Modelo de avaliação da capacidade das organizações da administração pública federal para a adoção de *software as a service* (SaaS) público

Wellington Galdino Evangelista
Universidade Católica de Brasília (UCB)

João Souza Neto
Universidade Católica de Brasília (UCB)

A adoção de computação em nuvem não é um processo simples, demandando maturidade em gestão e governança de tecnologia da informação. Esta pesquisa objetivou apresentar um modelo de avaliação de capacidade baseado nos critérios que devem ser considerados quando uma organização da administração pública federal decide contratar a modalidade de serviço da computação em nuvem conhecida como *software* como serviço. A metodologia contemplou uma pesquisa bibliográfica sobre computação em nuvem, seguida por uma análise de conteúdo, um grupo focal para avaliação do modelo e, finalmente, uma aplicação em cinco órgãos públicos, que constatou o despreparo para o consumo de *software* como serviço. O desempenho foi insuficiente nos domínios da tecnologia e infraestrutura, razoável em segurança da informação, e apenas suficiente nos domínios da estratégia organizacional e *software*. O modelo proposto pode auxiliar os gestores públicos na detecção de áreas que devem ser melhoradas para mitigação dos riscos.

Palavras-chave: governança de TI, tecnologia da informação, segurança da informação, administração federal, estudo de caso

[Artigo recebido em 17 de fevereiro de 2014. Aprovado em 4 e dezembro de 2015.]

Modelo de evaluación de la capacidad de las organizaciones de la administración pública federal para la adopción de software as a service (SaaS) público

La adopción de la computación en nube no es un proceso simple, sino que requiere madurez en la gestión y la gobernanza de tecnología de la información. Esta investigación tuvo como objetivo presentar un modelo de evaluación de la capacidad en base a los criterios que se deben considerar cuando una organización del gobierno federal decide contratar el modo de servicio de la computación en la nube conocida como el *software* como un servicio. La metodología incluyó una búsqueda bibliográfica en computación en nube, seguido de un análisis de contenido, un grupo de enfoque para evaluar el modelo y, finalmente, una aplicación en cinco agencias públicas, que encontró la falta de preparación para el consumo de *software* como servicio. La actuación fue insuficiente en las áreas de tecnología y infraestructura, razonable en seguridad de la información, y sólo lo suficiente en las áreas de estrategia organizacional y *software*. El modelo propuesto puede ayudar a los responsables en la detección de las áreas que deben ser mejoradas para mitigar los riesgos.

Palabras clave: gobernanza de TI, tecnología de la información, seguridad de la información, administración federal, estudio de caso

Model of evaluation of the capacity of federal public administration organizations for the adoption of public software as a service (SaaS)

The adoption of cloud computing is not a simple process, but requires maturity in information technology management and governance. This research aimed to present a capacity evaluation model based on the criteria that should be considered when an organization of the Brazilian federal government decides to hire the cloud computing service mode known as software as a service. The methodology included a literature search on cloud computing, followed by a content analysis, a focus group to evaluate the model and finally an application in five public agencies, which indicated their lack of capacity for consumption of software as a service. The performance was insufficient in the areas of technology and infrastructure, reasonable in information security, and just enough in the organizational strategy and software areas. The proposed model can help policy makers in the detection of areas that should be improved to mitigate the risks.

Keywords: IT governance, information technology, information security, federal administration, case study

Introdução

A computação em nuvem tem sido vista por especialistas do setor como algo capaz de revolucionar a tecnologia da informação tal como a conhecemos, uma vez que altera sensivelmente o modo como a tecnologia da informação (TI) é provida e consumida, mudando o panorama atual, em que as organizações gerenciam o próprio parque computacional, para outro, em que toda a TI é consumida como serviço (Information Systems Audit and Control Association, 2012; Cloud Security Alliance; Information Systems Audit and Control Association, 2012).

Nesse novo cenário, os serviços de TI são providos e consumidos de maneira similar ao que ocorre com outros recursos que estamos habituados a utilizar, como água, energia elétrica, gás e telefone. Assim, a computação em nuvem possibilita que os usuários finais utilizem os recursos computacionais sem o conhecimento da localização dos servidores ou da forma como esses recursos são entregues e, ainda, permite o pagamento apenas pelos recursos efetivamente consumidos.

Nos últimos anos, a TI tem não apenas apoiado as atividades finalísticas das organizações, como tem funcionado, muitas vezes, como elemento alavancador de novas oportunidades para as organizações. Essa afirmação pode ser facilmente comprovada em diversos ramos de atividade, seja na iniciativa privada, em órgãos públicos ou no terceiro setor. Esse fato é atestado por Grembergen, Haes e Guldentops (2004), quando afirmam que a dependência do negócio em relação à TI se torna ainda mais imperativa na atual economia baseada no conhecimento, em que as organizações estão utilizando a tecnologia na gestão, no desenvolvimento e na comunicação de ativos intangíveis, como a informação e o conhecimento.

O cenário descrito acima é confirmado com a previsão de Weill e Ross (2006) de que a tendência é de crescimento da influência da TI no desempenho empresarial. Os autores afirmam que, num ambiente que exige respostas cada vez mais rápidas e agilidade crescente, as equipes de gerência devem garantir que a TI seja um elemento que viabilize a mudança organizacional, e não um obstáculo.

Isso posto, é importante lembrar que, entre os ativos identificados por Weill e Ross (2006) – humanos, financeiros, físicos, propriedade intelectual, TI e relacionamentos –, a TI é vista como um dos mais difíceis de se gerenciar para agregação de valor para a organização.

Por outro lado, entre as diversas inovações tecnológicas que surgem a todo instante, a computação em nuvem tem um caráter disruptivo com o paradigma de TI tradicional por proporcionar o pagamento efetivo pelo seu uso, sob demanda, entre outras características. Dessa forma, segundo Suleiman *et al.* (2012), esse novo paradigma de TI pode proporcionar a redução de custos e o incremento

da flexibilidade e da agilidade do negócio por meio da utilização de serviços em nuvem. Isso é importante especialmente no momento atual, uma crise financeira internacional, iniciada na última década, que acirrou a concorrência e forçou a redução de custos em diversos segmentos em nome da sobrevivência do negócio.

No entanto, apesar de a computação em nuvem, apoiada por diversas tecnologias, com destaque para a internet, viabilizar o sonho do mercado e de acadêmicos com a operacionalização da computação utilitária com amplo acesso, como qualquer inovação, traz consigo também alguns riscos. Os principais estão relacionados à segurança da informação e à continuidade dos serviços, mas existem outros, como a falta de padrões técnicos que viabilizem a portabilidade entre fornecedores e legislação insuficiente ou inadequada para lidar com os desafios que o paradigma evidencia, conforme relatam a Cloud Security Alliance (CSA) e a Information Systems Audit and Control Association (Isaca) (2012). Como, nesse novo paradigma de computação, os ativos de TI não estão necessariamente sob o domínio da organização que os utiliza, a sua governança torna-se um desafio que precisa ser tratado com atenção especial.

O serviço público brasileiro também pode se beneficiar da computação em nuvem, e ações para que isso aconteça têm sido realizadas em âmbito federal, de maneira que os resultados dessa experiência podem repercutir em diversos segmentos no País (Brasil, 2012).

Por tudo isso, e para lidar com essa nova forma de consumir e contratar TI, a verificação de certos critérios, adequados ao desafio da adoção da computação em nuvem, pode fornecer parâmetros que auxiliem os gestores a traçar uma estratégia para que essa mudança de paradigma de computação aconteça com algum nível de previsibilidade e para que se aumente a probabilidade de sucesso.

Este trabalho pretende identificar quais são os critérios que devem ser considerados no momento em que uma entidade da administração pública federal (APF) decidir adotar a computação em nuvem. Para isso, foi realizada pesquisa bibliográfica para identificar o que tem sido realizado e pesquisado nessa área. Em seguida, foram selecionados os critérios com a ajuda de especialistas em TI com atuação na APF.

Referencial teórico

Computação em nuvem

Segundo Lombardi e Di Pietro (2010), a internet está no centro de uma revolução, em que os recursos são globalmente conectados e podem ser facilmente

compartilhados. Dessa forma, e em consequência dessa facilidade, a computação em nuvem descreve o movimento, iniciado na última década, de comoditização da TI (Subashini; Kavitha, 2011). Para Sharif (2010), se a computação em nuvem for utilizada e adotada de forma correta, poderá unir, identificar e criar novos negócios, setores e indústrias, da mesma forma que ocorreu com a revolução da internet.

