DESMISTIFICANDO A ADOÇÃO DE SERVIÇOS EM NUVEM GOVERNAMENTAL

IBGP
Instituto Brasileiro de
GOVERNANÇA PÚBLICA

DESMISTIFICANDO A ADOÇÃO DE SERVIÇOS EM NUVEM GOVERNAMENTAL

Breno Costa
Geraldo Loureiro
Antônio Ésio Salgado
Carlos Augusto Lins da Silva
Fernanda Haddad
Lorena Brasil Cirilo Passos
Lucio Melre da Silva
Renato Melo
Rodrigo Carvalho

IBGP
Instituto Brasileiro de
GOVERNANÇA PÚBLICA

1ª edição

Brasília/DF
2019

DESMISTIFICANDO A ADOÇÃO DE SERVIÇOS EM NUVEM GOVERNAMENTAL

Publicado pelo **IBGP – Instituto Brasileiro de Governança Pública**

José Geraldo Loureiro Rodrigues
Diretor Presidente

Carlos Augusto da Silva
Diretor Administrativo e Financeiro

Razão Social
Curso Loureiro Ltda.
CNPJ: 18.735.319/0001-20
Inscr. Est.: CF/DF 07.655.102/001-67

Endereço
SCN, Quadra 01, Bloco E, Salas 1909/1910, Ed Central Park,
Asa Norte, Brasília (DF), CEP: 70711-903

Telefone (61) 3037-7600

www.ibgp.net.br

Projeto gráfico e diagramação
Ars Ventura Imagem e Comunicação

Revisão gramatical
Paulo Henrique de Castro

D463 Desmistificando a adoção de serviços em nuvem governamental / Breno Costa, Geraldo Loureiro...[et al.].--Brasília, DF : IBGP, 2019.
208 p.

Texto de vários autores.
ISBN: 958-85-00000-00-0

1. Tecnologia da Informação. 2. Serviços em nuvem computacional. 3. Governança de TI, setor público. 4. Serviços em nuvem computacional. I. Instituto Brasileiro de Governança Pública.

CDU 004

Apoio para impressão aws

Distribuição GRATUITA

SUMÁRIO

PREFÁCIO

A computação em nuvem, embora ainda seja vista por algumas pessoas como o paradigma da nova era (no futuro) em TIC (Tecnologia da Informação e Comunicação), já é uma realidade (no presente) em todos os ramos da sociedade, provocando diariamente modificações estruturais nas ações e nos processos da área de informática dos órgãos e das empresas. A computação em nuvem, ao ser vista como um modelo que possibilita acesso, de modo conveniente e sob demanda, a um conjunto de recursos computacionais configuráveis que podem ser rapidamente adquiridos e liberados com mínimo esforço gerencial, possibilita forte aderência à necessidade da administração pública em garantir qualidade dos serviços prestados aos seus clientes. Atualmente, os negócios precisam de respostas rápidas, com novos serviços e funcionalidades diferentes e a quase obrigatoriedade de que estejam à frente de seu tempo. É necessário desmistificar que a computação em nuvem é um paradigma que trará mudanças radicais para a sua organização, que é insegura e que a melhor maneira de fazer gestão na área de TIC é manter toda a infraestrutura sob o controle integral da instituição.

A ideia essencial da computação em nuvem é permitir a transição da computação tradicional para um novo modelo, no qual os recursos computacionais serão consumidos e disponibilizados como serviço. Essa transformação digital precisa ser vivenciada de fato pelos órgãos da administração pública, pois o governo demanda

sair da visão de ter a computação centrada nos recursos, para uma computação orientada por serviço. Essa mudança de paradigma trará, em especial, a inovação, a agilidade e a eficiência, que são características tão desejadas pelos órgãos governamentais. O cenário econômico atual reforça, por várias razões (cito o compartilhamento dos recursos de TIC, o uso racional do espaço físico alocado, a diminuição do alto custo de energia elétrica, entre outros), que a mudança se faz necessária. O compartilhamento da infraestrutura de TIC permite o uso mais efetivo dos recursos e oferece economia de escala na administração pública – que deve ser uma bandeira dos grandes gestores deste século, em especial, nos órgãos e nas entidades do setor público.

Para que essa transformação ocorra, é necessário que haja uma mudança cultural e que a computação em nuvem seja vista como uma primeira opção de investimento da administração pública, como fizeram os Estados Unidos em 2011. Nesse ponto, convém ressaltar como as principais características da computação em nuvem (cito autoatendimento sob demanda, amplo acesso a serviços de redes, *pool* de recursos, elasticidade, e serviços mensuráveis) interagem em total harmonia com a realidade da administração pública, trazendo diretamente benefícios perseguidos pelos gestores de TIC em todo o governo. Além disso, por um lado, existem as demandas relacionadas ao crescente nível de exigência – o aumento da qualidade do serviço prestado, a modernização, a introdução de novos serviços e a celeridade dos processos de atendimento. E, por outro lado, percebe-se uma forte demanda imposta pelo controle da despesa pública, que acarreta a redução de custos de funcionamento, o aumento da eficiência e a eliminação de processos burocráticos, que devem ser tidos como obrigação. Outro fator valioso que deve guiar a administração pública na adoção desse paradigma é o fato

de que a computação em nuvem não é um modelo rígido e pode ser moldada às características e necessidades de cada órgão.

A questão primordial não é decidir se a sua instituição pública migrará para nuvem computacional ou não, mas sim quando essa instituição migrará e em qual velocidade essa transformação terá dominado a cultura interna dessa instituição. Diante dessa realidade, este livro representa uma ferramenta fundamental para alavancar a cultura de transformação das atividades de TIC em serviços no governo brasileiro. Este livro deve ser visto como um forte aliado para enfrentar os desafios que possam surgir na adoção da computação em nuvem como uma primeira e, em um futuro curto, como a principal opção de investimento na área de TIC pelos órgãos.

Assim, para desmistificar a adoção da computação em nuvem, este livro apresenta no capítulo "Conceitos de Serviços em Nuvem Computacional" os modelos de computação em nuvem, os principais papéis e responsabilidades e as camadas de serviços. Além disso, cita alguns serviços disponibilizados em nuvem. Na linha por continuar sendo um aliado no processo de adoção desse paradigma, o capítulo "Benefícios e Riscos da Adoção de Nuvem Computacional" descreve com conhecimento os grandes benefícios que a computação em nuvem poderá trazer aos órgãos e destaca também os riscos envolvidos nessa transformação. As análises encontradas nesse capítulo são valiosas porque, mesmo que o leitor decida não adotar a computação em nuvem, sua conclusão será pautada em critérios reais e sólidos, que devem levar em consideração o negócio da instituição.

O capítulo "Adoção de Serviços em Nuvem no Governo" descreve, de maneira rica e detalhada, as experiências vividas em outros países com a adoção de nuvem pelo governo. Esse capítulo é fundamental para ratificar que as possíveis angústias vividas por alguns gestores

do governo brasileiro não são de sua exclusividade, ou seja, elas já foram vividas em outras grandes nações, tais como Estados Unidos e Canadá. A diferença é que esses países já ultrapassaram a barreira da dúvida e agora colhem os benefícios das decisões tomadas.

O capítulo "Desmistificando a Adoção de Serviços em Nuvem" continua alinhado ao objetivo deste livro, que é fortalecer as decisões dos gestores e sedimentar a cultura de adoção do paradigma de nuvem no órgão. Para isso, ele trata de questões consideradas inibidoras à decisão de migração para nuvem computacional, tais como a segurança da informação e a elaboração do termo de referência, o que inclui os modelos de comercialização, os níveis de serviço e o padrão de disponibilidade, o uso de provas de conceito e os modelos de contratação, entre outros importantes pontos a serem considerados em um momento de transição para o paradigma de serviço. A proposta é que o leitor termine a leitura desse capítulo esclarecendo as principais dúvidas sobre essa transformação digital.

Em seguida, este livro apresenta no capítulo "Estratégias de Adoção de Nuvem Computacional" importantes pontos para solidificar, tranquilizar e desmistificar a decisão de adoção do ambiente de nuvem computacional no governo brasileiro. O objetivo desse capítulo é fortalecer a ideia de que o entrave para a computação em nuvem não pode ser por atitude dos gestores. A ideia é oferecer um modelo claro de como o processo de adoção pode ser uma transformação sem trauma, vivida de maneira profunda por todo o órgão, cujo pensamento comum deve ser a vontade de fazer a coisa acontecer e a colheita dos frutos – acesso facilitado a novos serviços, aumento de eficiência e agilidade nos serviços prestados, economia de escala, foco no negócio do governo e redução dos custos – deve ser uma vitória de todos. Assim, é esperado que o crescimento e a modernização das organizações públicas resultem como efeito imediato dessa adoção.

A relevância desta obra é ímpar, pois é fato que ninguém sabe afirmar em qual velocidade, verdadeiramente, a computação em nuvem será adotada pelos órgãos. Porém, é fato que o governo brasileiro já iniciou o seu ciclo de migração para este paradigma, e isso é um caminho sem volta. Assim, a decisão de cada gestor da administração pública deve ser na direção de fazer sempre melhor com menos, pois se vive uma situação social contemporânea na qual um ambiente de colaboração e de integração permitirá potencializar as inovações, a melhoria no desempenho interno e a redução de ambiguidade nos processos, reduzindo substancialmente o tempo e os custos operacionais.

O mundo da TIC respira inovação e, por isso, está sempre de olho no futuro. Logo, vem daí a importância deste livro, que analisa, sob a perspectiva do governo, as transformações silenciosas que ocorrerão no futuro e sua consequente mudança na relação entre a administração pública e o seu principal cliente – o cidadão. Não fique de fora desta transformação! Mergulhe neste paradigma e tenha uma excelente leitura deste livro!

Dra. Aletéia Patrícia Favacho de Araújo von Paumgartten

(Professora do Departamento de Computação da UnB – Universidade de Brasília)

INTRODUÇÃO

Você já pensou em quanto pode ser dispendioso construir e reformar um *data center*? Sala segura, resfriamento, geradores, circuitos elétricos, espaço físico. Não apenas construir um *data center* é caro, mas expandi-lo também. Com o crescimento da população e da atuação estatal, e ainda, a partir da evolução das soluções de *hardware* e *software*, é comum aumentarmos a capacidade de processamento, de memória e de armazenamento da nossa infraestrutura local quando a renovamos. À medida que precisamos recontratar cada um desses ativos, o que normalmente ocorre em momentos diferentes, não é incomum adquirirmos uma capacidade maior que a anterior e, eventualmente, com acréscimo do espaço ocupado e mesmo da carga elétrica necessária ao funcionamento da infraestrutura como um todo.

O processo de contratação de infraestrutura toma muito tempo e esforço de sua equipe? Quantos contratos a sua organização fiscaliza simultaneamente? É complexo e arriscado sincronizar as compras. Primeiro, pelo grande volume e, segundo, pelo risco de implementar mais de uma mudança estrutural ao mesmo tempo. Assim, efetuamos uma dezena de compras de razoável monta todos os anos: *storages*, *switches*, robôs e fitoteca de *backup*, *blades* e servidores, sistemas operacionais, solução de virtualização, ativos de segurança, solução de *backup*, servidor de aplicação, banco de dados, servidor de correio eletrônico, equipamentos de

videoconferência, soluções de mensageria, de gestão de serviços de TI, de monitoramento, de análise de dados, para citar algumas.

E quanto às licitações que demoram mais do que o planejado? Que dão errado, seja pela falta de interessados, seja pela judicialização pelos licitantes ou mesmo por algum erro material? Contratar equipamentos, *softwares* ou serviços dá trabalho, demora e traz riscos diversos. Entre dezenas de contratações, algumas darão problema e será preciso revogá-las, repeti-las ou até postergá-las.

Não nos esqueçamos das contratações de apoio técnico, seja de suporte de TI, seja de consultoria para tratar dos problemas mais complexos da operação dos equipamentos e das soluções contratadas. São exemplos as contratações de *service desk*, de operação da infraestrutura e suporte técnico para bancos de dados e sistemas operacionais.

Parte do problema de ter de gerenciar dezenas de contratações foi mitigado com o modelo de serviço gerenciado, em que se contratam os equipamentos e os *softwares* juntamente com a instalação e a operação, tudo fornecido como serviço, medido e pago com base nos resultados, com o uso de indicadores. *Outsourcing* de impressão e serviços gerenciados de segurança são exemplos dessa composição.

Esse é um movimento (terceirização e contratação de serviços gerenciados) que tenta mitigar outro problema: a falta de pessoal, em quantidade e com qualificação adequadas, para operar e gerenciar todos os produtos e serviços de responsabilidade dos departamentos de TI das organizações públicas. Cada vez mais, as ferramentas de Tecnologia da Informação compõem os mais variados processos de negócio das organizações. Adicione a isso uma demanda por tempos de respostas menores, devido à digitalização das interações da sociedade com o Governo. A consequência é uma demanda cada vez maior de atuação das áreas de TI em um cenário em que há estagnação ou diminuição de pessoal, devido a uma provável

reforma da Previdência, somada ao congelamento dos gastos das organizações públicas (Emenda Constitucional Nº 95 – EC 95[1]).

Mas e se fosse possível reduzir a quantidade de processos de contratação e manter a infraestrutura de hardware, software e serviços adequada e atualizada? Contratar serviços gerenciados é uma opção, mas que apenas posterga o problema, já que continuarão as tendências de aumento do uso da TI nos processos de negócio e diminuição da disponibilidade de pessoal.

A Computação em Nuvem pode ser um componente útil. Para algumas organizações, será indispensável. Os grandes provedores de Computação em Nuvem oferecem, como serviço, todos os componentes de infraestrutura citados nos primeiros parágrafos. Assim, ao contratar serviços em Nuvem, pode-se evitar uma dezena de contratações, provisionando, em minutos, ativos de processamento, armazenamento, *backup*, soluções de segurança, entre outros, com pagamento pelo uso.

