicos e dados”. Assim, novas configurações lógicas e de infraestrutura mudam o processo, mas podem não mudar a qualidade do serviço prestado ao cliente. A organização modifica a maneira dela de executar, mas não possui ganhos significativos com tal mudança. E, ainda, aumenta seus custos com a mudança realizada.

O importante é que se tenha um mecanismo de controle eficiente e eficaz, independente se a plataforma de serviços encontra-se local ou nuvem. A pretensão é que o nível de controle consiga retornar um conhecimento adequado do que se realiza, tirando o máximo de proveito dos recursos, transformando-os em soluções de negócios.

Assim, a preocupação no momento de implementação da computação em nuvem, no que diz respeito à governança de processos, é saber como os processos serão entregues e não quais processos serão entregues.

4 SEGURANÇA DA INFORMAÇÃO

Em 2009, uma pesquisa global do IDC com executivos de TI sobre quais eram suas preocupações com *Cloud Computing*, apontava que a segurança era a principal preocupação e impedimento para moverem-se em direção à nuvem.

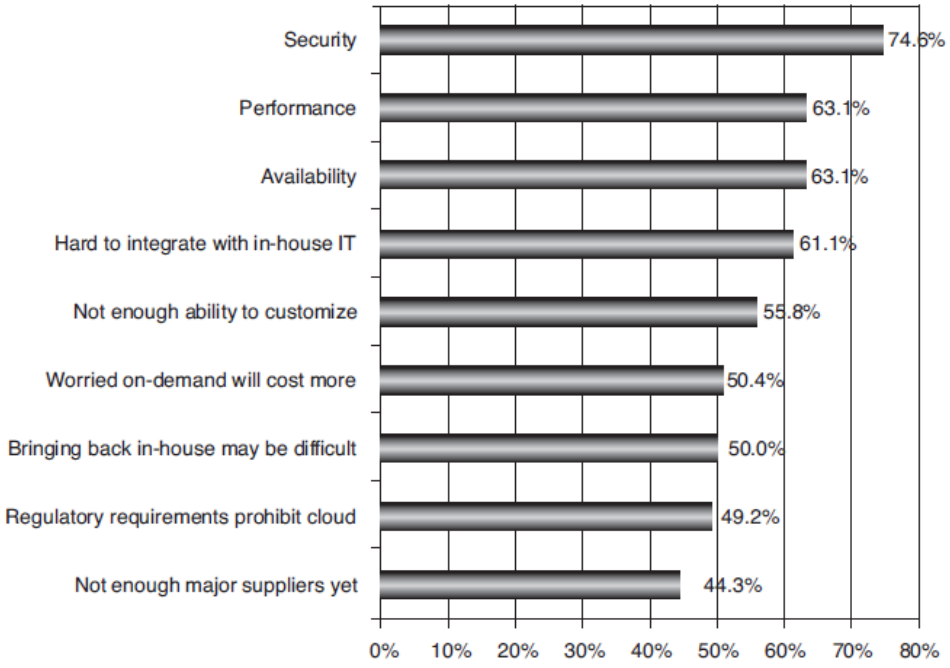


Figura 9: Resultados da pesquisa anual do IDC em 2009, com executivos de TI sobre preocupações com adoção de Cloud Computing para suas aplicações críticas. Segurança continua a ser a principal preocupação durante os últimos três anos[viii]

A Symantec (2011, p. 8) realizou uma pesquisa para avaliar a situação de *Cloud Computing* na América Latina, e seu estudo mostrou a Segurança como o principal objetivo e preocupação das organizações entrevistadas para migração para a nuvem. Dentre as principais ameaças apontadas estão: ataques de massa de *malware* ao provedor de nuvem; roubo de dados por *hackers* no provedor; compartilhamento inseguro de dados confidenciais via nuvem e uso irregular da nuvem, levando à violação de dados.

Num recente estudo da HP Research intitulado “O Futuro da Nuvem é Híbrido”, de alcance global e apresentado em abril de 2012, os respondentes listaram as três principais barreiras para adoção de serviços de nuvem: preocupações com segurança, preocupações com transformações e preocupações com conformidade ou governança, nesta ordem (RUSSELL & COLEMAN, 2012, p. 2).

Estes e outros estudos mostram que a Segurança da Informação e como seus dados serão acessados, manipulados, transmitidos e armazenados ainda é a questão mais preocupante das organizações quando considerando a adoção da computação em nuvem.