Essa revolução guarda muitas similaridades com a forma de computação praticada nas décadas de 1960 e 1970, é o que afirma a Isaca (2011). Esse aspecto é exemplificado com a lembrança de que há 40 anos a computação era centralizada dentro das organizações, em *mainframes* e com a interface com usuários limitada a terminais "burros" e a cartões perfurados. Na sequência, na década de 1980, a adoção de computadores de médio e pequeno porte distribuiu o poder computacional por toda a organização, e, na década seguinte (1990), o padrão computacional dominante foi o cliente-servidor. Atualmente, assistimos novamente à centralização do poder computacional por intermédio de serviços disponibilizados em servidores na internet. No entanto, esse novo padrão centralizado possui grandes diferenças se comparado àquele da época dos *mainframes,* como: o maior poder de processamento atual; a capacidade de armazenamento, que cresceu exponencialmente; a capacidade de atender usuários conectados simultaneamente, que é muito maior atualmente; e, por último, a conectividade, que atualmente pode se dar por meio da internet.

Para este trabalho foi adotada a definição do *National Institute of Standards and Technology* (Nist), apresentada por Mell e Grance (2011), por ser abrangente e por destacar diversos aspectos, deixando evidentes as características principais desse paradigma:

> a computação em Nuvem como um modelo para **acesso conveniente, sob demanda e de qualquer localização**, a uma rede compartilhada de **recursos de computação** (isto é, redes, servidores, armazenamento, aplicativos e serviços) que possam ser prontamente **disponibilizados e liberados com um esforço mínimo de gestão** ou de interação com o provedor de serviços (Mell; Grance, 2011, p. 2 , tradução livre e grifos nossos).

Mell e Grance (2011) ainda afirmam que o paradigma de computação em nuvem é composto por cinco características essenciais, três modelos de serviço e quatro modelos de implantação. Todos esses aspectos serão detalhados em subseções posteriores deste trabalho.

Características essenciais da computação em nuvem

Em meio à evolução dos conceitos e das tecnologias envolvidas, o *Open Cloud Manifesto* (Cloud Computing Group, 2009) declara que mais importante que conhecer as definições é entender o valor das proposições da computação em nuvem. De maneira semelhante, Mell e Grance (2011) definem algumas características essenciais desse modelo:

- **Auto-atendimento sob demanda:** um consumidor pode unilateralmente dispor de capacidades de computação, tais como tempo de processamento em um servidor e armazenamento em rede, conforme necessário, automaticamente, sem a necessidade de interação humana com cada prestador de serviço.
- **Amplo acesso à rede:** recursos são disponibilizados através da rede e acessados por meio de mecanismos-padrão que promovem o uso por plataformas-cliente heterogêneas com qualquer capacidade de processamento (por exemplo, telefones celulares, *tablets*, *notebooks* e estações de trabalho).
- **Agrupamento (*pooling*) de recursos:** os recursos de computação do provedor são agrupados para atender múltiplos consumidores por meio de um modelo multi-inquilino, com diferentes recursos físicos e virtuais atribuídos dinamicamente e realocados de acordo com a demanda do consumidor. O cliente geralmente não tem controle ou conhecimento sobre a localização exata dos recursos disponibilizados, mas pode ser capaz de especificar um local em um nível maior de abstração (por exemplo, estado, país ou centro de dados).
- **Elasticidade rápida:** capacidades podem ser elasticamente provisionadas e liberadas, em alguns casos automaticamente, para se ajustar à escala, crescente ou decrescente, de demanda. Para o consumidor, as capacidades disponíveis para provisionamento frequentemente parecem ser ilimitadas e podem ser apropriadas em qualquer quantidade e a qualquer momento.
- **Medição do serviço:** sistemas em nuvem controlam e otimizam automaticamente o uso dos recursos, aproveitando uma capacidade de medição em algum nível de abstração apropriado para o tipo de serviço (por exemplo, contas de armazenamento, processamento, largura de banda e usuário ativo). O uso de recursos pode ser monitorado, controlado e registrado em relatórios, proporcionando transparência, tanto para o provedor quanto para o consumidor do serviço utilizado.

Essas características essenciais da computação em nuvem são, hoje, "padrão" de mercado, sendo, praticamente, ofertadas por todos os provedores de nuvem de grande porte.

Modelos de serviços

Conforme afirmado anteriormente, a computação em nuvem é classificada em três modelos de serviços. Essa classificação é amplamente utilizada por diversos pesquisadores e também pelo mercado e, segundo a Isaca (2011), cada modelo provê um serviço distinto. Os modelos são:

- **IaaS**

A sigla em inglês significa *Infrastructure as a Service* (IaaS), traduzida para o português como infraestrutura como serviço, que, para o Nist, segundo Mell e Grance (2011), é o modelo de serviço que fornece ao consumidor a capacidade de processamento, rede de dados e outros recursos computacionais fundamentais para se poder implantar e utilizar qualquer tipo de *software*, incluindo sistemas operacionais e aplicativos de negócio. Nesse modelo, o consumidor não pode gerenciar ou controlar a infraestrutura, mas pode controlar os sistemas operacionais e seus aplicativos e, possivelmente, possuirá uma capacidade limitada para gerenciar outros componentes como, por exemplo, o *firewall*.

- **PaaS**

A sigla em inglês significa *Plataform as a Service* (PaaS), traduzida para o português como plataforma como serviço, que, para Mell e Grance (2011), é o modelo de serviço que permite ao consumidor fazer uso das linguagens de programação e ferramentas suportadas pela infraestrutura do provedor. O consumidor não gerencia nem controla a infraestrutura básica, incluindo rede, servidores e sistemas operacionais, mas controla as configurações da plataforma suportada por eles.

- **SaaS**

A sigla em inglês significa *Software as a Service* (SaaS), traduzida para o português como *software* como serviço, que, para Mell e Grance (2011), é o modelo em que é fornecida ao consumidor a capacidade de utilizar os aplicativos disponibilizados pelo provedor em sua própria infraestrutura. Os aplicativos são acessíveis aos consumidores, a partir de diversos dispositivos, por meio de uma interface simples, como um navegador, para acessar um serviço de correio eletrônico, por exemplo. O consumidor não gerencia nem controla a infraestrutura básica, incluindo rede, servidores e sistemas operacionais, nem mesmo as configurações de nenhum aplicativo, tendo a possibilidade de configurar apenas alguns aspectos restritos.

Com esse modelo de serviço surge o termo multi-inquilino, que é o modo de operação de *software* em que diversos consumidores independentes operam em um ambiente compartilhado ao mesmo tempo e com os respectivos dados separados através de partições lógicas (Gartner, 2013; Information Systems Audit and Control Association, 2011). Isaca (2011) destaca que o Facebook, G-Mail™, LinkedIn® e Google Docs são exemplos de aplicativos desse modelo de serviço.

Modelos de implementação

A computação em nuvem também é classificada em modelos de implementação, conforme as definições abaixo:

- **Privada**

Para Mell e Grance (2011), a infraestrutura da nuvem, nesse modelo, é utilizada somente por uma organização. Ela pode ser gerenciada pela organização e pode ser instalada dentro ou fora dos seus limites físicos.

- **Comunitária**

Mell e Grance (2011) ensinam que, nesse modelo, a infraestrutura da nuvem é compartilhada por diversas organizações que possuem os mesmos interesses (por exemplo, missão, requisitos de segurança e políticas). Segundo os mesmos autores, ela pode ser gerenciada pelas organizações, por uma delas ou pelo provedor e pode ser instalada dentro ou fora dos limites físicos dessas organizações.

- **Pública**

Novamente pode se recorrer a Mell e Grance (2011), que explicam que, nesse modelo, a infraestrutura é disponibilizada para o público em geral e pertence a uma organização que vende os serviços da nuvem.