E se, mesmo provendo para os clientes internos e externos diversas soluções de TI baseadas em software (suíte de escritório, *business intelligence*, gestão de serviços de TI), não tivéssemos que operar a infraestrutura de hardware subjacente, nem gerirmos o sistema operacional, mas houvesse a garantia de que ele estaria sempre atualizado? Assim funciona o modelo de Software como Serviço (SaaS), que permite realocar a equipe responsável pela operação da infraestrutura de hardware e software para áreas mais nobres, relacionadas mais diretamente com o negócio da organização ou com a inovação.

Que valor é agregado à sua organização caso você tenha acesso fácil – sem necessidade de novo processo de contratação e com disponibilidade imediata – a tecnologias e soluções inovadoras? *Machine Learning*, *Deep Learning*, Reconhecimento de Voz, *Text-To-Speech*, Internet das Coisas, Big Data, entre outros, podem ser instanciados ou experimentados com pouco esforço e tempo, diminuindo bastante o

prazo de resposta aos usuários dos serviços da TI ou da organização, quando se compara com a opção tradicional de fazer uma Prova de Conceito (POC, do inglês *Proof of Concept*) com um determinado fornecedor e, posteriormente, contratar por meio de licitação.

Mas se o uso de serviços de Computação em Nuvem pode trazer agilidade no provimento de recursos às organizações, ser um catalisador de inovação – ao permitir acesso fácil a novas tecnologias –, permitir a redução de pessoal necessário à operação da infraestrutura e eventualmente reduzir custos, qual é o sentido de não estar havendo uma corrida das organizações públicas nessa direção? São variados os fatores.

Inicialmente, há uma questão cultural. Nos últimos anos, acostumamo-nos a ter exclusividade e controle sobre os recursos de TI (mesmo quando estes são hospedados fora das nossas dependências físicas). Contratar uma infraestrutura, compartilhada com outros (muitos) consumidores que não conhecemos, parece uma operação arriscada. Além disso, diferentemente de outros países, no Brasil foram poucos os incentivos às organizações públicas para que adotassem Nuvem. Não há uma política nem um plano nacional para o tema, embora haja algumas ações esparsas. Junte-se a essas questões já citadas o receio com a segurança da informação, com a perda de privacidade dos dados.

Circunstancialmente, a citada EC 95[1], publicada em dezembro/2016, fez com que muitas organizações públicas antecipassem gastos como uma forma de garantir um teto maior, uma vez que ele seria (e foi!) congelado por 20 anos, aplicando-se anualmente a inflação do ano anterior. Essas antecipações de compras fizeram com que fossem reabastecidos os estoques de ativos de infraestrutura e trouxeram um complicador ao cenário: como contratar serviços de infraestrutura em Nuvem enquanto existem "em casa" recursos

ociosos? Alguns gestores têm o receio de que sejam questionados pelos órgãos de controle. E como a adoção de Computação em Nuvem é comumente iniciada pela aquisição de infraestrutura, percebemos um cenário de impasse.

Nos próximos capítulos, apresentaremos em mais detalhes as características, os benefícios e os desafios da Computação em Nuvem como forma de provimento de recursos de TI. Serão descritas as experiências de adoção de Computação em Nuvem pelos governos de diversos países. Serão abordados os normativos existentes no Brasil e apreciadas algumas questões acerca da segurança da informação. O livro apresenta, também, um levantamento das principais preocupações relativas à adoção de Computação em Nuvem, relatadas por um grupo seleto de gestores TI da Administração Pública brasileira, e faz uma análise imparcial, com o intuito de desmistificá-las frente aos normativos vigentes e à experiência dos autores. Por fim, é apresentada uma proposta para dar suporte ao início da adoção de Computação em Nuvem nas organizações públicas brasileiras: o Processo Primeira Nuvem.

O Processo Primeira Nuvem descreve um roteiro simplificado de ações que uma organização do Governo brasileiro deve seguir para adotar a Computação em Nuvem – seja ela federal, estadual ou municipal. Tal processo foi concebido a partir da experiência dos autores, gestores de TI que trabalham no âmbito da Administração Pública, e aprimorado com base em conteúdo relevante (artigos acadêmicos, normativos diversos, documentos de consultorias especializadas, casos reais de contratação e operação de Nuvem, entre outros).

Convidamos você a iniciar a leitura das próximas páginas e conhecer um pouco mais desta plataforma, que pode alterar, para melhor, os processos de negócios das organizações públicas.

CONCEITOS DE SERVIÇOS EM NUVEM COMPUTACIONAL

Este capítulo descreve os principais conceitos relacionados à Computação em Nuvem, suas características, sua arquitetura, os atores envolvidos e a nomenclatura. Caso você já tenha familiaridade com o conteúdo, sugerimos que inicie a leitura pelo capítulo seguinte e retorne apenas quando encontrar, nos demais capítulos, termos ou conceitos que ainda não estejam assimilados adequadamente.

Computação em Nuvem ou Nuvem Computacional é um modelo de computação em que todos os recursos (servidores, redes, aplicações e outros elementos relacionados a data centers) são disponibilizados para a TI e para os usuários finais por meio da *internet*, de maneira que a TI compra somente o tipo e a quantidade de serviços computacionais que realmente são consumidos (*International Data Group – IDG*)[2].

Serviços de Computação em Nuvem ou **Serviços em Nuvem** são quaisquer tipos de serviços, produtos e soluções, voltados a negócios ou ao consumidor final, utilizados em tempo real por meio da *internet* (*International Data Corporation – IDC)*[3].

Por outro lado, importa deixar claro que "virtualização" e "Computação em Nuvem" não são sinônimos, apesar de estarem intrinsecamente associados, pois, atualmente, as tecnologias de virtualização são amplamente utilizadas para sustentar qualquer forma de implantação de serviços em Nuvem Computacional.

É fato que a virtualização traz uma ampla flexibilidade, mas essa tecnologia sozinha não provê todas as características definidas para a Computação em Nuvem, como o autoprovisionamento e a rápida elasticidade. Os usuários não podem, apenas com essa tecnologia, criar máquinas virtuais de acordo com suas necessidades, tendo os recursos de TI alocados a qualquer hora e em qualquer volume.

Mas quais seriam as características essenciais que caracterizam um serviço em Nuvem Computacional?

O NIST (*National Institute of Standards and Technology*)[4] definiu as características essenciais do que seriam serviços em Nuvem Computacional:

- **Auto provisionamento sob demanda** ("*on-demand self-service*"): o consumidor pode ter a iniciativa de provisionar recursos na Nuvem e ajustá-los de acordo com as suas necessidades ao decorrer do tempo, de maneira automática, sem a necessidade de interação com cada provedor de serviços.
- **Acesso amplo pela rede** ("*broad network access*"): os recursos da nuvem estão disponíveis em uma rede e acessados por diferentes dispositivos (tais como: estações de trabalho, *tablets* e *smartphones*).
- **Compartilhamento por meio de *pool* de recursos** ("*resource pooling*"): os recursos computacionais do provedor são agrupados para servir a múltiplos consumidores (modelo *multi-tenant*), com recursos físicos e virtuais sendo alocados e realocados dinamicamente, de acordo com a demanda dos seus consumidores. Há uma ideia geral de independência de localização, uma vez que o cliente geralmente não possui controle ou conhecimento sobre a localização exata dos recursos providos. No entanto, é

possível especificar este local em um nível mais alto de abstração (por exemplo: país, estado ou data center). Os serviços são concebidos como um padrão, com a finalidade de atender à demanda de vários consumidores de maneira compartilhada, não sendo focados em necessidades customizadas de um único consumidor.

- **Rápida elasticidade** ("*rapid elasticity*"): os recursos podem ser elasticamente provisionados e liberados e, em alguns casos, de maneira automática, adaptando-se à demanda. Do ponto de vista do consumidor, os recursos disponíveis para provisionamento parecem ser ilimitados, podendo ser alocados a qualquer hora e em qualquer volume.
- **Serviços medidos e precificados por utilização** ("*measured service*"): os serviços de computação em nuvem automaticamente controlam e otimizam a utilização de recursos, por meio de mecanismos de medição utilizados em nível de abstração associado ao tipo de serviço utilizado (por exemplo: armazenamento, processamento, largura de banda e contas de usuário ativas). A utilização dos recursos pode ser monitorada, controlada e reportada, fornecendo transparência tanto para provedores como para consumidores. Portanto, a precificação, se houver, será balizada pelo uso dos serviços.
- **Multilocação** ("*multi-tenancy*"): recursos físicos ou virtuais são alocados de tal forma que vários usuários usam os recursos simultaneamente e seus cálculos e dados são isolados uns dos outros. Normalmente e dentro do contexto de multilocação, o grupo de usuários do serviço de nuvem que forma um contratante pertencerá à mesma organização de cliente do serviço de nuvem. Pode haver casos em que o grupo de usuários do serviço de nuvem envolva usuários de vários

diferentes serviços de nuvem, particularmente no caso de implantações de nuvem pública e de nuvem de comunidade. No entanto, uma determinada organização de clientes do serviço de nuvem pode ter diferentes locações com um único provedor de serviços de nuvem representando diferentes grupos dentro da organização.

Modelos de Computação em Nuvem

Já definimos o que é Nuvem Computacional, Serviços em Nuvem e características essenciais para que um provimento seja considerado um Serviço em Nuvem. Agora, vamos tipificar esses serviços quanto à forma de implantação e quanto à arquitetura dos serviços disponibilizados pela nuvem, sendo, de acordo com a definição do NIST,[5] o que segue:

I. Modelo baseado na forma de implantação
   - **Nuvem pública –** A infraestrutura de nuvem pública está disponível para uso aberto do público em geral e fica nas instalações do provedor. A sua propriedade, o seu gerenciamento e a sua operação podem ser de uma empresa, uma instituição acadêmica, uma organização do governo ou de uma combinação desses.
   - **Nuvem privada –** A infraestrutura de nuvem privada está disponível para uso exclusivo por uma única organização. Sua utilização, seu gerenciamento e sua operação podem ser feitos pela própria organização, por terceiros ou por uma combinação dos dois. Ela pode estar localizada em suas dependências ou fora delas. No entanto, o cliente terá controle sobre sua localização geográfica, o que a faz se tornar atrativa

para dados ou sistemas com restrições de acesso ou que são de missão crítica.

- **Nuvem comunitária –** A infraestrutura de nuvem comunitária está disponível para uso exclusivo de uma comunidade específica formada por organizações que possuem interesses e preocupações em comum (por exemplo: requisitos de segurança e conformidade). Sua utilização, seu gerenciamento e sua operação podem ser feitos por uma ou várias das organizações pertencentes à comunidade, por terceiros ou por uma combinação deles. Ela pode estar localizada nas dependências de uma ou mais dessas organizações ou fora delas.
- **Nuvem híbrida –** A infraestrutura de nuvem é uma composição de duas ou mais infraestruturas de nuvem (privada, comunitária ou pública), interligadas por tecnologias padronizadas ou proprietárias que permitem portabilidade de aplicações e de dados entre as nuvens.

II. Modelo baseado na arquitetura dos serviços disponibilizados pela nuvem

- **Infraestrutura como Serviço (*Infrastructure as a Service* – IaaS) –** Trata-se da disponibilização, pelo provedor de nuvem, de serviços de provisionamento de processamento, armazenamento, comunicação de rede e outros recursos de computação em que o consumidor poderá instalar e executar softwares em geral, incluindo sistemas operacionais e aplicativos. Nesse caso, o consumidor não gerencia nem controla a infraestrutura e os recursos disponibilizados na nuvem, mas detém o controle sobre os sistemas operacionais, o

espaço de armazenamento e os aplicativos instalados, além de controle segmentado de alguns componentes de rede (como *firewalls*).

- **Plataforma como Serviço (*Platform as a Service* – PaaS) –** Trata-se de serviços oferecidos pelo provedor de nuvem que envolvem acesso às linguagens de programação, bibliotecas, serviços e ferramentas de suporte ao desenvolvimento de aplicações, de modo que o cliente consumidor possa implantar, na infraestrutura da nuvem, aplicativos criados ou adquiridos por ele. Nesse caso, o cliente não gerencia a infraestrutura subjacente da nuvem, tais como rede, servidores, sistema operacional, banco de dados ou armazenamento, tendo controle, apenas, das aplicações implantadas e das configurações do ambiente que as hospeda.
- **Software como Serviço (*Software as a Service* – SaaS) –** Trata-se do conjunto de aplicações disponibilizadas pelo provedor de nuvem ao consumidor. As aplicações podem ser acessadas por vários dispositivos clientes, tais como um navegador *web* ou um *software* cliente. O consumidor não gerencia nem controla a infraestrutura da nuvem associada ao serviço, incluindo rede, servidores, sistemas operacionais, armazenamento ou mesmo recursos individuais da aplicação.

Além das definições apresentadas, que conceituam e caracterizam a Computação em Nuvem, há outros termos muito utilizados em documentos e artigos que tratam dessa matéria. Seguem os mais relevantes:

***Workload* –** A tradução literal do inglês é "carga de trabalho", que é uma definição muito genérica. Especificamente no contexto de Nuvem, um *workload* é o serviço que se deseja migrar para a Nuvem. Pode ser uma máquina virtual (VM), um sistema ou mesmo o conjunto completo de ativos que implementam um determinado serviço (servidores, softwares, balanceador de carga, banco de dados, espaço de armazenamento etc.).

***On-premises* –** Significa "no local". Mas o sentido mais específico do termo quer dizer que o ativo não tem características de Computação em Nuvem, mas sim da geração anterior de plataforma de TI. Ou seja, mesmo que a infraestrutura da organização esteja fisicamente fora dela (terceirização do *data center*, por exemplo, como em um *co-location*), ela não tem uma ou mais das características essenciais, citadas anteriormente (autoprovisionamento, acesso amplo pela rede, medição por uso, elasticidade).