Tal fator motivou a criação, em 2009 do **“Guia de Segurança para Áreas Críticas Focado em Computação em Nuvem”** pela *Cloud Security Alliance* (CSA, 2010), uma organização sem fins lucrativos liderada por uma ampla coalizão de profissionais da indústria¸ empresas, associações e outras partes interessadas, com a missão de promover a utilização das melhores práticas para a prestação de garantia de segurança dentro de *Cloud Computing*, e fornecer educação sobre os usos de *Cloud Computing.*

Seu objetivo é ajudar organizações ao redor do mundo na tomada de decisão quanto a e quando elas devem adotar os serviços e a tecnologia de Computação em Nuvem, entendendo melhor quais perguntas fazer, as melhores práticas recomendadas e as armadilhas a serem evitadas. Com foco nas questões centrais da segurança em Computação em Nuvem, busca especificar e contextualizar a discussão sobre o assunto, com recomendações práticas e objetivas para que se faça uma migração mais segura possível.

Em sua versão 2.1, o guia apresenta suas recomendações condensadas em 13 domínios, nos quais busca fornecer os conhecimentos necessários para uma avaliação mais aprofundada dos riscos de segurança a serem avaliados pelas organizações ao considerarem a adoção da Computação em Nuvem.

Neste tópico serão apresentadas algumas destas questões, considerando a perspectiva da administração pública, suas informações e seus processos, destacando-se os fatores críticos que podem impactar negativamente os serviços prestados aos cidadãos e o negócio do poder público como um todo.


4.1 Aspectos legais

Sendo a Computação em Nuvem e suas tecnologias relacionadas consideradas novas em relação à legislação vigente, a ausência de normas regulatórias e específicas que criminalizem ilícitos virtuais torna necessária a utilização de leis existentes para solucionar possíveis implicações jurídicas.

Isto posto é necessário que as contratações de serviços na nuvem pela administração pública estejam baseadas em contratos bem redigidos, que especifiquem de forma clara as responsabilidades de cada um dos atores envolvidos neste processo.

Há que se exigir nestes contratos a garantia dos provedores de nuvem de que seus sistemas de segurança atendem aos requisitos impostos pelo poder público. A segurança oferecida não pode ser inferior àquela que seria obtida pelo contratante caso mantivesse os dados sob sua custódia.

Deve estar previsto ainda um plano para quando do término da relação contratual, com o retorno adequado dos dados ou o seu descarte de forma segura, com garantias principalmente da confidencialidade das informações.

A conformidade com as leis locais é outro fator preocupante, uma vez que os dados na nuvem poderão estar hospedados em outros países, onde as leis existentes podem entrar em conflito com os interesses públicos do governo brasileiro, como o "*Patriot Act*", vigente nos Estados Unidos, ou o *"Data Protection Directive"* da UE, que restringe o fluxo de dados além das fronteiras da comunidade.

Os casos de resposta a possíveis intimações legais também precisam ser previstos, com a definição de um processo que estabeleça as responsabilidades do provedor de nuvem quanto ao cumprimento dessas obrigações.

Além disso, auditorias pré-contratuais, monitoramento pós-contrato e testes de vulnerabilidades no sistema devem ser estar descritos na especificação de requisitos a serem cumpridos pelo provedor de nuvem a ser contratado.


4.2 Portabilidade e interoperabilidade

Quando da contratação de serviços em nuvem, portabilidade e interoperabilidade devem ser consideradas desde o início pelos entes públicos, uma vez que pela própria natureza da Lei 8666/1993 (normas para licitações e contratos da Administração Pública), a necessidade de trocar de provedor pode ser inevitável, não só pelo término do contrato, impreterivelmente com prazo determinado de duração, como por outros fatores que possam vir a afetar os serviços prestados, tais como encerramento das operações do provedor, queda inaceitável na qualidade dos serviços ou incapacidade de cumprimentos dos acordos de níveis de serviço (SLAs) definidos.

A inexistência de padrões de interoperabilidade pode tornar o processo de transição entre provedores problemático, e caso não seja previsto em contrato, de difícil execução. A migração pode ocorrer tanto de um provedor para outro, quanto para o ambiente do contratante, que decida retomar o controle total dos serviços que estavam na nuvem.