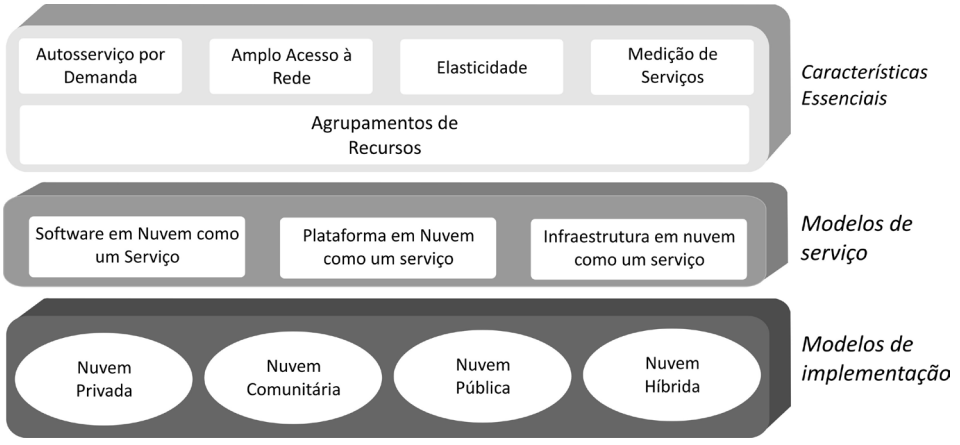
Isaca (2011) afirma que, nesse modelo, os diversos clientes compartilham aplicativos, poder de processamento e espaço de armazenamento de modo concorrente. Acrescenta também que os dados de um consumidor são misturados com os de outros, estando, entretanto, segregados logicamente através de metadados.

- **Híbrida**

De acordo com Mell e Grance (2011), nesse modelo, a infraestrutura é uma composição de duas ou mais nuvens (privada, comunitária ou pública) que continuam sendo únicas, mas estão unidas por tecnologias padronizadas ou proprietárias que permitem a portabilidade de dados e de aplicativos (por exemplo, para o balanceamento de carga entre nuvens).

As características essenciais, os modelos de serviço e os modelos de implementação podem ser visualizados na Figura 1:

Figura 1 – Características essenciais, modelos de serviços e de implementação



Fonte: Madhubala (2012), adaptado pelos autores.

Comparativo entre computação em nuvem e computação tradicional

O modelo de computação em nuvem é diferente, em diversos aspectos, do modelo tradicional de computação. Um dos aspectos mais relevantes diz respeito à capacidade computacional necessária para o atendimento satisfatório das demandas do negócio. Na computação tradicional, usa-se o conceito de escalabilidade que, segundo Gartner (2013), é a medida da capacidade de um sistema de aumentar ou diminuir seu desempenho em resposta a alterações nas exigências de demandas por processamento. Com a escalabilidade, não há preocupação com a remoção física de recursos e nem se os recursos são plenamente utilizados, pois os recursos adquiridos são custos absorvidos. Assim, os recursos são adquiridos para atender aos picos de demanda, ficando subutilizados no restante do tempo.

Por sua vez, para Armbrust *et al*. (2010), a computação em nuvem traz o conceito de elasticidade, que significa a capacidade de adicionar ou de remover recursos para acompanhar a carga de trabalho demandada. Dessa forma, caso ocorra uma repentina diminuição na necessidade de recursos computacionais, a organização poderá se beneficiar caso utilize o modelo de computação em nuvem, pagando pelo uso de tais recursos, o que não aconteceria no modelo tradicional, em que a organização é proprietária dos ativos de TI.

Ainda conforme Armbrust *et al*. (2010), é mais difícil a mensuração do prejuízo para a organização quando a capacidade computacional para atender as demandas do negócio são subestimadas, pois não só o cliente não é atendido no momento de pico de utilização dessa capacidade, deixando de gerar receita, como alguns deles nunca mais procurarão o serviço novamente.

Por meio da elasticidade rápida, característica do modelo de computação em nuvem, os recursos são providos em questão de minutos, enquanto que no modelo tradicional seriam necessárias semanas até que os equipamentos fossem adquiridos e configurados (Armbrust *et al*. 2010). Suleiman *et al*. (2012) explicam que a computação em nuvem pode prover, de forma rápida e eficiente, o volume de recursos necessários e, como resultado, os cenários de subutilização e de superutilização da capacidade computacional são reduzidos consideravelmente.

Outra questão diz respeito ao uso dos equipamentos empregados no parque computacional. A IBM (2013) estima que, com o uso do modelo de computação tradicional, a taxa de utilização dos servidores varia entre 10% e 20%, enquanto que com a computação em nuvem, em que se emprega a virtualização dos servidores, essa taxa é maior, variando entre 70% e 90%. Dessa forma, para o provedor, o custo para manter e atualizar os equipamentos é menor, pois esse é dividido entre diversos consumidores do serviço.

Consoante à diferença a respeito da utilização de equipamentos, de acordo com a Isaca (2011), está o fato de a organização alterar o paradigma dos custos de TI, de CapEx – *capital expenses* – (investimento), na computação tradicional, para OpEx – *operational expenses* – (custeio), na computação em nuvem, o que resulta em um potencial significativo de redução de custos iniciais e totais com TI. Segundo a mesma organização, do ponto de vista do consumidor, essa redução de custos ocorre por meio do compartilhamento (*pool)* de recursos utilizados, uma vez que, em vez de adquirir e utilizar o *hardware* da própria organização, com gastos de capital para adquiri-los e mantê-los, os recursos na computação em nuvem estão disponíveis e são compartilhados por diversas organizações.

Por outro lado, a conexão dos usuários aos serviços de tecnologia é dependente da internet na computação em nuvem, enquanto que, para a computação tradicional, a questão é resolvida com tecnologias de redes locais, conexões dedicadas ou redes privativas virtuais, *Virtual Private Network* (VPN) (Souza Neto, 2012). O uso da internet para a conexão aos dados e serviços institucionais é visto por Suleimain *et al*. (2012) como uma oportunidade para aprimorar o atendimento a volumes de carga de trabalho com grande variabilidade. No entanto, Haimes e Chittister (2012) enxergam a flexibilidade conquistada com o uso da internet como um fator que potencializa, mas que também deixa a computação em nuvem vulnerável.

A localização física dos equipamentos é outra grande diferença entre os dois modelos de computação. Subashini e Kavitha (2011) ensinam que, no modelo tradicional de computação, os dados sensíveis da organização residem em suas próprias fronteiras e, dessa forma, estão sujeitos às suas próprias políticas de controle de acesso e de segurança física e lógica. Por outro lado, os mesmos autores

afirmam que, no modelo de computação em nuvem, os dados da organização estão localizados fora de suas fronteiras, no ambiente do provedor e, dessa forma, é necessário exigir que o provedor adote medidas adequadas para garantir a segurança dos dados.

Desafios para a adoção de computação em nuvem

Apesar dos benefícios citados anteriormente, a computação em nuvem também pode, conforme já afirmado, expor a organização que a adota a alguns riscos, que são inerentes às tecnologias que a suportam e ao novo paradigma propriamente dito.

Como será detalhado mais adiante, diversos desafios para a adoção da computação em nuvem estão relacionados aos aspectos de segurança. Subashini e Kavitha (2011) afirmam que os diferentes modelos de serviços – IaaS, PaaS e SaaS – requerem acordos diferentes, entre provedores e consumidores, para a distribuição de responsabilidades sobre a segurança no ambiente de computação em nuvem, que também são afetados pelos modelos de implantação – privado, comunitário, público e híbrido. Segundo os mesmos autores, as responsabilidades do provedor e do consumidor do serviço sobre a segurança são inversamente proporcionais, isto é, quanto maior a de um, menor será a do outro.

A literatura lista diversos desafios relacionados à adoção de uma solução baseada ou mesmo apoiada pela computação em nuvem, tais como:

- **Localização dos dados**

Independentemente do modelo de implantação selecionado, a Isaca (2011) afirma que os clientes podem desconhecer a localização física dos servidores utilizados para armazenar e processar seus dados e aplicativos. Do ponto de vista da tecnologia, a localização dos dados é irrelevante, no entanto, para certos requisitos de governança de dados, essa é uma questão crítica e, por isso, torna-se importante que o provedor informe sobre a localização dos dados – qual o servidor, o centro de dados e o país.

- **Segregação de dados**

Segundo a Isaca (2011), muitos clientes podem utilizar a mesma aplicação ou o mesmo servidor simultaneamente, o que pode significar que os dados desses clientes serão processados nos mesmos servidores ou armazenados nos mesmos arquivos de dados. Os provedores alegam que cada registro possui um metadado associado, que é utilizado para segregar os dados de cada cliente. A criptografia é outro controle que pode ajudar na confidencialidade dos dados; contudo, os clientes precisam verificar como a chave de criptografia é gerenciada e como o dado é decriptografado. Algumas formas de auditoria também podem ser previstas em contrato para verificar se os dados não estão misturados ou expostos.