Tenant – É o consumidor da Nuvem, do ponto de vista do uso simultâneo dos recursos de nuvem e não da relação de consumo. É muitas vezes traduzido por 'inquilino', que também é uma tradução imprecisa. Sua organização, ao usar serviços em nuvem, será um *tenant* de um determinado provedor. Se a Nuvem for pública, haverá muitos *tenants* se utilizando do conjunto de recursos compartilhados, e isso equilibra a oportunidade de um consumidor ter acesso a um volume alto de recursos de modo fácil e rapidamente, pagando apenas por uso, com o grande investimento feito pelo provedor, diluído pelo pagamento realizado por diversos consumidores. O compartilhamento por vários *tenants*, embora seja essencial na equação, traz os riscos em relação à privacidade e ao atendimento dos níveis de serviço, tornando a gestão do serviço na nuvem mais complexa do que se implementada *on-premises*.

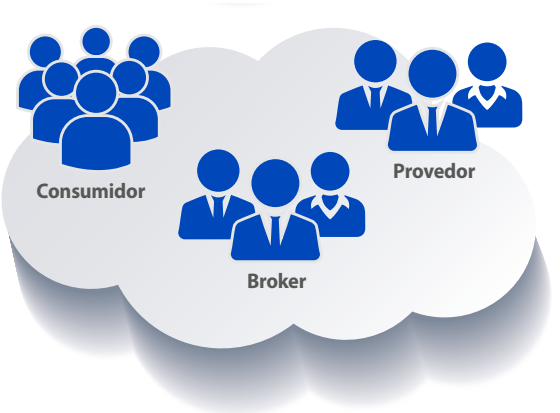
Papéis e Responsabilidades

Depois de termos tratado dos aspectos conceituais relacionados à Nuvem Computacional, vamos descrever os atores envolvidos na preparação, no provimento e no consumo dos serviços em nuvem.

O NIST descreve cinco atores principais, com suas funções e responsabilidades. São eles: Consumidor de Nuvem (*Cloud Consumer*), Provedor de Nuvem (*Cloud Service Provider*), Agente de Nuvem (*Cloud Broker*), Auditor de Nuvem (*Cloud Auditor*) e o Portador de Nuvem (*Cloud Carrier*) [6].

Vamos focar a análise nos três principais papéis: consumidor, provedor e *broker*, como segue.

Figura 1. Papéis e responsabilidades em Nuvem Computacional

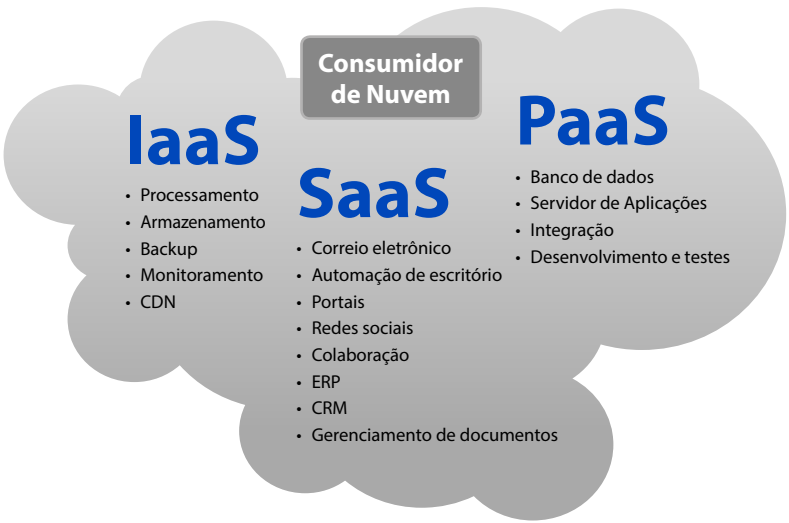


Consumidor de Nuvem (*Cloud Consumer*)

O papel de consumidor corresponde a uma pessoa ou organização que contrata serviços de um provedor de nuvem com o objetivo de fazer uso dos serviços oferecidos nos termos contratuais. Trata-se de um amplo conjunto de atores, considerando a imensa quantidade de serviços disponíveis em Nuvem Computacional.

A figura a seguir caracteriza a variedade de tipos de consumidores conforme a arquitetura de serviços a serem disponibilizados.

Figura 2. Tipos de Consumidores de Serviços em Nuvem[5]



Os consumidores de Software como Serviço (SaaS) envolvem usuários finais de aplicativos de software disponibilizados por organizações que contratam esses tipos de serviços.

Os aplicativos SaaS geralmente são implantados como serviços hospedados e acessados por meio de uma rede conectando consumidores e provedores de SaaS. Tais serviços são cobrados pelo número de licenças de consumidores ou pela quantidade/volume de serviços disponibilizados – neste caso, medidos em termos do tempo em uso, do consumo da largura de banda da rede ou da quantidade/duração dos dados armazenados.

Os consumidores de Plataforma como Serviço (PaaS) utilizam as ferramentas e os recursos de computação fornecidos pelos

provedores de nuvem com o objetivo de projetar, desenvolver, implantar e gerenciar aplicativos hospedados em um sistema de nuvem. Os consumidores de PaaS podem ser cobrados pelo número de licenças disponibilizadas, pelo tipo de recursos consumidos pela plataforma ou pela duração do uso da plataforma.

Os consumidores de Infraestrutura como Serviços (IaaS) utilizam recursos para acessar computadores virtuais, armazenamento acessível pela rede, componentes de infraestrutura de rede computacional e outros recursos fundamentais de computação. Os consumidores de IaaS podem ser desenvolvedores de sistemas, administradores de sistemas e gerentes de tecnologia da informação (TI) interessados em criar, instalar, gerenciar e monitorar serviços para operações de infraestrutura de TI, que, normalmente, são cobrados pela quantidade de recursos consumidos.

Provedor de Nuvem (*Cloud Service Provider*)

O provedor do serviço em nuvem é responsável por instalar, gerenciar, manter e suportar os aplicativos e/ou sistemas disponibilizados na infraestrutura de nuvem, prover e gerenciar a infraestrutura para os consumidores, fazer o gerenciamento do processamento físico, do armazenamento, da rede e de toda a infraestrutura necessária ao fornecimento do serviço. Pode ser uma organização ou entidade, contratada por meio de licitação pública, que é responsável por garantir a qualidade e a celeridade da entrega dos serviços contratados, dentro dos acordos de níveis de serviços acordados, bem como da segurança e privacidade dos serviços.

As atividades dos provedores de nuvem podem ser analisadas a partir das perspectivas de implantação de serviços, da orquestração de serviços, do gerenciamento de serviços em nuvem, da segurança e da privacidade.

Implantação de Serviços – Atividades que envolvem a operação de uma infraestrutura de nuvem em um dos seguintes modelos de nuvem: pública, privada, comunitária ou híbrida.

Orquestração de Serviços – Atividades que envolvem a organização, a coordenação e o gerenciamento da infraestrutura em nuvem para fornecer os recursos de otimização dos serviços, como uma maneira econômica de gerenciar recursos de TI, em conformidade com os requisitos estratégicos de negócios.

Gerenciamento de Serviços em Nuvem – Atividades e funções necessárias para o gerenciamento e a operação dos serviços exigidos ou propostos aos consumidores de nuvem. É descrito de modo a contemplar garantias dentro das perspectivas de suporte ao negócio, provisionamento e configuração e portabilidade e interoperabilidade.

Segurança nos Serviços em Nuvem – Atividades de grande importância e repercussão que envolvem todas as camadas de serviços prestados em nuvem, desde a segurança de acesso físico aos *data centers* dos provedores até a segurança implementada nos aplicativos desenvolvidos pelos consumidores, sendo, em geral, uma responsabilidade compartilhada entre o provedor e o consumidor de nuvem. Enquanto o provedor de serviços em nuvem é responsável pela segurança "da" nuvem, o usuário é responsável pela segurança "na" nuvem.

Privacidade nos Serviços em Nuvem – Atividades que envolvem a coleta, o processamento, a comunicação, o uso e a apresentação segura, adequada e consistente das informações pessoais (*Personal Information* – PI) e informações de identificação pessoal (*Personally Identifiable Information* – PII) no ambiente de

nuvem. PI refere-se às informações de identidade de um indivíduo, como nome, número de identificação civil, registros biométricos etc. PII refere-se às informações que podem ser usadas para distinguir ou rastrear um indivíduo específico, seja de forma isolada ou quando combinada com outras informações de identificação, como data e local de nascimento, nome de solteira da mãe etc.

De forma resumida, a tabela a seguir, elaborada pelo NIST[5], apresenta as atividades a cargo do consumidor e do provedor conforme o modelo de serviço envolvido:

Tabela 1. Consumidor de Nuvem e Provedor de Nuvem

Modelos de serviço	Atividades do consumidor	Atividades de provedor
SaaS	Utiliza aplicativo/ serviço para operações de processos de negócios.	Instala, gerencia, mantém e suporta o aplicativo de software em uma infraestrutura de nuvem.
PaaS	Desenvolve, testa, implementa e gerencia aplicativos hospedados em um sistema em nuvem.	Provê e gerencia infraestrutura e *middleware* em nuvem para os consumidores da plataforma. Fornece ferramentas de desenvolvimento, implantação e administração para os consumidores da plataforma.
IaaS	Cria/instala, gerencia e monitora serviços para operações de infraestrutura de TI.	Provisiona e gerencia o processamento físico, o armazenamento, a rede e o ambiente de hospedagem e a infraestrutura de nuvem para os consumidores de IaaS.

Agente de Nuvem (*Cloud Broker*)

Um *broker* é uma entidade que gerencia o uso, o desempenho e a entrega de serviços de nuvem e negocia relacionamentos entre provedores e consumidores de nuvem. O *broker* posiciona-se entre o consumidor e o provedor de nuvem e pode ajudar o consumidor de nuvem a cumprir suas atividades relacionadas aos serviços de nuvem, bem como diminuir a complexidade de monitorar e gerenciar serviços de um ou mais provedores. Um consumidor de nuvem pode exercer as atividades de *broker* se tiver, em sua equipe, pessoas qualificadas para o relacionamento direto com um ou mais provedores.

Em geral, um *broker* pode fornecer serviços em três categorias, podendo atuar em mais de uma simultaneamente [5]:

Intermediação de serviço – Um agente de nuvem aprimora um determinado serviço, aperfeiçoando alguns recursos específicos e fornecendo serviços de valor agregado para os clientes em nuvem. A melhoria pode ser o gerenciamento de acesso a serviços em nuvem, o gerenciamento de identidades, relatórios de desempenho, segurança aprimorada etc.

Agregação de serviços – Um agente de nuvem combina e integra vários serviços em um ou mais novos serviços. Por exemplo: um *broker* poderia fornecer integração de dados e garantir a movimentação segura de dados entre o consumidor de nuvem e vários provedores de nuvem.

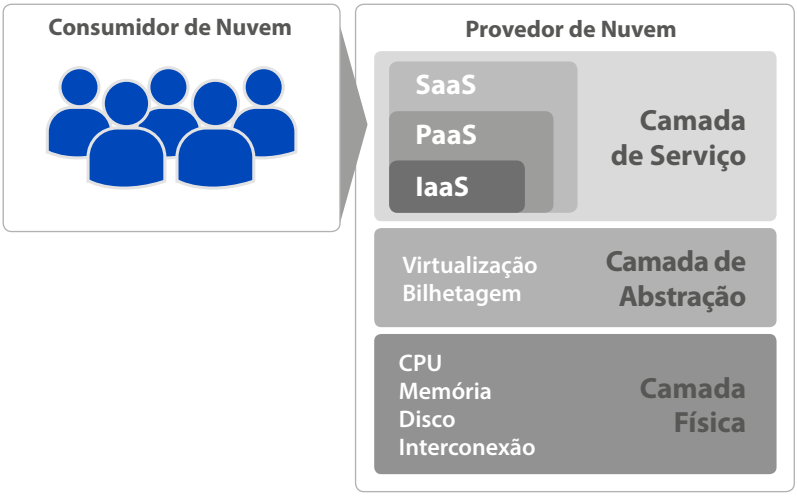
Arbitragem de serviço – A arbitragem de serviço é semelhante à agregação de serviço, exceto que os serviços que estão sendo agregados não são fixos. Arbitragem de serviços significa que um *broker* tem a flexibilidade de escolher serviços de vários provedores. O *broker*, por exemplo, pode usar um serviço de pontuação para medir e selecionar

um provedor com a melhor pontuação (menor latência, menor custo etc.) para determinado serviço solicitado pelo consumidor.

Camadas de Serviços em Nuvem

A figura a seguir, reproduzida do NIST[5], exibe os requisitos gerais e os processos para provedores de nuvem em cada um dos três modelos de arquitetura de serviços. O modelo se apresenta em três camadas: camada de serviço, camada de abstração e controle de recursos e camada de recursos físicos.

Figura 3. Requisitos gerais e processos para provedores de nuvem[5]



Na camada superior, o provedor define e provisiona cada um dos três modelos de serviço. Nesta camada, os consumidores da nuvem consomem os serviços ofertados por meio das interfaces disponibilizadas pelo provedor.

A segunda camada, denominada de abstração e controle de recursos, é utilizada para o provedor fornecer e gerenciar o acesso aos recursos de computação física por meio da abstração de

software. Essa camada normalmente inclui elementos de software, como máquinas virtuais, armazenamento de dados virtuais e outros componentes de abstração e gerenciamento de recursos necessários para garantir o uso eficiente, seguro e confiável.

A camada de recursos físicos inclui todos os recursos de computação física. Possui recursos de hardware, como computadores (CPU e memória), redes (roteadores, *firewalls*, *switches*, *links* de rede e interfaces), componentes de armazenamento (discos rígidos) e outros elementos da infraestrutura tecnológica.