Para lidar com estas questões, o tipo de serviço contratado na nuvem irá determinar quais os pontos de atenção a serem considerados, a fim de minimizar os impactos negativos neste processo.

Para todos os tipos de soluções de computação em nuvem, por exemplo, a substituição do provedor pode causar reações inesperadas do antigo provedor, o que deve ser planejado e evitado no processo de contratação. A transferência de grandes massas de dados também pode ser problemática, levando a interrupções do serviço durante a transição.

Para cada uma dos modelos de serviços existentes (SaaS, PaaS e IaaS), outras questões próprias relacionadas a cada modelo deverão ser consideradas, sempre com especificações bem definidas no processo de contratação que forneçam as garantias para um processo de transição o mais transparente e menos traumático possível.


4.3 Resposta a incidentes

Ao contratar serviços de Computação em Nuvem, um ente da administração pública precisa estar ciente das dificuldades que podem existir para as ocorrências de incidentes de segurança, vazamento de informação ou outros eventos que necessitem de investigação e resposta. Os mecanismos de resposta a incidentes usualmente adotados para operações tradicionais de *Data Center* muitas vezes não são eficazes em um ambiente de nuvem, exigindo adaptações para adequação ao cenário oferecido. Este mesmo cenário irá apresentar complexidades que exigirão uma observação detalhada das estratégias utilizadas pelo provedor, para que se possa avaliar se atendem às necessidades do contratante, uma vez que são essas estratégias que definem quais serão os níveis de serviços oferecidos.

A clara definição do que será considerado um incidente, como será o processo de investigação e tratamento deste incidente, quais serão as responsabilidades do provedor de serviços e do cliente, quais serão os canais de comunicação, precisa estar bem especificada nos contratos a serem firmados, com todos os requisitos a serem cumpridos bem estipulados.

Isso pode exigir uma adequação do provedor de nuvem quanto aos seus processos já definidos, levando a um aumento de custo que inevitavelmente será repassado ao contratante. É preciso entender que os grandes provedores oferecem seus serviços a milhares de clientes, e alterações significativas nos processos podem inviabilizar sua oferta de serviços do ponto de vista financeiro. Por outro lado, há que se considerar que ao prestar serviços para milhares de clientes, o provedor tem sob sua responsabilidade o monitoramento de centenas de milhares de eventos, tais como alertas de *firewalls* e sistemas de detecção de intrusos, o que não significa necessariamente um incidente de segurança. Este volume de eventos a serem monitorados, que tende a crescer de forma exponencial, pode ainda levar a tempos de resposta inaceitáveis para determinadas aplicações da administração pública.

Além disso, uma investigação ou mesmo a especificação de ferramentas de detecção e análise de incidentes a serem utilizadas pelo provedor irá garantir compatibilidade com os sistemas do contratante, o que pode ser crucial em investigações que envolvam questões legais.

Outro ponto de atenção refere-se à estratégia de contenção de incidentes, com o controle de danos e a respectiva coleta de evidências, essenciais para investigações posteriores. Exigências legais podem determinar requisitos que não são atendidos quanto à preservação dessas evidências, o que pode comprometer o processo investigatório exigido em uma organização pública. Ainda como alternativa para o tratamento de incidentes, deve ser avaliada a capacidade de remediação do provedor, que significa poder restaurar um sistema a um estado anterior considerado confiável. O provedor de serviços deverá garantir esta capacidade de acordo com as necessidades do cliente, o que pode representar a possibilidade de atendimento de requerimentos legais através do fornecimento de registros forenses.

4.4 Criptografia e Gerenciamento de Chaves

Ainda que a Lei de Acesso à Informação (Lei 12.527/2011), garanta ao cidadão o direito de acesso à informação sob guarda de órgãos e entidades públicas, a mesma lei estabelece ressalvas para aquelas cuja confidencialidade esteja prevista no texto legal, consideradas sigilosas. Assim, existem informações que por sua natureza exigem controles que garantam a sua confidencialidade, tais como informações dados pessoais sob tutela do estado. Desta forma, ao tomar a decisão de adotar serviços na nuvem, um ente da administração pública deve precaver-se contra a perda e o roubo de dados.

Para este propósito, a criptografia e o gerenciamento de chaves apresentam-se como um método eficiente e eficaz, fornecendo a proteção e acesso aos recursos protegidos. É um método não só recomendado, como também exigido por lei e regulamentos em determinados países.