Conforme Subashini e Kavitha (2011), a característica da computação em nuvem de prover um ambiente mutilocatário é o que provoca o problema da segregação de dados e o que torna possível tecnicamente que usuários maliciosos roubem ou alterem dados armazenados.

- **Política de segurança para a nuvem**

Armbrust *et al.* (2010) ensinam que são várias as questões que devem ser tratadas pelas políticas de segurança, entre elas, por exemplo, a forma como o provedor de nuvem vai se desfazer de um disco rígido, pois ele pode conter dados de seus clientes e, por isso, precisam ser limpos de forma garantida.

Para a Isaca (2011), alguns provedores podem ser menos transparentes que outros quando se trata da política corrente de segurança da informação, e isso pode ser justificado por essas serem políticas proprietárias. No entanto, essa prática pode provocar conflitos com os requisitos legais de informações dos clientes. Os clientes precisam ter a compreensão apropriada e contratos detalhados com acordos de nível de serviço (ANS) que possam prover o nível desejado de segurança para garantir que seus provedores implementem os controles apropriados.

- **Propriedade dos dados na nuvem**

Alguns contratos podem estabelecer que o provedor é o proprietário dos dados armazenados em seus servidores de computação em nuvem. Além disso, o provedor pode cobrar taxas para os dados retornarem à organização ao término do contrato (Information Systems Audit and Control Association, 2011).

- **Dependência de Application Programming Interface (API) proprietárias do provedor**

Para Armbrust *et al.* (2010), a falta de um padrão técnico para acessar a nuvem não permite que uma organização que possua uma nuvem privada utilize, em momentos de pico de demanda, uma nuvem pública para, por exemplo, executar tarefas extras. Para a Isaca (2011), essa dependência torna a mudança de provedor extremamente difícil, demorada e trabalhosa.

- **Viabilidade organizacional do provedor**

À medida que a computação em nuvem amadurecer, muitos provedores sairão do mercado. Os clientes precisam considerar esse risco, avaliando como seus dados e aplicativos podem ser transferidos de volta ao ambiente tradicional, interno à organização, ou para outro provedor (Information Systems Audit and Control Association, 2011).

- **Proteção dos registros para auditorias forenses**

A Isaca (2011) diz que os clientes precisam considerar a disponibilidade dos dados quando requeridos para auditorias forenses. Como os dados podem estar

misturados aos dados de outros clientes e distribuídos entre diversos servidores ou centros de dados, a recuperação desses dados pode ser difícil em determinado momento. Além disso, as autoridades locais podem apreender um servidor para a análise detalhada dos dados de um cliente suspeito, o que poderia prejudicar os demais.

- **Gerenciamento de acesso e detecção de invasão**

Com a migração de serviços sofisticados para um provedor de computação em nuvem, é exigida a utilização de ferramentas que gerenciem os acessos de forma mais granular, e os provedores de computação em nuvem podem não possuir os controles de privilégios de acesso adequados (Information Systems Audit and Control Association, 2011).

Para Subashini e Kavitha (2011), essa vulnerabilidade pode vir de um dos principais componentes da computação em nuvem: a virtualização. Segundo os autores, uma das principais responsabilidades de um *software* de virtualização é manter as diversas instâncias que rodam na mesma máquina isoladas entre si, no entanto, diversas falhas já foram encontradas nesses *softwares*.

Por fim, a Isaca (2011) diz que se deve considerar se o provedor utiliza um sistema para detecção de invasão que monitore adequadamente toda a atividade realizada no ambiente de computação em nuvem. Também é importante verificar se existe um sistema para fornecer, em tempo real, informações de *logs* de auditoria e registros de incidentes de segurança.

- **Seleção de outros clientes do provedor**

Para a Isaca (2011), por definição, os provedores de nuvem pública podem aumentar sua receita oferecendo seus serviços para diversos clientes. Entretanto, deve-se considerar quais são os outros clientes com quem se compartilham os mesmos servidores – e em caso de SaaS, os mesmos aplicativos e arquivos de dados – e se eles possuem uma reputação compatível com a sua.

- **Requisitos de conformidade**

A Isaca (2011) informa que, para diversos requisitos de conformidade – incluindo diversos relatórios da área financeira –, os serviços de computação em nuvem podem significar um obstáculo para a realização de auditorias já regulamentadas. Localização dos dados, transparência da política de segurança e gerenciamento de acesso são questões que sempre desafiaram os esforços de auditoria.

- **Destruição de dados**

Para a Isaca (2011), no contexto da computação em nuvem, quando dados são transferidos de um servidor para outro, os arquivos de dados podem permanecer intactos no servidor antigo, mas disponíveis para serem sobrescritos. A existência

desses dados pode representar uma falha de confidencialidade, mas, por outro lado, esses dados podem ser úteis em caso de emergência, mesmo assim é necessária a garantia de que esses dados serão destruídos ao término do contrato.

- **Recuperação de desastres**

Subashini e Kavitha (2011) afirmam que o provedor dos serviços precisa garantir que é realizado *backup* de todas as informações sensíveis de seus clientes para facilitar a rápida recuperação em caso de desastre. Os autores também dizem que algum esquema de criptografia pode ser utilizado para proteger essas informações de vazamento.

A Isaca (2011) lembra que, no paradigma tradicional de TI, a organização conhece o local exato em que seus dados estão, para o caso de precisar recuperá-los. O paradigma de computação em nuvem pode alterar sensivelmente esse cenário, pois os dados estão sob o domínio de um provedor que, eventualmente, pode terceirizar parte da capacidade fornecida para outros provedores. Os contratos devem prever detalhes para os testes e tempos de recuperação.

Metodologia

Para a realização da pesquisa, foi estabelecida uma metodologia que contemplou uma pesquisa bibliográfica sobre computação em nuvem, modelos de implantação e as implicações para a sua adoção.

Também foi executada uma análise de conteúdo para correlacionar e comparar os diversos critérios encontrados na literatura. Na análise de conteúdo, foram definidas categorias *a priori* e, em seguida, foram identificadas as suas subcategorias, conforme recomendado por Bardin (2010).

Na terceira etapa da pesquisa, foi realizado um grupo focal com especialistas de TI que atuam em organizações da APF para o aprimoramento do modelo de avaliação para a adoção de SaaS públicos. Após o grupo focal, foi realizada uma análise para se avaliar a concordância dos participantes em relação às questões apresentadas.

Finalmente, o modelo validado pelos especialistas foi aplicado em cinco organizações para a uma avaliação preliminar da situação de alguns órgãos da APF.

Critérios para a adoção de computação em nuvem extraídos da literatura

Dados os diversos desafios que envolvem a migração do paradigma de TI tradicional para o da computação em nuvem, é preciso definir critérios que possam ser avaliados antes e durante o processo de mudança, com a finalidade de preparar a organização de forma adequada para a transição.

Após o estudo de diversas publicações com essa finalidade, é possível extrair critérios que podem indicar o sucesso ou não de uma estratégia de adoção de computação em nuvem. Com a correta avaliação de tais critérios, uma organização pode antecipar a ocorrência de riscos, implementando ações para melhorar seus pontos fracos e para reforçar seus pontos fortes.

A análise desses diversos aspectos encontrados na literatura permitiu uma reflexão sobre o que deve ser feito e, ainda, o que é ou não adequado, considerando a sua utilização na APF.

Nesta seção, serão analisados os critérios presentes na bibliografia estudada: princípios orientadores da Isaca, guia da *Archives and Records Association* (ARA), modelo do governo norte-americano e as diretrizes da Presidência da República para computação em nuvem.

A Isaca (2012) propõe, em seu trabalho, seis princípios para nortear as ações que envolvem a adoção da computação em nuvem. Um guia definitivo com a finalidade de auxiliar a adoção e utilização do novo paradigma seria oportuno. Nesse sentido, Convery (2010), que propôs o Guia para Terceirização de Armazenamento de Informações na Nuvem da *Archives and Records Association* (ARA), cita, em seu trabalho, considerações que julgou relevante realizar.

Kundra (2011), responsável pelo modelo de adoção e utilização de computação em nuvem do governo norte-americano, fala em considerações e em fatores que precisam ser investigados antes e durante a utilização do paradigma de computação em nuvem.

As diretrizes da Presidência da República para o uso da computação em nuvem focam na segurança da informação e de comunicações e demonstram a atenção do governo brasileiro ao tema.

Em comum, todas as publicações estudadas procuram fazer com que as organizações que pretendem se beneficiar das vantagens da computação em nuvem empreendam esforços para mitigar riscos e para que os benefícios do novo paradigma sejam efetivamente conquistados, uma vez que a sua simples adoção não representa nenhum avanço por si só.