Este modelo foi concebido de modo que os três modelos de arquitetura possam ser construídos um sobre o outro (ou seja, SaaS baseados em PaaS e PaaS baseados em IaaS) ou diretamente na infraestrutura de nuvem subjacente. Tal concepção pode facilitar, para o órgão contratante que ainda apresenta baixa maturidade nesse tipo de serviço, o estabelecimento de metas de curto e médio prazos, permitindo que, num primeiro momento, se contrate determinada arquitetura para, somente após o implemento de maturidade e maior conhecimento do modelo, a contratação de outros modelos.

Lista de Serviços em Nuvem

Para ilustrar as potencialidades dos serviços em nuvem que podem ser adquiridos por organizações do setor público, são detalhados os principais serviços prestados por provedores de serviços de nuvem que atuam no Brasil (relatório *Right Scale Cloud Comparison, março/2019*).[7]

Serviços Básicos

Os Serviços Básicos envolvem a disponibilização de infraestrutura e de plataformas em ambiente de nuvem computacional contemplando serviços como:

Máquinas Virtuais (vCPU) – Todos os provedores disponibilizam máquinas na nuvem com uma ou mais CPUs virtuais. Atualmente, alguns provedores já disponibilizam máquinas com mais de 125 vCPUs.

Memória RAM – Todos os provedores disponibilizam máquinas com possibilidade de escolha da quantidade de memória RAM, algumas vezes superando a casa do 3TB.

Sistema Operacional – A ampla maioria dos sistemas operacionais de servidores é disponibilizada para os consumidores de serviços de nuvem, tais como: *CentOS*, *Ubuntu, Windows*, *CloudLinux*, *Debian*, *OpenSUSE*, *Oracle Linux*, entre outros.

Armazenamento (*Storage*) – Vários serviços relacionados a armazenamento são disponibilizados: *Archive Storage*, *Block Storage*, *File Storage*, *Object Storage* e até o transporte físico de dados em dispositivos móveis (cartuchos, HD externos etc.) para os casos de maior urgência ou de grandes volumes de dados a serem transferidos.

Banco de Dados – Vários tipos de banco de dados são disponibilizados como serviços: Banco de Dados Relacionais (*Microsoft SQL Server, MySQL, Oracle, PostgreSQL, Serverless DB* etc.), Banco de Dados Não Relacionais (*Graph Database, Hadoop, NoSQL*) e outras atividades relacionadas (*Caching, Data Warehouse, Database Migration*).

Serviços de Rede – São serviços que suportam a rede em ambiente de nuvem computacional (*Direct connection, DNS, Load Balancing, Virtual private cloud network, VPN Gateway* etc.).

Certificações – Os principais provedores disponibilizam ambientes de nuvem com as principais certificações relacionadas (*CSA,*

FedRAMP, FISMA, HIPAA, IRAP, ISO 27001, ISO 27017, ISO 27018, MPAA, PCI DSS, SSAE16 SOC1, SSAE16 SOC2, SSAE16 SOC3, EU Model Clauses).

Serviços Adicionais

Mais do que serviços, são tecnologias disponibilizadas pelos provedores de nuvem, que permitem um salto de qualidade e ganhos efetivos de produtividade, posto que tais serviços já foram testados e utilizados por outros clientes do provedor.

Análise de Dados – Vários serviços de *Data Analytics* já estão implementados e prontos para serem utilizados pelos consumidores de nuvem (*Batch data pipelines, Search, Stream processing, AI and Machine Learning, Chatbot, Image Analysis, Machine learning, Speech-to-Text, Text Analysis, Text-to-Speech, Translation*).

Aplicações – Também várias aplicações são disponibilizadas igualmente pela maioria dos provedores, ampliando as capacidades dos consumidores de nuvem (*Email Sending, IoT, Push Notifications, Queueing, Scheduler, Serverless Compute, Transcoding/encoding, Workflow, API Management, Container as a Service*).

Segurança e Identidade – Vários serviços de segurança já estão disponíveis para uso no ambiente dos provedores de nuvem (*AD as a Service, Certificate Management, Dedicated HSM, IAM, Key Storage & Management, Security Assessment, Threat Detection & Monitoring, Web Firewall*).

Embora cada um dos serviços citados possa ser (e eles são!) contratado independentemente dos outros e possa, assim, suprir uma demanda específica da organização, é interessante entender as ofertas de serviços básicos e adicionais na Nuvem como um

conjunto de blocos de montar, em que a composição dos serviços é facilitada e gera novos serviços agregados. O trabalho de montar os blocos pode ser da organização ou pode ser contratado de um *Cloud Broker* ou de fornecedores especializados. Alguns exemplos são:

Backup e recuperação – Rotinas de backup e recuperação são facilitadas em ambiente de Nuvem, devido às altas velocidades de comunicação interna na Nuvem, à facilidade de se fazerem cópias e às funções de automação disponíveis. A nuvem pode ser utilizada também apenas como forma adicional de armazenamento. Há várias soluções de mercado que já se utilizam da nuvem (montaram os blocos) e oferecem interfaces simples e conectores para diversas soluções legadas.

Desenvolvimento e testes – Uma aplicação interessante para organizações que estão iniciando o uso da Nuvem é a criação de ambientes de desenvolvimentos e testes de sistemas. Uma vez criados e configurados, são facilmente replicados. Portanto, dão autonomia às equipes de desenvolvimento para que iniciem vários ambientes simultaneamente, quando necessário, com pagamento apenas pelo uso.

Jogos – Assim como ocorreu com o *streaming* de vídeo (*Netflix*, *Amazon Prime* etc.) e com o *streaming* de áudio (*Spotify*, *Deezer* etc.), o *streaming* de jogos começa a ser uma realidade habilitada pela Computação em Nuvem. O poder computacional da Nuvem é utilizado para processar interações complexas entre os usuários com imagens cada vez mais reais, que podem ser enviadas para dispositivos com baixo poder de processamento (celulares, *tablets*, *desktops*), desobrigando o usuário de adquirir um console de jogos sem perder a qualidade do conteúdo.

Entrega de conteúdo – Muitos provedores de nuvem e vários fornecedores independentes que desenvolveram serviços específicos

baseados na Nuvem oferecem soluções para a mudança de formato de vídeo, adaptação do conteúdo à tela do dispositivo de acesso e *cache* do conteúdo em pontos da rede mais próximos aos usuários. Essas funcionalidades reunidas criam uma melhor experiência do usuário no consumo de vídeos e outros conteúdos de mídia, diminuindo a complexidade da organização que é responsável pela geração e pela distribuição do conteúdo. Por exemplo: vídeos das sessões públicas de tribunais judiciários, treinamentos, entre outros.

Além dos exemplos citados, há um sem-número de soluções disponíveis, criadas por fornecedores independentes. Vários provedores oferecem um catálogo destas soluções por meio de um *marketplace*, uma loja virtual que vende pacotes especializados e que normalmente são fáceis de configurar (ou não precisam de configuração alguma). Os pacotes são compostos de serviços básicos e adicionais do provedor, com alguma agregação de valor oferecida pelo fornecedor independente. Por exemplo, é possível se contratar no *marketplace* da AWS o *SAP Business Objects* 4.2 para 40 usuários concorrentes, que executará em um servidor com 16 CPUs virtuais e 64 GB de RAM, com *Windows Server 2012*. Ao clicar no botão de "assinar" o serviço, o servidor é criado e iniciado e o usuário poderá se utilizar dele imediatamente, sem a necessidade de novo processo de compra e pagando por hora de uso (incluindo as licenças de *software*) e com direito, neste caso, à abertura de até 10 incidentes de suporte por mês e a até 4 horas de suporte em configurações. O pagamento do uso deste pacote virá na fatura mensal do provedor, juntamente com os demais serviços consumidos no período.

O Apêndice B reproduz uma lista, não exaustiva, de serviços de nuvem disponíveis para um consumidor, segundo a visão do NIST.

BENEFÍCIOS E RISCOS DA ADOÇÃO DE NUVEM COMPUTACIONAL

São inegáveis os benefícios para adoção de Nuvem Computacional nas organizações, porém há de se sopesar o nível de riscos aceitáveis na migração de plataforma. A vantagem é que a decisão não precisa ser "tudo ou nada", pois é possível (e recomendável) a migração paulatina de infraestrutura, sistemas e aplicativos.

A migração seletiva faz com que seja aproveitado o máximo de benefícios do ambiente de Nuvem Computacional com o mínimo de riscos.

Benefícios na Adoção de Computação em Nuvem

Vejamos, então, os relevantes benefícios apontados por organizações nacionais e internacionais na utilização do ambiente de computação em nuvem.

- **Aumento da produtividade da equipe de TI** – Para o IDC[9], o uso de IaaS (Infraestrutura como Serviço) acelera o desenvolvimento de aplicações e otimiza o seu gerenciamento, reduzindo a necessidade de alocação de equipamentos servidores no processo. Assim, considerando-se que 50% das organizações públicas federais brasileiras estão em patamares iniciais de práticas de governança de TI, segundo o TCU[8], o aumento da produtividade da equipe de TI se torna um importante aliado para as organizações públicas de baixa maturidade.

- **Melhoria da experiência do cidadão** – Segundo o IDC[9], os usuários finais se beneficiam pela menor indisponibilidade do serviço, reduzindo o tempo de inatividade em 72%. Fato de alta relevância para organizações públicas, muitas vezes com baixa capacidade de manter atualizada a sua infraestrutura de TI.
- **Acesso a recursos avançados e redução dos ciclos de inovação** – Segundo o CSCC[10] e a ISACA[11], há disponível, no mercado de serviços de nuvem, um conjunto de soluções de prateleira (*off-the-shelf*), como: inteligência artificial, *blockchain, data mining* etc., que possibilitam uma ampla inovação com um mínimo investimento em pesquisa ou submissão a processos burocráticos de contratação dessas tecnologias inovadoras (segundo o TCU,[8] 56% de toda a administração pública federal possui práticas incipientes de governança de contratações).
- **Flexibilidade na disponibilização de serviços conforme picos de demanda** – Para a ISACA[12], os serviços em nuvem computacional possibilitam o pagamento por consumo, permitindo que as organizações adequem rapidamente sua oferta de serviços em picos de demanda e reduzam suas despesas com infraestrutura nos períodos de baixa demanda.
- **Benefício para organizações públicas de pequeno porte –** A adoção de serviços em nuvem torna-se um atrativo a mais para as organizações públicas de pequeno porte que possuem escassos capitais humanos e tecnológicos na gestão de TI.
- **Redução do tempo para implementação** – Para a ISACA[11], ao oferecerem ampla escalabilidade no poder de processamento e na capacidade de armazenamento de dados, quase em tempo real, os provedores de serviços

em nuvem podem reduzir drasticamente o tempo de implementação de soluções de TI.

- **Resiliência** – Ainda para a ISACA[11], a computação em nuvem pode fornecer um ambiente altamente resiliente e reduzir o potencial de falha e o risco de *downtime*.

No aspecto que envolve segurança, a ENISA – *European Network and Information Security Agency*[13] – entende que os benefícios de escala decorrentes da adoção de serviços em nuvem reduzem sensivelmente os valores de investimento em segurança, ao mesmo tempo em que permitem uma melhor proteção. Isso inclui todos os tipos de medidas defensivas, como: filtragem, gerenciamento de atualizações, o *hardening* das instâncias de máquinas virtuais e *hypervisors* etc. Outros benefícios da escala proporcionada pelos provedores de nuvem incluem: multiplicidade de localizações, redes de borda (conteúdo entregue ou processado mais perto de seu destino), menor tempo de resposta em incidentes e gerenciamento de ameaças.

Em resumo, a adoção dos serviços em nuvem computacional permite que as organizações usufruam de aspectos relevantes na área de segurança, como:

- **Maior resistência a ataques –** O provedor de serviços em nuvem possui maior capacidade em realocar dinamicamente os recursos de filtragem, *traffic shaping*, autenticação, criptografia etc.
- **Informações para auditoria –** O uso da virtualização e os padrões amplamente adotados pelos provedores de serviços em nuvem permitem a extração de informações para os processos de auditoria, fortalecendo as práticas de controle interno já defendidas amplamente por órgãos de controle.

- **Melhoria dos padrões de segurança:** A padronização de imagens de máquinas virtuais e dos módulos de software, usados pelos consumidores de serviços em nuvem, possibilita ajustes finos (*hardening*) de parâmetros de segurança.

Economia com a Computação em Nuvem

Outro benefício importante na adoção de serviços em nuvem é a redução de custos dentro e fora da área de TI das organizações. Segundo a IDC, as organizações conquistam importantes benefícios financeiros, que ajudam a incrementar sua eficiência, além de obterem importantes reduções de custos no longo prazo. Além de economias indiretas, já citadas anteriormente, como aumento da eficiência e produtividade da equipe de TI ou a redução do tempo para implantar nova infraestrutura de processamento e armazenamento, estimativas da empresa AWS (*Amazon Web Service*) apontam para 51% de redução do custo de TI em 5 anos e retorno financeiro a partir de 6 meses.[14] [15].

Segundo a ISACA, os provedores de nuvem são capazes de fornecer serviços de maneira menos dispendiosa do que nos modelos tradicionais de serviços de TI, devido a dois fatores principais: padronização e escala de serviços[12], a saber:

- **Padronização –** Por meio da padronização e abstração de tecnologias (por exemplo, uso de máquinas virtuais), os provedores podem aprimorar e reduzir o custo de armazenamento e capacidade de processamento de maneira mais eficiente. Isso reduz os custos de adição e remoção de sistemas à medida que as demandas de serviço mudam.
- **Escala –** Por meio do compartilhamento de recursos de TI em vários clientes com diferentes ciclos de demanda, eles

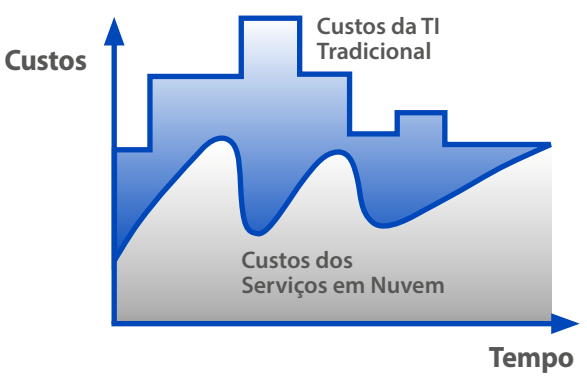
podem eliminar a subutilização de recursos. Isso reduz os custos indiretos associados à capacidade ociosa.