Como forma de implementação, a recomendação é que se adote a criptografia não só para os dados em trânsito, aqueles trafegados entre o cliente e o provedor de nuvem, quanto para aqueles que estejam em repouso no ambiente do provedor, além das mídias de *backup* destes dados. Isto irá proteger os dados contra acessos indevidos de outros locatários dos serviços de nuvem, de provedores maliciosos, perda ou roubo de mídias dentre outros.

Para garantir o acesso aos dados criptografados por usuários legítimos e de direito, é fundamental que um processo de gerenciamento de chaves seja definido, com a criação de repositórios seguros de chaves, o acesso limitado a estes repositórios, e a da adoção de soluções de *backup* e recuperação de chaves. Neste processo o gerenciamento das chaves deve ser segregado do provedor onde os dados são hospedados, fornecendo maior garantia de confidencialidade.

Cabe ressaltar que, para a adoção de criptografia pela administração pública, a estipulação de tal tecnologia nos contratos deve assegurar a aderência a padrões existentes e reconhecidos no mercado, em conformidade com a legislação existente quando for o caso.

O modelo de serviço a ser contratado irá determinar de quem são as responsabilidades para garantir a criptografia de dados sigilosos em trânsito, em repouso e em backup. Para ambientes IaaS, esta responsabilidade é do próprio cliente, para ambientes PaaS tanto do cliente quanto do provedor, e para ambientes SaaS somente do provedor.

5 CONSIDERAÇÕES FINAIS

Neste artigo, buscou-se apontar alguns pontos de atenção para a implementação da tecnologia de computação em nuvem pela administração pública, com o objetivo de se alcançar níveis de maturidade que satisfaçam as necessidades de órgãos e entidades de todos os poderes e esferas.

Devido à amplitude do tema, não se pretendeu esgotá-lo, mas sim oferecer uma referência que sirva como ponto de partida para a discussão e criação de uma política que regulamente a adoção de serviços de computação na nuvem pelos entes públicos da administração pública brasileira de forma segura e sistematizada, e que garanta a qualidade, continuidade e melhoria contínua dos serviços prestados aos cidadãos.

Cada serviço ou ativo disponibilizado na nuvem necessita ser avaliado quanto ao nível de controles de segurança adotado pelo provedor, como disponibilidade, criptografia, requisitos de auditoria, retenção de dados e recuperação de desastres. Devem-se avaliar potenciais pontos de exposição das informações e operações sensíveis ao considerar mover aplicações ou serviços para a nuvem.

Para tanto, torna-se importante conhecer as combinações e os modelos de implantações e serviços disponíveis e em constante evolução. Cada contexto organizacional exigirá uma análise para entendimento aprofundado dele e posterior decisão quanto ao tipo e modelo de computação em nuvem a ser implementado.

O importante é compreender a necessidade de ser conhecer a maturidade da organização quanto à segurança da informação e mapeamento dos processos de negócio, uma vez que ambos impactam na implementação de novas tecnologias.

Deste modo, a construção de uma política de adesão a *Cloud Computing* em organizações públicas, considerando as ponderações aqui realizadas mostra-se pertinente para o desenvolvimento da nova administração pública que se vem estruturando no estado brasileiro.

REFERÊNCIAS

BSA. **Pontuação Global de BSA, Computação em Nuvem da BSA** - Um Guia para Oportunidades Econômicas. Disponível em: < http://portal.bsa.org/cloudscorecard2012/assets/pdfs/GlobalCloudScorecard_pt.pdf > Acesso em: 22 fev. 2012.

COMPUTERWORLD. **Seis dicas para a migração do e-mail para a *cloud***. 01 Abril 2011. Disponível em: <http://www.computerworld.com.pt/2011/04/01/seis-dicas-para-a-migracao-do-e-mail-para-a-cloud/> Acesso em: 20 fev. 2012.

CONVEGÊNCIADIGITAL. **Associação de governança cria guia para controles efetivos em cloud.** 10 ago 2011. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=27213&sid=97> Acesso em: 20 fev. 2012.

CSA (Cloud Security Alliance). **Guia de Segurança para Áreas Críticas Focado em Computação em Nuvem**, 2010. Disponível em: <http://gpupo.com/?tag=seguran%C3%A7a> Acesso em: 20 fev. 2012.