Para a consolidação dos critérios, as informações foram organizadas e analisadas de forma qualitativa e interpretativa, por meio da técnica de análise de conteúdo. Tal opção foi escolhida por permitir que os caminhos metodológicos possibilitem o alcance dos objetivos deste estudo.

Critérios presentes na publicação da Isaca

Como princípios, a Isaca (2012) considera que existem algumas premissas que devem se fazer presentes na organização, e não somente na TI. Segundo a

publicação, a presença de tais premissas permite o controle dos riscos inerentes ao paradigma. As premissas encontradas foram:

1. a migração para a computação em nuvem deve fazer parte de uma estratégia da organização;
2. deve-se fazer a avaliação do custo-benefício da mudança de paradigma;
3. deve-se avaliar o risco organizacional;
4. deve-se planejar a integração entre as equipes de TI;
5. deve-se garantir a segurança da informação; e
6. deve-se garantir a eficácia dos aplicativos.

Critérios do Guia ARA

Esse guia trata de diversas questões e enfatiza as questões técnicas da adoção da computação em nuvem, em especial as relacionadas à segurança da informação (Convery, 2010). A seguir, são apresentados os critérios constantes do guia:

1. devem-se classificar as informações que serão migradas;
2. devem-se identificar os riscos de segurança devidos à migração para a nuvem;
3. devem-se desenvolver respostas aos riscos devidos à migração para a nuvem;
4. deve-se garantir a qualidade das informações;
5. deve-se identificar as legislações pertinentes;
6. deve-se fazer o alinhamento do contrato entre o provedor e a organização;
7. deve-se calcular o custo total da migração para a nuvem;
8. deve-se monitorar e auditar o ambiente de computação em nuvem;
9. devem existir procedimentos para a saída do ambiente do provedor;
10. deve existir segurança física adequada no ambiente do provedor;
11. devem existir recursos técnicos adequados e suficientes no provedor; e
12. deve-se gerenciar o acesso adequadamente.

Critérios do modelo norte-americano

Por se tratar de um modelo de adoção de computação em nuvem para um governo que estima despender de 20 bilhões de dólares nos próximos anos para a migração para a nuvem, esse documento apresenta pontos relevantes que consideram o tamanho e a força que um cliente desse porte pode ter em um mercado emergente como o de provedores de computação em nuvem. A seguir, são apresentados os critérios encontrados em Kundra (2011):

1. devem-se identificar os requisitos de segurança;
2. sevem-se classificar os dados quanto ao nível de sigilo;
3. devem-se mapear os aplicativos organizacionais;
4. deve-se ter conhecimento dos provedores de nuvem que atuam no mercado;
5. deve-se adequar a infraestrutura de TI interna ao uso de computação em nuvem;
6. devem-se capacitar os gerentes de TI para o gerenciamento do ambiente em nuvem;
7. deve-se fazer um gerenciamento de mudanças eficiente;
8. devem existir ANS adequados;
9. devem-se utilizar padrões técnicos de mercado;
10. deve-se planejar a obtenção de valor;
11. deve-se preparar a TI para contratar e gerenciar serviços; e
12. deve-se monitorar adequadamente o ambiente.

Critérios da Presidência da República para computação em nuvem

Os critérios presentes na Norma Complementar nº 14 do Departamento de Segurança da Informação e Comunicações, Gabinete de Segurança Institucional da Presidência da República, publicada em 2012, possuem caráter imperativo para os órgãos e entidades da APF. A norma trata exclusivamente de questões ligadas à segurança da informação. A seguir, são apresentados os critérios extraídos da norma:

1. deve-se fazer o alinhamento do normativo da organização às normas e diretrizes de segurança da informação e comunicações;
2. deve-se fazer o alinhamento normativo da organização às diretrizes de gestão de riscos do processo de segurança da informação;
3. deve-se fazer o alinhamento normativo da organização às diretrizes de gestão de continuidade de negócios;
4. deve-se fazer o alinhamento da arquitetura de nuvem ao normativo da organização;
5. devem-se obter garantias legais sobre a propriedade das informações;
6. devem-se obter garantias contratuais sobre as informações;
7. devem-se classificar as informações;
8. deve-se conhecer o valor do ativo de informação;
9. deve-se controlar o acesso; e
10. deve-se conhecer a localização física onde os dados serão hospedados.

Segundo Bardin (2010), o estudo da literatura selecionada permite definir categorias *a priori*, conforme preconiza a análise de conteúdo. Em seguida, é possível identificar as subcategorias, que foram definidas *a posteriori*. Assim, o Quadro 1 apresenta os critérios encontrados e classificados.

Quadro 1 – Classificação dos critérios segundo a categoria

Categoria	Critérios
Estratégia organizacional	Alinhamento às diretrizes de gestão de continuidade de negócios
	Avaliação do risco organizacional
	Garantias legais sobre a propriedade das informações
	Alinhamento às normas de segurança da informação e de comunicações
Avaliação custo-benefício	Cálculo do custo total da migração
	Plano para obtenção de valor
	Conhecimento do valor do ativo de informação
Infraestrutura de TI	Existência de recursos técnicos
	Mapeamento dos aplicativos organizacionais
	Adequação da infraestrutura interna
	Utilização de padrões técnicos
	Alinhamento da arquitetura da nuvem às normas da organização
Segurança da informação	Classificação das informações
	Garantia de qualidade das informações
	Segurança física adequada no provedor
	Gerência de acesso adequada
	Identificação dos riscos de segurança
	Alinhamento às diretrizes de gestão de riscos
	Controle de acesso
	Conhecimento da localização física onde os dados serão hospedados
Contrato e gerenciamento de serviços	Identificação de legislações pertinentes
	Alinhamento do contrato entre provedor e organização
	Conhecimento do mercado
	Capacitação dos gerentes de TI
	Existência de ANS adequados
Operação da nuvem	Integração entre equipes de TI
	Eficácia dos aplicativos
	Desenvolvimento de respostas aos riscos
	Monitoramento e auditoria do ambiente
	Procedimento para encerrar as operações com o provedor
	Gerência de mudanças eficiente

Fonte: Elaboração dos autores.

Modelo para a mensuração da capacidade do órgão de adotar a computação em nuvem

Com base nos estudos e análises realizados na literatura sobre os riscos, as recomendações e os cuidados a serem observados na utilização da computação em nuvem, entende-se que uma avaliação da situação da área de TI de uma determinada organização se faz necessária para que se apontem seus pontos fortes, para que esses sejam assim preservados; e seus pontos fracos, para que sejam fortalecidos antes que o negócio seja colocado em risco com a adoção do novo paradigma.

Dessa forma, a definição de questões relevantes do ponto de vista dos desafios que devem ser enfrentados na migração para a nuvem e do tipo de organização que se pretende investigar torna-se primordial para auxiliar os órgãos da APF na utilização segura da computação em nuvem.

Conforme já descrito, o objetivo deste trabalho é propor critérios relevantes para serem avaliados por órgãos da APF no momento em que estejam avaliando a utilização de serviços SaaS de nuvens públicas. Tais questões foram formuladas a partir dos critérios para adoção da computação em nuvem encontrados na literatura acadêmica, das práticas propostas por provedores de computação em nuvem do mercado e das características próprias dos órgãos da APF, dadas as legislações pertinentes e a avaliação de governança de TI realizada pelo Tribunal de Contas da União (TCU) em 2012.

Proposta

A proposta aqui apresentada busca ser ampla o bastante para abordar a maioria dos desafios encontrados na literatura para a adoção da computação em nuvem, tais como garantia da informação, propriedade dos dados, conformidade a normas, questões legais e contratuais, e segurança da informação. Assim, o questionário elaborado nesta pesquisa pode ser utilizado para a investigação da situação de diversos aspectos relacionados à utilização da computação em nuvem, mas com foco na utilização de um SaaS público.

No entanto, é preciso salientar que a proposta aqui definida não representa um guia definitivo que uma entidade da APF possa seguir para utilizar com sucesso um ambiente de SaaS público. Na presente proposta também não são sugeridas boas práticas para que, ao implementá-las, a organização conquiste uma avaliação satisfatória para um determinado requisito.

A presente proposta deve ser vista como uma referência para que as áreas de TI das entidades da APF possam realizar uma avaliação de seu estado em relação aos aspectos que devem ser considerados para a utilização de serviços SaaS públicos.