Por outro lado, o fator de economia mais relevante é a medição do serviço por utilização, uma das características essenciais dos serviços em nuvem computacional. O modelo de serviço baseado na demanda "*pay as you go*" ajudará a reduzir a imobilização de recursos em hardware e licenças de software (apropriadas como despesas de capital), permitindo que as organizações paguem apenas pelos serviços efetivamente utilizados em determinado espaço de tempo.

Para a ISACA, além da alteração do perfil das despesas, saindo de CAPEX – capital – para OPEX – correntes –, suprime-se o custo de obsolescência identificado em equipamentos, servidores e softwares envolvidos[12].

A figura a seguir apresenta um ambiente tradicional de TI, no qual as curvas de custo, ao longo do tempo, representam dispêndios para dotar recursos para TI (*hardware*, *software e peopleware*), de modo a atender às demandas atuais e futuras pelo pico, gerando uma subutilização de recursos na maior parte do tempo.

Figura 4. Subutilização de recursos em infraestrutura de TI[12]



Em um ambiente de nuvem computacional com pagamento por consumo, os custos ficam mais próximos do efetivamente consumido e a administração da dotação de recursos para a TI fica a cargo do provedor de nuvem, que se vale do compartilhamento da infraestrutura com vários clientes, ganhando a escala de serviços e reduzindo significativamente seus custos.

Para o CSCC[10], também é importante analisar os benefícios específicos de serviços em nuvem considerando a arquitetura dos serviços a serem utilizados, de modo a orientar o processo de priorização das soluções a serem migradas para o novo ambiente.

Infraestrutura como Serviços (IaaS):

- redução das despesas operacionais de TI e despesas de capital, melhorando a utilização de recursos e as taxas entre o administrador e o servidor;
- maior rapidez de comercialização graças ao aumento da eficiência e automação de soluções padronizadas;
- gerenciamento simplificado e integrado, incluindo monitoramento em tempo real e provisionamento de baixa escala e alta tecnologia;
- maior visibilidade dos processos de negócios e desempenho do sistema para identificar redundâncias e gargalos;
- operações escalonadas que podem atender à dinâmica do mercado e à estratégia de negócios.

Plataforma como Serviços (PaaS):

- Fornecimento altamente padronizado e automatizado de cargas de trabalho (*workloads*) predefinidas;

- uma plataforma integrada de desenvolvimento e tempo de execução para cargas de trabalho específicas;
- implantações consistentes baseadas em padrões para as cargas de trabalho mais comuns;
- forte suporte para aplicativos nativos da nuvem, incluindo tecnologias como contêineres, computação "sem servidor" e microsserviços;
- capacidade de desenvolvimento e operações que facilitam a comunicação, colaboração e integração entre desenvolvedores de software e profissionais de TI;
- gerenciamento integrado de carga de trabalho para aplicação de Acordos de Nível de Serviço (ANS), gerenciamento dinâmico de recursos, alta disponibilidade e prioridades de negócios;
- conscientização e otimização de cargas de trabalho com base nas prioridades de negócios e nos ANS;
- consolidação de cargas de trabalho sob um sistema de gerenciamento simplificado.

SaaS:

O SaaS possui como recursos principais:

- as ofertas de SaaS são acessíveis por meio da internet pública, o que torna muito fácil distribuí-las para um grande público dentro de um curto período de tempo;
- o SaaS trabalha com um modelo de precificação baseado no uso, que permite que as empresas assinem apenas os serviços de que precisam e para o número necessário de usuários;
- o SaaS geralmente oferece um conjunto de recursos tipo padrão que permite algum nível de configuração

para clientes individuais, mas normalmente não possui personalização;

- as organizações podem reduzir seus gastos de capital na aquisição de licenças de software, adotando ofertas de SaaS com base em assinatura;
- a implantação de SaaS é normalmente muito menor do que a implantação de soluções tradicionais empacotadas, o que permite que as empresas façam uso de qualquer pequena "janela de oportunidade" que possa se apresentar;
- as atualizações de SaaS são geralmente instantâneas e os provedores de serviços são responsáveis pela implantação (os softwares podem ser testados antes da implantação e o processo é transparente para os usuários finais);
- as ofertas de SaaS geralmente são escalonáveis à medida que os provedores planejam a escalabilidade em suas soluções de nuvem, o que permite que as organizações atendam rapidamente a um crescimento de demanda, se as necessidades de negócios exigirem;
- os problemas de segurança e privacidade são de responsabilidade do provedor de serviços em nuvem (provedores de serviços em nuvem têm um forte requisito de negócios para garantir que suas soluções lidem com esses problemas adequadamente);
- a disponibilidade da solução, incluindo o *backup* dos dados do cliente, geralmente é tratada pelo provedor de serviços em nuvem, eliminando a necessidade de os usuários finais manterem seus próprios procedimentos de recuperação de desastres para essas soluções.

Riscos Envolvendo Serviços em Nuvem Computacional

Em muitos aspectos, a gestão de riscos tem como uma das atividades mais complexas a identificação dos itens que comporão o mapa de riscos para o cenário que se deseja acompanhar, em especial quando se trata de uma nova tecnologia a ser adotada.

O fato é que os ambientes de nuvem computacional estão expostos às mesmas ameaças dos ambientes tradicionais de *data center*. Entretanto, a responsabilidade pela mitigação dos riscos resultantes dessas vulnerabilidades, muitas vezes, é compartilhada entre o provedor e o consumidor na nuvem; já outras somente pelo provedor, e algumas estão exclusivamente a cargo do consumidor. Como resultado, os consumidores devem ter bem clara a divisão de responsabilidades, confiar no fato de que o provedor cumprirá suas obrigações contratuais e ter uma equipe capacitada a responder rapidamente por seus encargos.

Para Timothy Morrow, do *Software Engineering Institute*[16], as organizações continuam a desenvolver novos aplicativos ou a migrar aplicativos existentes para serviços baseados em nuvem. Uma organização que adota tecnologias de nuvem ou escolhe provedores de serviços de nuvem computacional sem se tornar totalmente informada sobre os riscos envolvidos se expõe a uma variedade de riscos comerciais, financeiros, técnicos, legais e de conformidade.

A seguir, são descritos 12 riscos, ameaças e vulnerabilidades que, na visão de Timothy, as organizações enfrentam ao mover aplicativos ou dados para a nuvem computacional, ficando claro que não são de forma alguma exaustivos, visto que os problemas envolvidos nos processos de migração para a nuvem estão em constante evolução. Os cinco primeiros itens listados são exclusivos

do uso de serviços em nuvem, enquanto que os sete itens adicionais se aplicam tanto à nuvem quanto a ambientes *on-premises*.

1. **Redução da visibilidade e controle de ativos/operações** – Ao fazer a transição de ativos/operações para a nuvem, as organizações perdem alguma visibilidade e controle sobre esses ativos/operações. Ao usar serviços de nuvem externos, a responsabilidade por algumas das políticas e pela infraestrutura é transferida para o provedor.

   A real mudança de responsabilidade depende do(s) modelo(s) de serviço em nuvem usado(s), o que leva a uma mudança de paradigma para os órgãos em relação ao monitoramento e a *logs* de segurança. As organizações precisam realizar o monitoramento e a análise de informações sobre aplicativos, serviços, dados e usuários na nuvem sem usar o monitoramento e *logs* baseados em rede, disponível para TI local.

2. **Uso não autorizado de serviços sob demanda** – Os provedores de nuvem facilitam muito a oferta de novos serviços. Os recursos de provisionamento de autoatendimento sob demanda da nuvem permitem que o pessoal de uma organização provisione serviços adicionais a partir do provedor do órgão sem o consentimento da TI.

   Devido aos custos mais baixos e à facilidade de implementação dos produtos PaaS e SaaS, a probabilidade de uso não autorizado de serviços na nuvem aumenta. No entanto, os serviços provisionados ou usados sem o conhecimento

da TI apresentam riscos para uma organização. O uso de serviços de nuvem não autorizados pode resultar em um aumento de infecções por *malware* ou vazamento de dados, já que a organização não pode proteger os recursos que não conhece. O uso de serviços em nuvem não autorizados também diminui a visibilidade e o controle da rede e dos dados de uma organização.

3. **Comprometimento das APIs de gerenciamento com acesso à internet** – Os provedores de nuvem expõem um conjunto de interfaces de programação de aplicativos (APIs) que os clientes usam para gerenciar e interagir com os serviços de nuvem (também conhecidos como plano de gerenciamento). As organizações usam essas APIs para provisionar, gerenciar, orquestrar e monitorar seus ativos e usuários. Essas APIs podem conter as mesmas vulnerabilidades de *softwares* de uma API para um sistema operacional, biblioteca etc. Diferentemente das APIs de gerenciamento para computação local, as APIs de provedores de nuvem são acessíveis pela *internet*, expondo-as de maneira mais ampla a possíveis explorações.

   Os agentes de ameaças procuram vulnerabilidades nas APIs de gerenciamento. Se descobertas, essas vulnerabilidades podem se transformar em ataques bem-sucedidos e os ativos da nuvem da organização podem ser comprometidos. A partir daí os invasores podem usar os ativos da organização para perpetrar novos ataques contra outros clientes do provedor de nuvem.

4. **Falha na separação entre vários inquilinos** – A exploração de vulnerabilidades de sistema e *software* na infraestrutura, nas plataformas ou nos aplicativos de um provedor de serviços de criptografia que oferecem suporte à multialocação pode levar a uma falha na manutenção do isolamento entre os inquilinos. Essa falha pode ser usada por um invasor para obter acesso ao recurso de uma organização inicialmente e, a partir dele, acessar ativos ou dados de outro usuário ou de outra organização. A multialocação aumenta a superfície de ataque, levando a uma maior chance de vazamento de dados se os controles de isolamento falharem.

   Esse ataque pode ser obtido pela exploração de vulnerabilidades nos aplicativos, no *hypervisor* ou no *hardware* do provedor de nuvem, subvertendo controles de isolamento lógicos ou ataques à API de gerenciamento do provedor. Embora haja o risco, não se conhece caso de falha de segurança da plataforma SaaS de um provedor que tenha permitido a um invasor externo acessar os dados dos inquilinos.

5. **Exclusão de dados incompleta** – Ameaças associadas à exclusão de dados existem porque o consumidor reduziu a visibilidade de onde seus dados são fisicamente armazenados na nuvem e reduziu a capacidade de verificar a exclusão segura de seus dados. Esse risco é preocupante porque os dados são distribuídos por vários dispositivos de armazenamento diferentes dentro da infraestrutura do provedor de nuvem em um ambiente de multialocação.

Além disso, os procedimentos de exclusão podem diferir de provedor para provedor. As organizações podem não conseguir verificar se seus dados foram excluídos com segurança e se os dados remanescentes não estão disponíveis para os invasores. Essa ameaça aumenta à medida que um órgão usa mais serviços do provedor.

6. **Credenciais roubadas** – Se um invasor obtiver acesso às credenciais da nuvem de um usuário, o invasor poderá ter acesso aos serviços do provedor de nuvem para provisionar recursos adicionais (se as credenciais permitirem o acesso ao provisionamento), além de direcionar os ativos da organização. O invasor pode aproveitar recursos de computação em nuvem para atingir os usuários administrativos da organização, outras organizações que usam o mesmo provedor ou os administradores do provedor. Um invasor que obtiver acesso às credenciais da nuvem do administrador do provedor poderá usar essas credenciais para acessar os sistemas e dados do órgão.

   As funções de administrador variam entre um provedor de nuvem e uma organização. O administrador do provedor tem acesso à rede, aos sistemas e aos aplicativos da infraestrutura do provedor (dependendo do serviço), enquanto os administradores do consumidor têm acesso apenas às implementações em nuvem da organização. Em essência, o administrador do provedor tem direitos de administração sobre mais de um cliente e oferece suporte a vários serviços.

7. **Aprisionamento do fornecedor complica a mudança para outros provedores –** O aprisionamento do fornecedor se torna um problema quando uma organização considera a movimentação de seus ativos/operações de um provedor para outro, seja qual for o motivo. A organização descobre que o custo, esforço e tempo necessários para a mudança são muito maiores do que os inicialmente considerados, devido a fatores como formatos de dados não padronizados, APIs fora do padrão e dependência das ferramentas e APIs exclusivas de um provedor.

   Essa questão aumenta nos modelos de serviço em que o provedor assume mais responsabilidade. Quando um órgão usa mais recursos, serviços ou APIs, a exposição a implementações exclusivas de um provedor aumenta. Essas implementações exclusivas exigem alterações quando um recurso é movido para um provedor diferente. Se um provedor selecionado sair do negócio, ele se tornará um grande problema, já que os dados podem ser perdidos ou não podem ser transferidos para outro provedor de nuvem em tempo hábil.

8. **Aumento da complexidade que sobrecarrega a equipe de TI** – A migração para a nuvem pode introduzir complexidade nas operações de TI. Gerenciar, integrar e operar na nuvem pode exigir que a equipe de TI existente do órgão aprenda um novo modelo. A equipe de TI deve ter capacidade e nível de habilidade para gerenciar, integrar e manter a migração de ativos e dados para a nuvem, além de suas responsabilidades atuais de TI no local.