GARTNER. **Gartner Says *Cloud Computing* Will Be As Influential As E-business.** STAMFORD, Conn., 26 Jun., 2008. Disponível em: <http://www.gartner.com/it/page.jsp?id=707508> Acesso em: 20 fev. 2012.

ISACA. **Cloud Computing Benefits and Risks Detailed in New ISACA Guidance.** Rolling Meadows, IL, USA, 29 Out., 2009. Disponível em: <http://www.isaca.org/About-ISACA/Press-room/News-Releases/2009/Pages/Cloud-Computing-Benefits-and-Risks-Detailed-in-New-ISACA-Guidance.aspx> Acesso em: 20 fev. 2012.

LINTHICUM, David. **Cloud computing and SOA convergence in your enterprise**. EUA: Pearson Education, 2009.

NIST (National Institute of Standards and Technology's). **Final Version of NIST Cloud Computing Definition Published.** 25 Out. 2011. Disponível em: <http://www.nist.gov/itl/csd/cloud-102511.cfm> Acesso em: 20 fev. 2012.

VERAS, M., **Virtualização: componente central do datacenter.** Rio de Janeiro: Brasport, 2011.

ROSENBERG, Jothy; MATEOS, Arthur. **The Cloud at Your Service**. Manning, EUA, 2011.

RUSSELL, Lorraine; COLEMAN, Molly. **HP Research: The Future of Cloud Is Hybrid**. Disponível em: <http://www.hp.com/hpinfo/newsroom/press_kits/2012/convergedcloud2012/NA_Research.pdf>. Acesso em: 15 abr. 2012.

SYMANTEC. **Pesquisa sobre Situação de Cloud Computing**: Resultados América Latina. Disponível em: < http://www.symantec.com/content/pt/br/enterprise/images/theme/state-of-cloud/State-of-Cloud-Report-LAM-PORT-FN.pdf>. Acesso em: 22 abr. 2012.

Notas

[i] Disponível em: <http://csrc. nist.gov/groups/SNS/cloud-computing/index.html>

[ii] Disponível em:<http://www.opencrowd.com/assets/images/views/views_cloud-tax-lrg.png>

[iii] Disponível em: <http://portal.bsa.org/cloudscorecard2012/countries.html>

[iv] Tradução do original realizada pelos autores do artigo.

[v] LINTHICUM, 2009, p.129

[vi] LINTHICUM, 2009, p.130

[vii] LINTHICUM, 2009, p.133

[viii] ROSENBERG & MATEOS, 2011, p.74

AUTORIA

Fernando C. G. D. Guerra – Mestrando em Administração Profissional pela Faculdade de Estudos Administrativos de Minas Gerais (FEAD). Especialista em Gestão Estratégica da Informação pela Universidade Federal de Minas Gerais (UFMG). MBA em Gestão de Projetos e Graduado em Administração de Sistema de Informação pelo Centro Universitário UNA (UNA). Atualmente é assessor da Diretoria Central de Gestão de Recursos de TIC da Secretaria Estadual de Planejamento e Gestão de Minas Gerais (SEPLAG/MG).

Endereço eletrônico: war_tj@yahoo.com ou fcgdguerra@gmail.com

Marcelo de Alencar Veloso – MBA em Gestão de Segurança da Informação pela Universidade FUMEC, Bacharel em Sistemas de Informas pela Pontifícia Universidade Católica de Minas Gerais (PUC-Minas). Possui as Certificações MCSA, MCITP, MCTS, MCDST, MCP, ITIL Foundation, ISO 27002 Information Security Foundation. Atualmente é assessor da Diretoria Central de Gestão de Recursos de TIC da Secretaria Estadual de Planejamento e Gestão de Minas Gerais (SEPLAG/MG).

Endereço eletrônico: maveloso@hotmail.com

Rogério Luís Massensini – Mestre em Ciência da Informação e Especialista em Gestão Estratégica da Informação pela Universidade Federal de Minas Gerais (UFMG). Graduado em História pelo Centro Universitário de Belo Horizonte. Atualmente é assessor da Diretoria Central de Política de Otimização de Processos da Secretaria Estadual de Planejamento e Gestão de Minas Gerais (SEPLAG/MG).

Endereço eletrônico: rogeriomassensini@gmail.com