Ao mesmo tempo, respondendo às questões, o respondente pode ser acautelado para assuntos relevantes desse tipo de contratação.

As questões formuladas devem ser respondidas no âmbito da TI por gestores com a ajuda de especialistas em áreas específicas, considerando a profundidade do conhecimento exigido em algumas delas sobre aspectos essencialmente técnicos.

Foram criados domínios para agregar questões que tratam de assuntos afins. Com a análise do resultado de cada domínio, é possível reconhecer os pontos fortes e os pontos que precisam ser melhorados para que a área de TI do órgão utilize um SaaS público. Também foram criadas avaliações para medir a probabilidade de o órgão utilizar a computação em nuvem com sucesso. Essas avaliações analisam questões gerais, próprias da organização.

Os domínios do modelo representam uma adaptação das categorias encontradas na análise realizada. São sete domínios que agrupam questões que tratam de um mesmo assunto e que podem auxiliar na tomada de decisão do gestor de TI sobre como agir para preparar a organização sob um determinado aspecto. São eles:

g. Operação – tecnologia: agrega as questões relacionadas à manutenção e monitoramento do ambiente.

h. Operação – organização: trata das questões relacionadas à manutenção de um ambiente propício à utilização da computação em nuvem.

i. Segurança da informação: agrupa as questões que tratam da informação, desde a sua classificação até a segurança propriamente dita.

j. Infraestrutura de TI: domínio que compreende as dúvidas observadas sobre como o ambiente tecnológico deve se comportar para suportar a arquitetura de serviços provida na nuvem.

k. *Software*: desdobramento do domínio de infraestrutura de TI, que mereceu destaque no modelo por esse tratar da avaliação de questões relacionadas a *software* como serviço (SaaS).

l. Contrato e gerenciamento de serviços: esse domínio agrupa as questões essenciais ao relacionamento entre o órgão e o provedor de serviços.

m. Estratégia organizacional: agrupa as questões relacionadas às garantias que as áreas de negócio necessitam.

As questões relacionadas à tecnologia podem ser analisadas a partir de dois prismas: 1) substituição de um serviço já existente, provido internamente, por um serviço provido externamente, no formato de SaaS; 2) contratação de um serviço inexistente na organização, ainda não provido pela área de TI.

Dessa forma, as questões propostas para a avaliação da organização são apresentadas no Quadro 2.

Quadro 2 – Questões relacionadas à organização

Operação	Q.1: A área de tecnologia da informação do órgão possui ANS acordados com as áreas de negócio?
	Q. 2: Foi pesquisado se os principais provedores de nuvem do mercado têm condições de fornecer ao órgão os meios necessários para o monitoramento do desempenho dos serviços contratados?
	Q. 3: Existe, por parte da TI do órgão, a compreensão das mudanças que a utilização de uma nuvem pública impõe à gestão da TI, implicando a necessidade de integração entre as equipes técnicas do órgão e do provedor para que os objetivos de negócio sejam alcançados?
Estratégia Organizacional	Q. 4: Os processos de negócio que serão impactados pela migração ou adoção da computação em nuvem foram identificados?
	Q. 5: A utilização de aplicativos disponibilizados em uma nuvem pública, com todas as características inerentes aos SaaS públicos, não contraria nenhuma legislação aplicável ao órgão ou aos seus negócios?
	Q. 6: A TI do órgão possui a estrutura necessária para a gestão dos serviços contratados junto a um provedor de SaaS público?
Contrato E Gerenciamento De Serviços	Q. 7: Foi realizada a análise de viabilidade da contratação, conforme preconizado pela Instrução Normativa nº 4, editada pela Secretaria de Logística e Tecnologia da Informação (SLTI) do Ministério do Planejamento, Orçamento e Gestão (MPOG)?
	Q. 8: A TI do órgão possui gestão de riscos para que esses sejam identificados antecipadamente, a tempo de serem mitigados ou eliminados para que não comprometam a contratação de serviços SaaS?
	Q. 9: Existe um plano de sustentação para os serviços a serem contratados?
	Q. 10: Existe um processo formal de gestão de contratos que é seguido pela TI do órgão?

Fonte: Elaboração dos autores.

As questões propostas sobre tecnologia são apresentadas no Quadro 3.

Quadro 3 – Questões relacionadas à tecnologia

Operação	Q. 1: Existe plano de contingência para os negócios em caso de interrupção do funcionamento do aplicativo que os apoia e que será fornecido pelo provedor da nuvem?
	Q. 2: A inexistência de um quadro de profissionais da área de TI, com conhecimento técnico e disponibilidade para prover o serviço de maneira adequada é, nesse caso, uma das justificativas para a adoção da computação em nuvem?
	Q. 3: Foi pesquisado se os provedores de nuvem do mercado têm condições de suportar o ANS acordado pela TI com suas áreas de negócio para esse serviço?
Segurança Da Informação	Q. 4: Considerando o nível de privacidade das informações que o serviço utilizará, a rede de dados entre o órgão e o provedor provê os mecanismos adequados (criptografia, entre outros) para a garantia da segurança dessas informações?
	Q. 5: Considerando a confidencialidade dos dados que serão manipulados pelo aplicativo, foram analisadas as legislações pertinentes acerca de sua guarda por terceiro, fora do órgão, inclusive em países estrangeiros, e foi constatado que não há riscos para o negócio?
	Q. 6: Já foi verificada, junto aos principais provedores de serviço de nuvem do mercado, a viabilidade do acesso às informações e ao ambiente do provedor, para fins de auditoria, em atendimento às normas reguladoras?
Infraestrutura De Ti	Q. 7: Em relação à infraestrutura de TI do órgão, foram realizados estudos para verificar se ela está dimensionada para consumir o aplicativo como um serviço, disponibilizado em um centro de dados localizado fora de suas instalações físicas, implicando em maior consumo da rede internet?
	Q. 8: O perfil de utilização do aplicativo apresenta picos de processamento em curtos períodos de tempo ou, ainda, há previsão para que a sua utilização seja incrementada ou diminuída, dificultando, assim, que a TI do órgão disponibilize a capacidade necessária internamente?
Software	Q. 9: A área de negócio necessita acessar o serviço através de diversos meios de acesso, inclusive dispositivos móveis, ou a partir de diversas localizações geográficas, no País ou no Exterior?
	Q. 10: O aplicativo precisará ser integrado com outros aplicativos que funcionam no ambiente interno de TI do órgão? CASO SIM: Q. 10.1: Foi realizado um estudo de viabilidade dessa integração?

Fonte: Elaboração dos autores.

Avaliação de especialistas

O grupo focal realizado nesta pesquisa teve a participação de seis especialistas em TI que atuam na APF, alguns deles em função de liderança e, por isso, acostumados a lidar com contratações de fornecedores de produtos e de serviços de TI.

A reunião foi dividida em duas etapas. Na primeira, a pesquisa foi apresentada, dando destaque aos conceitos que balizariam a discussão e aos objetivos da pesquisa. Na segunda etapa, foram iniciadas as discussões entre os participantes sobre os temas relacionados ao objetivo da pesquisa.

A primeira rodada de discussões girou em torno da pergunta: qual é, no seu entendimento, o requisito obrigatório para uma organização pública migrar para a nuvem?

O participante 1 declarou que, sem a classificação das informações quanto ao nível de privacidade, não é possível nem mesmo decidir se um serviço pode ou não ser provido fora da organização. Porém, o participante também observou que esse requisito na verdade é insumo para que se realize uma análise de risco adequada, sendo, portanto, em sua opinião, a análise de risco o requisito primordial para esse tipo de contratação. Por fim, o participante afirmou perceber uma clara mudança para a TI dos órgãos, que devem, agora, dar uma ênfase maior aos processos de gestão de contratos.

O participante 4 destacou que é primordial que a organização possua processos maduros relacionados à contratação e à gestão de contratos, além de processos eficientes para o monitoramento e respostas a incidentes.

O participante 6 comentou que a elasticidade da computação em nuvem traz impactos à área financeira, aos quais os gestores públicos não estão habituados. Como exemplo disso, o participante relatou a possibilidade de gestores de TI terem de justificar gastos elevados que ocorreram em decorrência de um pico de demanda. O participante 3 contribuiu lembrando que o gestor pode responder também por recursos que foram alocados, mas que não foram utilizados.

Depois, a seguinte pergunta foi pautada para discussão dos participantes: no seu entender, a Instrução Normativa nº 4 da SLTI/MPOG (IN 04) é aplicável a esse tipo de contratação? Ela precisa ser atualizada?