Os principais serviços de gerenciamento e criptografia se tornam mais complexos na nuvem. Os serviços, as técnicas e as ferramentas disponíveis para registrar e monitorar serviços em nuvem normalmente variam entre os provedores de nuvem, aumentando ainda mais a complexidade. Também pode haver ameaças e riscos emergentes em implementações de nuvem híbrida devido à tecnologia, às políticas e aos métodos de implementação, que adicionam complexidade. Essa complexidade adicional leva a um maior potencial de falhas de segurança na nuvem e em implementações locais de um órgão.

9. **Abuso dos acessos privilegiados** – Funcionários e administradores das organizações e dos provedores podem abusar dos acessos privilegiados às redes, aos sistemas e aos dados da organização, podendo causar danos ou expor informações confidenciais.

   O impacto é provavelmente maior quando se usa IaaS, devido à capacidade de um administrador de provisionar recursos ou executar atividades espúrias que exijam análise forense para detecção. Essas análises forenses podem não estar disponíveis com recursos da nuvem.

10. **Perda de dados armazenados –** Os dados armazenados na nuvem podem ser perdidos por outros motivos que não sejam ataques mal-intencionados. A exclusão acidental de dados pelo provedor de serviços de nuvem ou uma catástrofe física, como um incêndio ou terremoto, pode levar à perda permanente dos dados do cliente. O ônus

de evitar a perda de dados não recai unicamente nos ombros do provedor. Se um cliente criptografar seus dados antes de carregá-los na nuvem, mas perder a chave de criptografia, os dados serão perdidos. Além disso, a compreensão inadequada do modelo de armazenamento de um provedor de nuvem pode resultar em perda de dados. Os órgãos devem considerar a recuperação de dados e estar preparados para a possibilidade de seu provedor ser adquirido, alterar ofertas de serviços ou ir à falência.

Essa ameaça aumenta à medida que um órgão usa mais serviços do provedor de nuvem. Recuperar dados em um provedor pode ser mais fácil do que recuperá-lo em um órgão, porque um SLA designa percentuais de disponibilidade/tempo de atividade. Essas porcentagens devem ser investigadas quando o órgão selecionar um provedor de nuvem.

11. **Comprometimento dos fornecedores do provedor de nuvem** – Se o provedor terceirizar partes de sua infraestrutura, suas operações ou sua manutenção, esses terceiros poderão não satisfazer/suportar os requisitos que o provedor é contratado para fornecer a um órgão. O órgão precisa avaliar como o provedor impõe a conformidade e verificar se ele direciona seus próprios requisitos para terceiros. Se os requisitos não estão sendo cobrados na cadeia de suprimentos, a ameaça para o órgão aumenta. Essa ameaça aumenta à medida que o órgão usa mais serviços de nuvem computacional ou depende de vários provedores individuais.

12. **Auditoria insuficiente aumenta o risco de segurança cibernética** – Os órgãos que migram para a nuvem geralmente realizam auditorias insuficientes. Eles movem dados para a nuvem sem entender todo o escopo de fazê-lo, as medidas de segurança usadas pelo provedor e sua responsabilidade de fornecer medidas de segurança. Eles tomam decisões para usar serviços de nuvem sem entender como esses serviços devem ser protegidos.

ADOÇÃO DE SERVIÇOS EM NUVEM NO GOVERNO

A estratégia de migração de serviços computacionais de uma estrutura própria para uma estrutura em nuvem tem sido objeto por parte de empresas particulares e por parte de governos. São exemplos de iniciativas preconizadas por governos, que passaram a ser consideradas exemplos de passos iniciais para a adoção de recursos em nuvem, as recomendações *Cloud First* e *Cloud Smart* do governo norte-americano, as recomendações G-Cloud do governo britânico, além de iniciativas dos governos do Canadá, da Austrália, da Estônia, entre outros.

Processos de Adoção de Nuvem pelo Governo Americano

Em 2011, Vivek Kundra, então CIO do governo americano, publicou a estratégia de adoção de serviços em nuvem (*Federal Cloud Computing Strategy*), denominada de *Cloud First* [17], enfatizando a prioridade de migração da infraestrutura *on-premises* das agências governamentais (órgãos públicos) para o ambiente de nuvem computacional, de modo a minimizar um conjunto de problemas que impactavam o bom atendimento ao público, tais como: utilização não otimizada de ativos de TI por parte do governo americano, a fragmentação na demanda por recursos, sistemas duplicados, ambientes que apresentavam dificuldade de gerenciamento, entre outros.

A análise, apresentada no documento *Federal Cloud Computing Strategy*, mostrou que os dispêndios totais estimados em TI, à

época, por parte do governo americano, totalizavam cerca de US$ 80 bilhões. Além disso, estimou que, dos US$ 80 bilhões, US$ 20 bilhões poderiam ser potencialmente aplicados na contratação de serviços em nuvem.

O foco do governo americano, ao publicar a estratégia de adoção de serviços em nuvem, foi direcionar as soluções de TI das agências governamentais de forma sincronizada e com um mínimo de padronização nas ações. Com isso, estratégias de decisão e casos de implantação seriam disseminados entre as agências, facilitando e uniformizando minimamente as ações de migração ou adoção de recursos em nuvens por parte de diferentes agências federais.

Além das motivações de caráter técnico, o documento *Federal Cloud Computing Strategy* destacou a oportunidade de tornar os serviços públicos americanos mais eficientes, ágeis e inovadores, com a aplicação mais efetiva dos investimentos destinados a TI, aderentes às práticas adotadas pelo setor privado. A preocupação inicial do governo americano foi nivelar as agências com relação aos conceitos de serviços em nuvem. Neste sentido, todos os conceitos de serviços em nuvem foram apresentados (*Cloud Infrastructure as a Service – IaaS; Cloud Plataform as a Service – PaaS; Cloud Software as a Service – SaaS*), sendo destacadas as seguintes vantagens:

- melhorias decorrentes da utilização de recursos em nuvem;
- melhor utilização de ativos de TI;
- redução de esforços duplicados;
- possibilidade de tornar os serviços mais responsivos;
- escalabilidade dos recursos;
- rapidez na implantação de inovações; e
- encorajamento de uma cultura empreendedora com redução de riscos na área de TI.

Passados cinco meses da publicação do documento *Federal Cloud Computing Strategy*, a *TechAmerica Foundation*, fundação que tem como objetivo representar empresas americanas de tecnologia, instituiu a *Commission on the Leadership Opportunity in U.S. Deployment of the Cloud* (CLOUD^2), que, por sua vez, gerou o documento *Cloud First Buyer's Guide for Government*, com sugestões de diretrizes que deveriam ser adotadas pelas agências governamentais americanas para a adoção de serviços em nuvem.

Principais orientações estabelecidas para o *Cloud First*

A estratégia do documento *Federal Cloud Computing Strategy* foi apresentar, de forma didática, às agências governamentais americanas, os conceitos fundamentais de serviços em nuvem (IaaS, PaaS e SaaS), elencar os principais benefícios do uso de soluções em nuvem e estabelecer uma estratégia inicial de implantação de serviços em nuvem nessas agências.

O objetivo à época foi ambicioso: orientar cada agência governamental a escolher pelo menos três serviços a serem "disponibilizados em nuvem" em um prazo de 36 meses, sendo que o primeiro em pelo menos 18 meses.

Os benefícios dos serviços em nuvem foram destacados observando-se as seguintes características:

1. **Eficiência –** O uso de nuvem permite melhor utilização dos ativos de TI, melhor produtividade no desenvolvimento de soluções de TI (redes, aplicações etc.), melhor gerenciamento de recursos, enquanto que nos modelos convencionais há casos de baixo uso de recursos de ativos de TI disponíveis, casos de duplicação desnecessária de plataformas e dificuldade de gerenciamento de diferentes ambientes.

2. **Agilidade nas ações inerentes aos recursos de TI –** O uso de nuvem permite a aquisição de recursos "como serviços" de fornecedores já cadastrados previamente, escalabilidade (que permite o aumento e o decréscimo de recursos conforme a necessidade) e respostas mais ágeis às necessidades urgentes das agências federais. As críticas colocadas em relação ao modelo convencional são muito semelhantes às dificuldades encontradas em diferentes governos, como: períodos longos para implantação de novos recursos de *data center* para novos serviços e, muitas vezes, períodos longos para incrementar serviços já existentes.

3. **Inovação –** O uso de nuvem permite deslocar o foco das ações do gerenciamento de ativos para o gerenciamento de serviços, tornando mais efetivo o serviço prestado ao cidadão. Permite soluções próximas às soluções de ponta adotadas pelo setor privado, estimula o empreendedorismo no serviço público e permite ao setor de TI governamental estar próximo a tecnologias emergentes. Naturalmente, as críticas colocadas ao modelo convencional são as dificuldades de manter a infraestrutura de soluções de TIC do governo, por vezes desatualizadas frente às do setor privado, por conta de diferentes dificuldades, além da sobrecarga, no modelo convencional, de atividades de gerenciamento de ativos (servidores, redes etc.).

A adoção inicial de serviços em nuvem foi, então, apresentada na forma de um *framework* com três etapas propostas para orientar a decisão de migração para nuvem:

- **Primeira etapa:** seleção do serviço da agência passível de ser migrado para a nuvem.
- **Segunda etapa:** disponibilização de recursos (todo tipo de recurso) para possibilitar a primeira migração e disponibilização dos serviços escolhidos na nuvem.
- **Terceira etapa:** gerenciamento dos serviços e migração.

Primeira etapa: seleção do serviço

No processo de "seleção do serviço" de TI passível de migração, a orientação foi no sentido de identificar valores que justificassem a migração, baseados em eficiência, agilidade e inovação, sempre tendo como objetivo final a melhoria na prestação dos serviços ao cidadão.

Em paralelo, neste processo de identificação dos serviços passíveis de migração, foi destacada a necessidade de identificar:

- Características de segurança necessárias: necessidade de aderência a leis, regulações governamentais etc., características dos dados a serem acessados, necessidades de privacidade e confidencialidade, integridade, controles e políticas de acesso, além de governança, de forma a garantir o controle e a transparência dos serviços.
- Características do serviço: observar os aspectos de interoperabilidade, disponibilidade, performance, confiabilidade, escalabilidade, portabilidade, confiabilidade do eventual fornecedor e compatibilidade de arquitetura do serviço com o ambiente de nuvem.
- Características de infraestrutura: verificação de infraestrutura de redes, aplicação que suporta o serviço e dados, para entender se todos esses itens estão preparados para uso

de ambiente de nuvem. Como exemplo, a infraestrutura de redes deve ser analisada para verificar se suporta conexões de alta velocidade, redundâncias etc. A aplicação que suporta o serviço deve ser analisada para verificar se está apta a ter interfaces via *web* e se os dados fornecidos ou acessados estão em formatos adequados para ambiente em nuvem.

- Disponibilidade de soluções no mercado: as soluções de mercado devem ser conhecidas, de forma a identificar se há ou não solução para acomodar os serviços analisados em ambiente de nuvem.
- Disponibilidade, por parte do governo, em patrocinar a migração: inclui uma autoanálise sobre estar preparado para colocar um serviço em nuvem (equipes, sistemas, gerenciamento etc.) e se há disposição e financiamento do governo para tal.
- Ciclo de vida da tecnologia em observação: as soluções de nuvem avaliadas devem ser também analisadas à luz do estado da arte na respectiva tecnologia, de forma a identificar se estão ou não dentro do ciclo de vida de utilização ou se estão em fim de uso.

Apesar de ser uma decisão aparentemente natural, o documento *Federal Cloud Computing Strategy* enfatiza que, no processo de seleção de serviços passíveis de migração para a nuvem, devem ser considerados prioritários aqueles que possuem alto valor agregado (atendimento de áreas sensíveis, como saúde, serviços essenciais ao cidadão etc.) e que estejam prontos, ou seja, em produção no ambiente convencional, deixando para etapas posteriores serviços que devem ser disponibilizados ou concluídos para disponibilização ao público em médio e longo prazo. É uma estratégia extremamente

direta, com o objetivo de usufruir de imediato os benefícios de uso de nuvem em serviços existentes. Isso traz mais segurança ao processo de implantação, com o retorno de reconhecimento por parte de usuários e prestadores.

Segunda etapa: prover os serviços adequadamente na nuvem

O documento *Federal Cloud Computing Strategy* destaca que, para prover os serviços na nuvem, é necessária uma mudança de mentalidade da agência governamental.

Nos ambientes convencionais, os esforços são no sentido de gerenciar recursos computacionais e de comunicação de dados. No ambiente de nuvem, os esforços passam a ser a gerência da qualidade dos serviços prestados, o que envolve, além dos recursos de infraestrutura, avaliações do atendimento, fornecimento e qualidade na prestação dos serviços contratados.

Terceira etapa: gerenciar serviços na nuvem

Trata-se da etapa operacional de manter os serviços na nuvem, continuação natural da segunda etapa, envolvendo a consolidação na mudança de atitude da agência com relação aos recursos computacionais, já que passam a ser gerenciadas também a qualidade e a continuidade da prestação dos serviços, além dos recursos computacionais.

O documento *Federal Cloud Computing Strategy* inclui, ainda, estudo de caso para ilustrar às agências governamentais como aplicar o *framework* sugerido.

Na sequência do documento, a *TechAmerica* publicou o documento *Cloud First Buyer's Guide*, para servir de guia prático para a implantação de serviços em nuvem nas diversas agências federais americanas.

Cloud First Buyer's Guide

O documento foi preparado pela já citada *Commission on the Leadership Opportunity in U.S. Deployment of the CLOUD*[2]. No documento, houve orientação para que as agências americanas fizessem um estudo cuidadoso sobre serviços em nuvem, de forma a identificar quais dos serviços atenderiam às suas necessidades, para então adotar a solução quando fosse apropriado. A preparação da agência considerou os seguintes passos:

Passo 1 – Iniciar o processo de uso de nuvem

Deve-se iniciar o processo de uso de nuvem com um caso de negócio no qual fosse possível identificar requisitos necessários e o desempenho desejado, sem associar essas necessidades a um tipo específico de nuvem (pública, privada ou híbrida).