O participante 3 iniciou destacando que a IN 04 pressupõe que seja realizada uma análise de riscos antes da realização da contratação e que essa exigência vai ao encontro das necessidades de uma contratação de computação em nuvem, uma vez que o novo paradigma de computação está sujeito a riscos com os quais as organizações públicas brasileiras não estão habituadas a lidar.

O participante 4 lembrou que a instrução normativa em questão também remete à necessidade de se realizar uma análise de viabilidade da contratação e de se planejar diversas atividades como sustentação, continuidade de serviços e transferência de conhecimento. Todas essas atividades, segundo o participante, são relevantes para que se realize uma contratação de TI com sucesso, mas, muitas vezes, são negligenciadas e, em se tratando de contratos de serviços SaaS públicos, merecem atenção especial.

Na última rodada de discussões, os participantes responderam à seguinte indagação: nuvem pública tem futuro na APF?

O participante 3 demonstrou pessimismo quanto ao uso futuro de computação em nuvem na APF, dada a realidade dos órgãos que conhece, pois eles possuem baixa maturidade em processos importantes para a contratação de SaaS públicos. Entretanto, destacou que a computação em nuvem já é realidade em alguns órgãos que, na ausência de condições de prover internamente alguns serviços às áreas de negócio, contrataram serviços de provedores de SaaS públicos, mesmo não possuindo uma gestão de TI eficiente.

O participante 6 acredita que a adoção do paradigma de computação em nuvem é um caminho natural para a APF. O participante 6 acha, inclusive, que a APF pode e deve buscar os benefícios prometidos pela computação em nuvem, desde que o gestor público tome as medidas necessárias para mitigar seus riscos.

Para o participante 5, a computação em nuvem é viável para a APF; no entanto, teme o risco de dependência das soluções proprietárias dos fornecedores. Isso poderia provocar dificuldades para a transferência de dados ao término do contrato, seja para outro provedor ou para a própria organização contratante, cujo parque tecnológico tende a ficar defasado enquanto o serviço não é provido internamente.

O participante 2 acredita que uma nuvem pública que pertença ao Governo Federal possa ser a solução para riscos de vazamento de informações, entretanto, não acredita que tal infraestrutura consiga o nível de excelência que os grandes fornecedores multinacionais possuem.

Finalizado o grupo focal, os especialistas foram convidados a responder à seguinte afirmativa para cada uma das questões propostas: **Esta questão (Quadros 2 e 3) é relevante para avaliar se uma organização da APF tem condições de utilizar um serviço SaaS de nuvem pública?** As opções de resposta, em escala Likert, variavam de 1 (discordo totalmente) até 5 (concordo totalmente).

Como as respostas foram dadas nessa escala Likert, a pontuação positiva se refere aos pontos 5 (concordo totalmente) e 4 (concordo parcialmente). Por outro lado, a pontuação negativa se refere aos pontos 1 (discordo totalmente) e 2 (discordo parcialmente). A pontuação 3 (neutro) não é computada em nenhum dos casos.

Por meio de uma análise positiva, é possível perceber a concordância ou não dos participantes em relação às questões apresentadas.

Para o cálculo da pontuação positiva foi utilizada a seguinte fórmula:

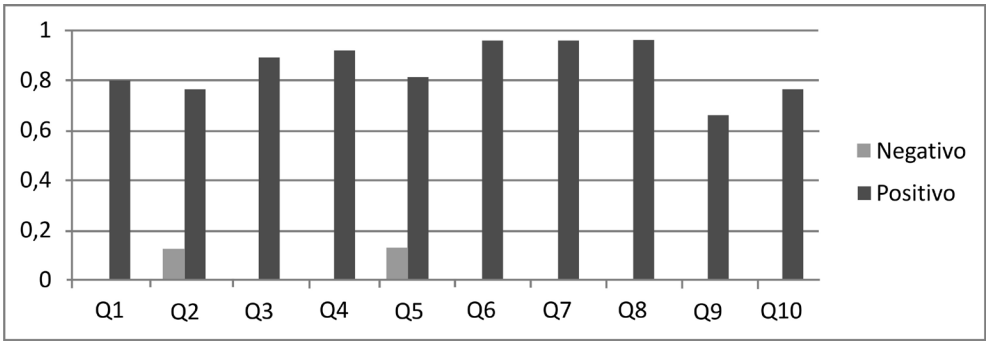
$$Positiva = \frac{(\text{nº de respostas "concordo totalmente"} \times 5) + (\text{nº de respostas "concordo parcialmente"} \times 4}{5\ (quantidade\ de\ organizações\ pesquisadas)})$$

Já para o cálculo da pontuação negativa foi utilizada a seguinte fórmula:

$$Negativa = \frac{(\text{nº derespostas "discordo totalmente"} \times 5) + (\text{nº de respostas "discordo parcialmente"} \times 4)}{5\ (quantidade\ de\ organizações\ pesquisadas)}$$

O Gráfico 1 apresenta o resultado da análise das respostas fornecidas para as questões sobre a organização.

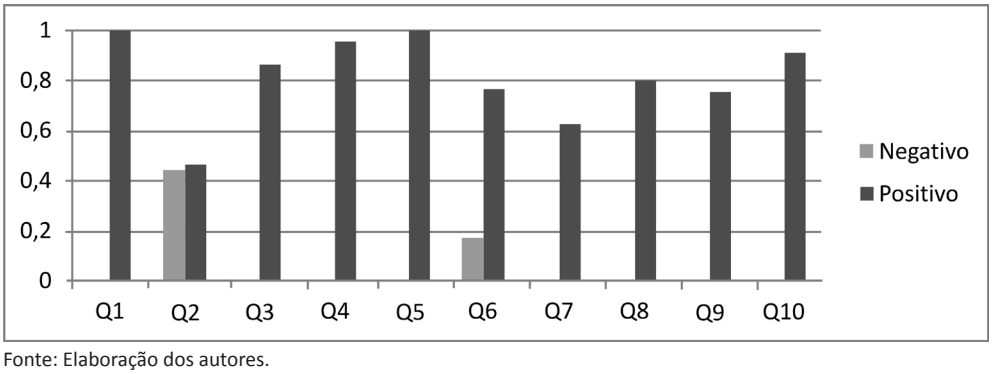
Gráfico 1 – Análise das questões sobre a organização



Fonte: Elaboração dos autores.

O mesmo processo foi repetido para as questões relacionadas à tecnologia. O Gráfico 2 apresenta o resultado da análise das respostas fornecidas sobre essas questões.

Gráfico 2 – Análise das questões sobre tecnologia



Fonte: Elaboração dos autores.

Percebe-se que todas as questões foram aprovadas pelos especialistas, com exceção da Q2 sobre tecnologia (a inexistência de um quadro de profissionais da área de tecnologia da informação, com conhecimento técnico e disponibilidade para prover o serviço de maneira adequada é, nesse caso, uma das justificativas para a adoção da computação em nuvem?). Por esse motivo, essa questão foi excluída do modelo final e as seguintes foram renumeradas.

Aplicação do modelo

Para verificar a aplicabilidade do modelo e demonstrar a sua utilização, o questionário foi aplicado em cinco organizações da APF. Os resultados obtidos representam o percentual de respostas que indicam boas práticas (respostas 5 (concordo totalmente) e respostas 4 (concordo parcialmente) sobre o total de questões para o domínio e sobre a quantidade de organizações pesquisadas), conforme a equação abaixo:

$$Boas\ práticas = 100 \times \frac{\left(\frac{quantidade\ de\ respostas\ satisfatórias}{quantidade\ de\ questões}\right)}{quantidade\ de\ organizações\ pesquisadas}$$

O Quadro 4 apresenta os resultados das organizações.