O cuidado nessa orientação foi no sentido de não fechar a solução em um determinado modelo de nuvem, pois isso poderia limitar o benefício de adotar diferentes soluções.

Ainda neste passo, a orientação dada pelo governo americano às agências foi para que observassem casos de soluções em nuvem já implantados em outras agências ou mesmo no setor privado, partindo de soluções mais simples para soluções mais complexas, tais como o uso da nuvem para:

- Armazenamento, processamento, hospedagem *web*, *backup* de dados, ou seja, serviços de nuvem na categoria IaaS;
- Banco de dados, gerenciamento de identidade, sistemas de informações georreferenciais e sistemas similares que se enquadram em serviços de nuvem PaaS;

- Serviços de correio eletrônico, colaboração, processamento de dados e centrais de serviços, que caracterizam serviços de nuvem SaaS.

Passo 2 – Mapear as prioridades da agência no uso de serviços em nuvem

É importante fazer com que cada agência governamental tenha uma compreensão clara dos atributos e recursos de nuvem que são mais relevantes para atender às suas necessidades.

Neste sentido, o documento publicado pelo governo americano apresentou uma lista de atributos a serem considerados, devendo caber às agências dar o peso a cada um dos atributos de acordo com suas necessidades e de acordo com as características do negócio conduzido.

Os atributos que foram considerados são os seguintes:

- *Frequência de atualização e patches automáticos necessários ao ambiente computacional da agência* – Neste caso, o uso de nuvem pode ser uma alternativa vantajosa para as agências que têm necessidades constantes de atualizações e manutenção de sistemas.
- *Colaboração com outras agências e ambiente externo* – A nuvem pode ser considerada um ambiente adequado para otimizar trabalho colaborativo entre agências e possibilitar o uso de aplicações em redes sociais para o acesso a informações, sempre destacando os aspectos de segurança necessários.
- *Conformidade dos serviços de nuvem com padrões existentes* – Este atributo é colocado para que as agências avaliem

a capacidade de provedores de serviços em nuvem em atender requisitos de conformidade de determinados serviços. Um exemplo seria avaliar se o provedor atende aos requisitos colocados na regulamentação de portabilidade de planos de saúde, o *HIPAA – Health Insurance Portability and Accountability Act*.

- *Necessidade de plataforma de desenvolvimento na nuvem* – Determinadas agências podem necessitar de soluções customizadas. Neste caso, são agências que podem necessitar de ambientes PaaS e SaaS, com plataforma de desenvolvimento que ofereça recursos tais como: diferentes linguagens de programação, estruturas adequadas para desenvolvimento de aplicações (controle de acesso e versões), segurança, transparência e privacidade.
- *Identificação de facilidade de uso* – As agências devem considerar um universo de usuários com diferentes conhecimentos de TI e, neste sentido, deve avaliar a facilidade do uso dos recursos em nuvem disponibilizados, notadamente nos ambientes PaaS e SaaS. Esta avaliação é importante para definir a satisfação dos usuários, escolher provedores e definir melhorias.
- *Eficiência no uso de energia* – Além dos recursos computacionais, os ambientes de *data center* têm requisitos de infraestrutura que oneram a sua manutenção, que são a refrigeração e a energia. O uso de nuvem pode ser impactante com relação à eficiência energética, e isso foi observado às agências.
- *Integração entre ambiente de nuvem e ambiente interno* – Deve-se identificar a necessidade de integração entre aplicativos em nuvem e aplicativos internos.

- *Interoperabilidade e aderência a padrões abertos* – Deve-se identificar se os serviços da agência que utilizam ambiente de nuvem são aderentes a padrões abertos adotados. Observe que não se trata de analisar o ambiente de colaboração, mas sim a necessidade da agência de aderência a padrões abertos no provedor de nuvem a ser contratado.
- *Necessidade de recursos de mobilidade* – Caso a agência faça uso massivo de plataformas móveis, isso pode ter impacto na escolha do serviço de nuvem. Neste caso, este atributo ganha em importância.
- *Portabilidade* – Atributo comum a todas as agências, considerando-se que eventualmente haja a necessidade de migração dos dados entre diferentes plataformas e provedores.
- *Importância da escalabilidade dos recursos a serem contratados* – As agências devem avaliar a necessidade de escalabilidade dos serviços a serem contratados em função da natureza dos serviços prestados pela própria agência. Ações sazonais ou mesmo perspectiva de crescimento ou melhoria programada dos serviços são fatores que impactam neste atributo.
- *Requisitos de segurança* – Atributo comum a todas as agências. Devem ser avaliados os requisitos de segurança em função do tipo de serviço prestado. Um item em separado na documentação do *Cloud First* trata da segurança no serviço em nuvem.
- *Requisitos de agilidade na implantação do serviço em nuvem* – Atributo comum a todas as agências. Deve ser avaliada a necessidade de rapidez na implantação dos serviços selecionados no ambiente de nuvem.

- *Requisitos de sustentabilidade* – Atributo comum a todas as agências. Deve ser avaliada a capacidade dos fornecedores de atender novas demandas de forma alinhada com a missão da agência governamental. O objetivo é verificar quão sustentável é a solução adotada em função da capacidade do fornecedor.
- *Requisitos de transparência na monitoração dos serviços* – Atributo comum a todas as agências. Devem ser avaliadas as ferramentas de monitoração de desempenho, confiabilidade e disponibilidade para as implementações de serviços em nuvem. Esta avaliação garante a governança mínima com relação aos recursos de infraestrutura disponibilizados.

Passo 3 – Identificar os requisitos de segurança

Neste passo, o guia orienta a agência a avaliar os requisitos de segurança do serviço analisado e indica que, da mesma forma que determinados serviços necessitam de homologação por parte das agências de segurança americanas quando implantados em ambientes convencionais, há a necessidade do mesmo tipo de autorização para serviços a serem disponibilizados em nuvem.

Passo 4 – Identificar como um serviço será implantado na nuvem

Trata-se de uma orientação para que sejam avaliados os serviços que podem ser migrados de acordo com a necessidade de negócios e a missão da agência e que possam ser compartilhados com outras agências com necessidades semelhantes. Neste caso, o guia atenta para aspectos como: facilidade de configuração do serviço na nuvem, possibilidade de compartilhamento da solução ou do serviço colocado na nuvem com outra agência governamental, impacto de alterações feitas no serviço em

outras agências que eventualmente compartilhem o mesmo serviço, grau de automação nos procedimentos de portabilidade dos dados relativos ao serviço disponibilizado em nuvem (de modo a evitar a dependência de fornecedores) e, ao final, a integração das soluções utilizadas no ambiente de nuvem com as ferramentas internas do respectivo serviço.

Passo 5 – Identificar as sugestões ao processo de implantação do serviço em nuvem

É uma orientação no sentido de que sejam publicadas solicitações de propostas (*RFP – Request for Proposals*) ao processo de implantação de serviços em nuvem, de forma a possibilitar que fornecedores, usuários e demais envolvidos no processo se manifestem com sugestões.

Passo 6 – Identificação de outras iniciativas de governo na implantação de serviços em nuvem

Devem ser pesquisados – junto a órgãos normatizadores (NIST, FedRAMP etc.), junto às áreas de compras do governo federal e junto a outros órgãos – processos e orientações para a implantação de serviços em nuvem, observando-se todos os aspectos, desde aspectos técnicos de infraestrutura, aspectos de segurança necessários e definidos pelo governo, além de aspectos administrativos.

Passo 7 – Observar a necessidade de envolvimento das pessoas no processo de migração para nuvem

O guia destaca a importância de envolver as pessoas e gerenciar o processo e os problemas inerentes a este processo, como uma ação fundamental.

Passo 8 – Identificar um parâmetro comum para medições de desempenho que seja comum a diferentes fornecedores

É necessário procurar identificar parâmetros concretos de avaliação de desempenho de fornecedores aplicáveis a diferentes fornecedores. Este esforço é comum a qualquer agência.

Passo 9 – Identificar gatilhos adequados para implementação de serviços em nuvem

É essencial procurar identificar gatilhos (oportunidades) para a implantação de serviços em nuvem em função das ações vinculadas ou submetidas ao órgão ou em função do comportamento do mercado, como, por exemplo:

- necessidade de atualização de ativos de ti;
- atendimento a implementações e/ou atualizações de sistemas;
- novas infraestruturas de TI para testes, desenvolvimento ou conversão de ambientes;
- projetos-piloto ou novas capacidades utilizadas esporadicamente.

Na sequência, o documento *Cloud First Buyer's Guide* elenca um conjunto amplo de profissionais com capacitação em cada um dos segmentos necessários ao processo de implantação em atendimento ao *Cloud First*, destacando:

- Gerente de compras com conhecimento profundo da área técnica correlata, ou seja, com conhecimento em processos de compra, descrição de requisitos e gerenciamento do processo de compras.

- Gerente de programa com conhecimento de gerenciamento do processo de compras e capacidade de interfaceamento com outras agências e órgãos governamentais.
- Diretor financeiro responsável pelas ações financeiras e administrativas do processo.
- CIO (*chief information officer*) e CISO (*chief security officer*) com a missão de conduzir tecnicamente a organização de TIC (infraestrutura e segurança), observando as questões de padrões, escalabilidade, atualizações, reutilizações etc.
- Diretor de RH com a missão de garantir a força de trabalho e a preparação adequada (treinamento) dela.
- Diretor/liderança da agência com a missão de conduzir todo o processo, realizando, inclusive, o interfaceamento com outras agências, buscas por recursos financeiros, o acompanhamento de riscos e o sucesso da empreitada.

Resultados do *Cloud First*

Em 2012, as agências americanas compartilharam os sete desafios comuns para a migração das estruturas tradicionais para a computação em nuvem:

- Dificuldade no atendimento dos requisitos de segurança federal.
- Orientação insuficiente para a tomada de decisão.
- Capital humano insuficiente para a implementação de serviços em nuvem.
- Dificuldade na certificação e no credenciamento de fornecedores.
- Falta de garantia da portabilidade e interoperabilidade de dados.
- Barreiras culturais das agências americanas.

- Dificuldade na definição de quantidades e custos específicos devido aos custos flutuantes.

De fato, o incremento dos serviços em nuvem foi executado conforme a estratégia, mas de maneira desigual. Um estudo elaborado pela GAO [18] no ano de 2014 demonstrou que, embora o número de serviços de computação em nuvem tenha pulado de 21 para 101 (381%) desde 2012, o número implementado por cada agência durante esse período variou. Por exemplo, desde 2012, o HHS (*U.S. Department of Health and Human Services*) implementou 33 desses serviços, enquanto a SBA (*U.S. Small Business Administration*), o Estado e o Tesouro implementaram 3, 11 e 2, respectivamente. E, a despeito das agências coletivamente e individualmente aumentarem a porcentagem de seus orçamentos de TI alocados para serviços em nuvem, o estudo demonstrou que as agências ainda estão dedicando uma grande parte de seus orçamentos de TI a gastos não relacionados à computação em nuvem. As agências estavam orçando coletivamente 2% de seus orçamentos de TI para serviços em nuvem, enquanto os 98% restantes ainda estavam dedicados a despesas não relacionadas à nuvem.

Uma das principais razões citadas pelos funcionários da agência para explicar por que a maioria de seus serviços não havia sido migrada para nuvem foi a decisão de considerar a utilização de serviços em nuvem somente quando ocorresse modernização do serviço ou substituição de um produto no final do ciclo de vida, por exemplo. Soma-se a isso o desafio de substituir os sistemas legados, pois havia uma relutância em ceder o controle direto dos recursos de TI de missão crítica a uma empresa contratada.

Tais resultados, no entanto, não chegam a invalidar a estratégia *Cloud First*, que acabou sendo adotada com sucesso por várias empresas privadas, em especial por conta da estratégia de migração criada.

Cloud Smart*, uma evolução do *Cloud First

Em 2018, após sete anos da publicação do *Federal Cloud Computing Strategy*, o governo americano publicou a primeira versão do documento *Cloud Smart Strategy*.

A justificativa para o *Cloud Smart Strategy* foi acelerar e atualizar as ações e recomendações de uso de soluções em nuvem para as agências federais americanas. A crítica aos documentos iniciais foi a falta de implementação de um plano estratégico no governo americano, o que tornou lenta a adoção de soluções em nuvem por parte de muitas agências. O *Cloud Smart Strategy* objetiva retomar a celeridade pretendida na implantação de serviços em nuvem nas agências governamentais americanas.

As agências precisarão compartilhar suas experiências transformadoras com seus pares para que o governo possa alavancar, de maneira coletiva, o compartilhamento do conhecimento. O governo, em conjunto com suas agências federais, busca desenvolver um plano de trabalho de ações e atualizações políticas direcionadas durante 18 meses, que considerará soluções baseadas em fornecedores, soluções hospedadas por agências, serviços compartilhados inter e intra-agências, soluções de multinuvem e híbridas [(19)].

Os itens seguintes contêm os destaques de cada um desses documentos, observando-se que se trata de comentários de caráter introdutório, para permitir ao leitor uma visão macro das estratégias adotadas pelo governo americano. O acesso aos documentos citados permitirá ao leitor acesso às informações detalhadas.

Durante os quase oito anos da política de *Cloud First*, em que se deu bastante ênfase em mover a infraestrutura para a nuvem computacional, ficou claro que as diferenças entre as agências se tornaram um empecilho à execução da estratégia. Para Suzette Kent, atual CIO

do governo americano, "*a política foi lançada em um momento em que a computação em nuvem ainda era uma tecnologia muito nova*". Seria necessário lançar uma nova estratégia que atualizasse a abordagem original e fechasse algumas lacunas nas políticas para permitir uma adoção mais rápida e simplificada, mais baseada nas necessidades específicas de cada agência, ao invés de se querer tratar todas como se fossem iguais, utilizando-se de atividades-padrão que servissem a "todos os tamanhos". Como exemplo, aponta o fato de que a maior parte das orientações está concentrada nos benefícios potenciais, ao invés dos resultados a serem obtidos.