Quadro 4 – Resultados das organizações por domínio

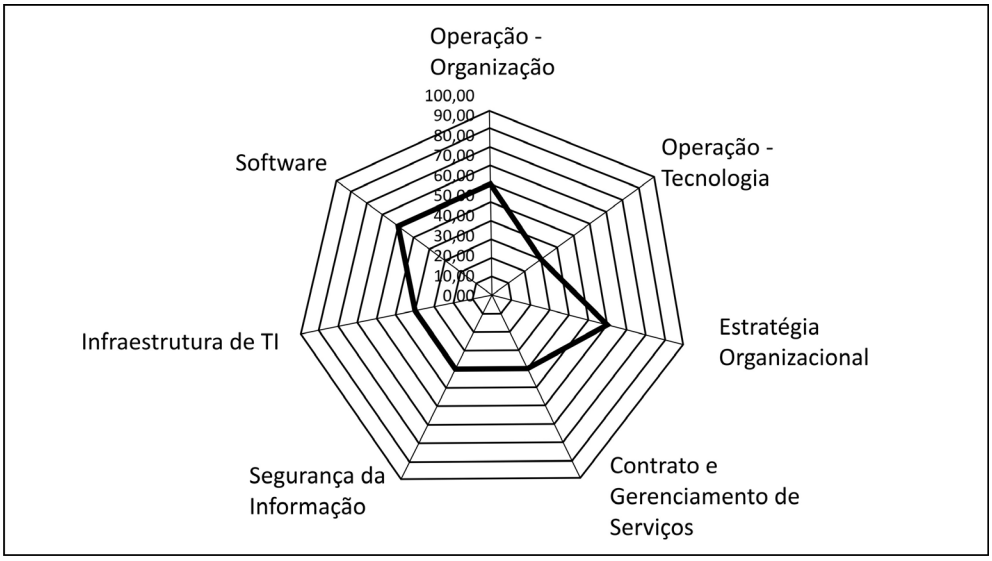
Domínio	Resp. satisfatórias	Total de questões	Valor
Operação – organização	8	3	53,33
Operação – tecnologia	3	2	30,00
Estratégia organizacional	9	3	60,00
Contrato e gerenciamento de serviços	8	4	40,00
Segurança da informação	6	3	40,00
Infraestrutura de TI	4	2	40,00
Software	6	2	60,00

Fonte: Elaboração dos autores.

Como resultado geral, as organizações pesquisadas apresentaram pior desempenho no domínio operação – tecnologia, o que significa que, numa eventual migração para a nuvem, as organizações teriam dificuldades em manter e controlar o uso dos serviços contratados, segundo o modelo. Os melhores resultados foram encontrados nos domínios da estratégia organizacional e *software*. A segurança

da informação, preocupação recorrente de quem contrata serviços na nuvem, apresentou desempenho apenas razoável. A infraestrutura de TI também aparentou não estar compatível com as exigências que enfrentaria com a contratação de serviços externos. O Gráfico 3, no formato de radar, apresenta os resultados obtidos pelas organizações para cada domínio.

Gráfico 3 – Resultados das organizações por domínio



Fonte: Elaboração dos autores.

Conclusão

Este trabalho de pesquisa objetivou propor um modelo para a avaliação da capacidade da área de TI de uma organização da APF de contratar e operar *software* como serviço (SaaS) disponibilizado em um provedor de nuvem pública, obtendo os benefícios esperados.

O modelo proposto teve como base trabalhos encontrados na literatura acadêmica. O texto desses trabalhos foi submetido a uma análise de conteúdo que resultou num conjunto de 20 critérios para o modelo.

No geral, as organizações pesquisadas apresentaram um desempenho mediano, com desempenho insuficiente nos domínios operação – tecnologia e infraestrutura de TI; desempenho razoável em segurança da informação, e desempenho apenas suficiente nos domínios da estratégia organizacional e *software*.

O fato de a computação em nuvem ser assunto incipiente na APF, ao mesmo tempo que motivou a pesquisa, foi um fator que limitou as discussões do grupo

focal, uma vez que nenhum dos presentes tinha experiência na implantação dessa nova forma de se consumir TI em uma organização.

Para uma melhor adequação do modelo, seria necessário que esse fosse validado em diversos estudos de caso. Por sua vez, para que isso ocorresse, seria necessário haver a oportunidade de acompanhar a contratação e operação de serviços SaaS na modalidade pública por entidades da APF. Dessa forma, seria possível validar se os requisitos presentes no modelo proposto condizem com os fatores de sucesso dos serviços. Este trabalho pode servir como insumo de pesquisa para outros trabalhos que versem sobre o mesmo tema: utilização de computação em nuvem em organizações públicas.

O modelo proposto pode ser complementado com as ações necessárias para que uma determinada organização possa galgar melhores resultados na avaliação. Assim, práticas podem ser associadas a níveis de capacidade do modelo.

Referências bibliográficas

Armbrust, M. *et al*. Clearing the clouds away from de true potential and obstacles posed by this computing capability: a view of cloud computing*. Communications of the ACM*, v. 53, n.4, p. 50-58, April 2010.

Bardin, L. *Análise de conteúdo*. Lisboa: Edições 70, 2010.

Brasil. Secretaria de Logística e Tecnologia da Informação. *Instrução normativa SLTI nº 4***,** de 19 de maio de 2008. Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal. Brasília: SLTI/MPOG, 2008.

Brasil. Presidência da República. *Norma Complementar nº 14***,** de 30 de janeiro de 2012. Diretrizes relacionadas à segurança da informação e comunicações para o uso de computação em nuvem nos órgãos e entidades da administração pública federal. Brasília, 2012b. Disponível em: < http://dsic.planalto.gov.br/legislacaodsic/53>. Acesso em: 13 maio. 2013.

Cloud Computing Group. *Open cloud manifesto*. 2009. Manifesto. 2009. Palo Alto, CA: Cloud Computing Group, 2009. Disponível em: http://www.opencloudmanifesto.org/opencloudmanifesto2.htm. Acesso em: 25, abril 2012.

Cloud Security Alliance (CSA); Information Systems Audit and Control Association (Isaca). *Cloud Computing Market Maturity Study Results.* 2012.

Convery, N. *Cloud Computing Toolkit*. Archives & Records Association. Department of Information Studies, Aberystwyth University. August, 2010.

Gartner. *Gartner IT GLossary*. Disponível em: <http://www.gartner.com/it-glossary/>. Acesso em: 18 fev. 2013.

Grembergen, W. V.; Haes, S. W.; Guldentops, E. *Strategies for information technology governance.* Hershey, PA: Idea Group Publ, 2004.

Haimes, Yacov Y.; Chittister, Clyde C.. *Risk to cyberinfrastructure systems served by cloud computing technology as systems*, John Wiley Online Library, Wilmington, n. 3, p.213-224, 09 fev. 2012. Disponível em: <http://olabout.wiley.com>. Acesso em: 12 fev. 2013.

International Business Machines (IBM). *IBM Smart Cloud Enterprise.* 2013. Disponível em: <http://www-935.ibm.com/services/br/pt/cloud-enterprise/tab-benefits.html>. Acesso em: 07 fev. 2013.

Information Systems Audit and Control Association (Isaca). *Guiding principles for cloud computing adoption and use.* February, 2012.

Information Systems Audit and Control Association (Isaca). *IT control objectives for cloud computing*: controls and assurance in the cloud. 2011.

Kundra, V. *Federal cloud computing strategy.* Washington: The White House, 2011.

Lombard, Flavio; Di Pietro, Roberto. Secure virtualization for cloud computing. *Journal of Network and Computer Applications*, p. 1113-1122, June 2010.

Madhubala, R. An illustrative study on cloud computing. *International Journal of Sost Computing and Engineering, v*.1, n. 6, p. 286-290, January 2012.

Mell, P., Grance, T. *The NIST definition of cloud computing.* Gaithersburg: NIST, 2011. Disponível em: http://csrc.nist.gov/publications/PubsSPs.html. Acesso em: 29, abril 2012.

Sharif, Amir M. It's written in the cloud: the hype and promise of cloud computing. *Journal Of Enterprise Information Management*, p. 131-134, 2010

Souza Neto, João. *Governança corporativa de TI na computação em nuvem.* Brasília: Universidade Católica de Brasília, 2012. 51 slides, color.

Subashini, S.; Kavitha, V. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, v. 34, n.4, p. 1-11, January 2011.

Suleiman, Basem *et al*. *On understanding the economics and elasticity challenges of deploying business applications on public cloud infrastructure*. Sydney: **The Brazilian Computer Society,** set. 2012. p. 173-193.

Weill, Peter; Ross, Jeanne. W. *Governança de tecnologia da informação.* São Paulo: M. Books do Brasil Editora Ltda., 2006.

Wellington Galdino Evangelista

Mestre em Gestão do Conhecimento e da Tecnologia da Informação pela Universidade Católica de Brasília (UCB). Contato: wgevangelista@gmail.com

João Souza Neto

Doutor em Engenharia Elétrica pela Universidade de Brasília (UnB) e Professor do Curso de Mestrado em Gestão do Conhecimento e da Tecnologia da Informação pela Universidade Católica de Brasília (UCB). Contato: joaon@ucb.br


RSP