Uma nova estratégia precisaria englobar esses aspectos de forma urgente: "*Mover um aplicativo de um data center tradicional para um fornecedor de infraestrutura virtualizado geralmente não permite a escalabilidade automática de aplicativos com maior demanda do usuário. Para atingir esse objetivo, os esforços de desenvolvimento e execução de projetos serão frequentemente necessários para refatorar aplicativos com o objetivo de aproveitar novos recursos, como provisionamento automático, e isso deve ser levado em conta na análise e no planejamento*" [19].

Foi com esse objetivo que o governo dos USA desenvolveu o *Cloud Smart* para atualizar a estratégia de adoção de nuvem no governo federal. A principal evolução trazida pela atualização da estratégia está no fornecimento de apontamentos mais específicos sobre como realizar a adoção da nuvem, focando-se em três pilares: segurança, aquisição e habilidades necessárias da força de trabalho.

- **Segurança:** A nova estratégia define que a evolução da política e da segurança cibernética do governo federal americano é essencial para a modernização, sugerindo o uso de abordagem de avaliação dos riscos. Ao adotarem a abordagem para a adoção da nuvem, as agências devem fazer uma transição

dos mecanismos de segurança para a *camada de dados*, em vez de nas camadas de infraestrutura física e de rede, além de melhorar a governança dos sistemas. Definem, ainda, como essencial "que as agências tenham total visibilidade de seus dados, no local e na nuvem, realizando o monitoramento contínuo para detectar atividades maliciosas".

- **Aquisição:** Considerando a afirmação da atual CIO do governo americano, por sua característica inovadora, várias agências, grupos de trabalho e parceiros do governo passaram a colaborar com uma série de recomendações para profissionais de tecnologia da informação e responsáveis pelas aquisições no governo acerca das melhores formas de se contratar nuvem. No entanto, percebeu-se a necessidade de uma orientação única e consistente para todo o governo, incluindo aí o compartilhamento de informações entre agências sobre melhores práticas. Essa lacuna levou as agências a pesquisar em várias fontes para obter uma compreensão básica dos tipos de serviços em nuvem vendidos no mercado comercial, as diferentes ofertas disponíveis em contratos existentes em todo o governo e a melhor maneira de avaliar qual abordagem beneficiaria um determinado requisito, o que acabou criando preocupações atinentes ao uso da tecnologia, em especial no que se referia à segurança das informações das agências. Percebeu-se a necessidade de uma maior atenção para garantir que o pessoal técnico das agências tenha as ferramentas necessárias para reduzir os riscos de segurança e proteger os dados do governo. A nova estratégia foca na capacitação das agências na utilização de uma variedade

maior de abordagens para alavancar os pontos fortes do governo federal, possibilitando *vantagens sobre compras em massa e conhecimento compartilhado de bons princípios de aquisição*. Como parte da abordagem multidisciplinar da *Cloud Smart*, eles também precisarão colocar as questões de segurança na vanguarda de qualquer esforço de aquisição.

- **Força de trabalho:** O governo americano tem o entendimento claro de que as equipes de tecnologia da informação das agências federais são responsáveis por executar as missões da agência, fornecer serviços ao público e proteger os sistemas e as informações críticos dos USA. Enfatizam que, "*da mesma forma que as agências não podem terceirizar o risco, não podem terceirizar a tomada de decisões críticas para os fornecedores*". Dessa forma, a nova estratégia também tem como pilar o aprofundamento do conhecimento técnico de sua própria força de trabalho com as habilidades necessárias para levar a estratégia adiante, elevando a maturidade da equipe, para que, à medida que as agências adotem e migrem seus serviços para plataformas de nuvem, o impacto dessas migrações na força de trabalho seja visível e precise ser constantemente examinado, juntamente com a identificação de possíveis lacunas de habilidades. Afirmam que "as agências devem prever quais novas habilidades e abordagens programáticas serão necessárias para abordar suas lacunas e evolução". Como exemplo, citam que "a migração para tecnologias de nuvem pode reduzir as necessidades de gerenciamento de *hardware* de tecnologia da informação, mas provavelmente aumentará a necessidade de habilidades de programação no uso de 'infraestrutura como código' ". Ao mesmo tempo, as agências

devem preparar suas equipes de aquisição com habilidades e conhecimentos próprios para acompanhar a lista cada vez maior de opções de tecnologia disponíveis. Dessa forma, as políticas e estratégias de nuvem das agências devem possuir um componente de planejamento e desenvolvimento da força de trabalho que inclua "a identificação de lacunas de habilidades atuais e futuras", "a requalificação e a retenção de talentos", "o recrutamento e a contratação de acordo com as lacunas de habilidade da agência", "estratégias de comunicação, engajamento e transição de funcionários" e a "remoção de barreiras para a contratação de talentos com prontidão".

Processos de Adoção de Nuvem pelo Governo Inglês

Em março de 2011, o governo britânico publicou o documento *Cloud Government Strategy*, com o objetivo de orientar os órgãos públicos federais na migração para serviços em nuvem. Publicado um mês após o documento *Cloud First* do governo americano, o documento inglês detalhou uma abordagem sensivelmente diferente na orientação para adoção de serviços em nuvem às suas agências públicas, porém considerou a iniciativa *Cloud First* americana como sendo uma das referências a serem observadas não somente para prover introdução e educação na área de serviços em nuvem, mas também para ser referência em aquisição e operação de serviços comuns em nuvem.

Em seu documento, o governo inglês descreveu as características de serviços em nuvem e destacou a mudança de paradigma no modelo de contratação de serviços por parte de órgãos públicos federais. A disponibilização de serviços em nuvem para os órgãos do governo britânico foi estruturada em uma "loja" virtual, denominada inicialmente *Government Application Store* ou *Cloud Store* e, desde 2014, é denominada *Digital Marketplace*.

Os objetivos iniciais da *Cloud Store* foram:

- Disponibilizar um mercado/loja aberto, com alta visibilidade, com produtos comuns de serviços de TIC, de forma a ser o primeiro ponto de consulta para a aquisição de necessidades de TIC por parte do setor público.
- Criar um mercado/loja no qual as agências públicas possam encontrar soluções, inovação e diferentes fornecedores.
- Explorar um conjunto relevante de soluções comuns ao setor público.
- Permitir a comunidades de arquitetura da informação e de segurança da informação ter acesso a informações relativas a condições de segurança e certificação de serviços.
- Ser o embrião de processos colaborativos de aquisição de serviços e soluções, incluindo a disseminação de informações sobre fornecedores e servindo como agente facilitador de reuso de serviços no sentido de aumentar a eficiência e a economia de custos.

Com isso, o governo inglês procurou aumentar o leque de soluções comuns de mercado, dar mais flexibilidade e liberdade de escolha de soluções por parte de órgãos públicos, facilitar e agilizar o uso dessas soluções disseminadas no mercado, diminuir custos e aumentar a competitividade.

Para os fornecedores, estabeleceu-se a oportunidade de um mercado aberto, permitiu processos mais justos e simples de fornecimento de soluções ao governo e liberdade de inovações no fornecimento dos serviços.

A orientação do *G-Cloud* para as agências governamentais foi no sentido de que considerem e avaliem o potencial de uso de nuvem antes de qualquer outra opção quando se tratar de serviços existentes.

De acordo com o *G-Cloud*, o governo cria *frameworks* de fornecimento de serviços de nuvem de acordo com as necessidades observadas junto às agências governamentais.

Desde o início da *G-Cloud* foram publicados 10 f*rameworks* para cadastro de fornecedores, especialistas e colaboradores. O último chamado (*G-Cloud 10*) para cadastro de fornecedores junto ao governo britânico ocorreu em abril de 2018, com a publicação dos fornecedores cadastrados no *Digital Marketplace* em julho de 2018.

Para cadastro no *Digital Marketplace*, os fornecedores devem consultar o documento *Cloud Supplier's Guide* publicado pelo governo britânico. O documento descreve o *Digital Marketplace* e o *G-Cloud*, quem pode se submeter ao *framework* mais recente para o *G-Cloud* (atualmente, é o *framework G-Cloud 10*), quais serviços podem ser vendidos em atenção ao chamado, como submeter a intenção de ser fornecedor de soluções de nuvem ao governo britânico, quando se submeter e os serviços existentes.

Os serviços que podem ser oferecidos vão desde a hospedagem em nuvem, soluções de *software* e suporte, espaço em *data centers* etc. Um serviço que convém destacar é a possibilidade de contratação de especialistas em nuvem para apoio às atividades da agência governamental e facilidades de pesquisa para usuários (contrato de grupos de pesquisa).

Os serviços oferecidos no *Digital Marketplace* estão divididos em:

- ***Cloud Hosting*:** Plataforma de nuvem e infraestrutura para implantação, gerenciamento e execução de SW, recursos de processamento, armazenamento e recursos de redes e outros serviços descritos no *Supplier's Guide*.
- ***Cloud Software*:** Aplicações acessadas pela *internet* e hospedadas na nuvem.

- ***Cloud Support*:** Serviços de suporte a usuários em atividades de parametrização, ajustes e manutenção de serviços em nuvem.

As agências governamentais e os fornecedores devem observar as publicações e orientações do *Government Digital Service – GDS*. De acordo com o GDS, fornecedores devem trabalhar no sentido de ajudar o governo a projetar, construir e comprar melhores tecnologias.

Com esse objetivo, o GDS publica o *Technology Code of Practice* – TCP, que contém os critérios para a ajuda citada.

Da mesma forma, as agências governamentais devem observar o TCP para saber das orientações com relação às compras e devem pesquisar no *Digital Marketplace* o que há de disponível para atender às necessidades levantadas. Antes de iniciar um projeto de serviços em nuvem, a agência deve submetê-lo ao GDS para aprovação, que inclui o registro em uma área do governo que reserva recursos financeiros para tal.

Ao cadastrar o projeto no GDS, a agência interessada deve atentar para os seguintes aspectos:

- Definir as necessidades do usuário.
- Definir a acessibilidade da solução por parte de usuários.
- Considerar que o sistema/serviço deve adotar soluções abertas, preferencialmente.
- Adotar padrões abertos.
- Usar conceitos do *Cloud First* americano.
- Cuidar para que sistemas e dados envolvidos sejam mantidos em nível apropriado de segurança.
- Garantir que os direitos e a privacidade dos cidadãos estão respeitados e protegidos no sistema proposto.
- Evitar esforços duplicados, dividindo e reusando recursos.

- Usar e integrar o serviço/sistema proposto às tecnologias existentes, à infraestrutura e aos processos da agência.
- Fazer melhor uso dos dados, evitando sua duplicação.
- Definir a estratégia de compra, demonstrando que foram observados aspetos técnicos e comerciais.
- Ser aderente aos padrões *Digital Service Standard* do governo britânico, de forma a verificar se o serviço proposto é bom o suficiente para uso público.

O modelo inglês, desta forma, tem uma abordagem diferente do modelo americano, considerando que tem uma série de documentos e procedimentos que objetivam uniformizar, desde o início da implantação de nuvem pelo governo, um padrão de compra e de venda dos serviços, facilitando sobremaneira as ações de implantação de serviços em nuvem nas agências governamentais.

Em fevereiro de 2013, o GDS publicou o documento *Government Cloud First Policy*, reiterando às agências governamentais a importância de considerar o uso de nuvem como primeira alternativa e orientando que, para os casos em que soluções em nuvem não forem escolhidas, deve ser comprovado que a solução alternativa oferece mais valor ao dinheiro pago.

Ainda com relação ao modelo inglês, em *whitepaper* publicado em 2018, a empresa *Solarwind* divulgou pesquisa junto às agências inglesas, a fim de apurar o nível de implantação de soluções em nuvem em resposta às orientações do *G-Cloud*, submetendo um *FOI – Freedom of Information* (formulário para coleta de informações). Os aspectos mais relevantes observados foram:

- A maior parte das agências e demais entidades do governo britânico, incluindo a *National Health Service – NHS*, tem conhecimento do *G-Cloud*.

- Os principais impeditivos citados para a implantação de soluções em nuvem foram: segurança, conformidade, recursos financeiros, legado tecnológico e dependência de fornecedores.
- Outro foco restritivo citado é a dificuldade de monitoração de serviços em nuvem pública, considerando a nuvem como parte da infraestrutura da agência governamental. As agências e o NHS utilizam, em média, quatro ou mais ferramentas distintas para monitorar recursos em nuvem. Todos citam que não é possível a monitoração de todos os recursos usando-se somente uma ferramenta, e a solução neste caso é utilizar diferentes ferramentas para cobrir a necessidade total de monitoração.
- Os principais desafios colocados pelas agências e pelo NHS foram: uniformização de ferramentas de monitoração e gerenciamento de recursos em nuvem, falta de controle de performance dos recursos e mecanismos de proteção e segurança para ambientes em nuvem. A ausência de ferramentas consistentes para gerenciar toda a infraestrutura é fator significante para a falta de confiança em relação aos benefícios do uso de serviços em nuvem pública.
- O governo britânico precisa de ferramentas para monitoração e gerenciamento que atendam às características de nuvem e da sua infraestrutura, incluindo tecnologia legada, possibilitando uma visão geral de todos os recursos de TIC. Com isso, pode ser avaliado o *Return of Investiment* – ROI.

Processo de Adoção de Nuvem pelo Governo Canadense

A partir de 2011, os principais serviços de TI do governo canadense (*data centers*, redes e serviço de correio eletrônico, por exemplo) passaram a ficar sob gerência do órgão *Shared Services*

Canada (SSC). Desde então, várias orientações vêm sendo publicadas pelo SSC no sentido de orientar as agências federais e os programas de governo a oferecer aos usuários do serviço público canadense soluções que envolvam tecnologias modernas e robustas.

No ano de 2014, o governo canadense realizou uma consulta a mais de 60 organizações da indústria de TI do país, convocando os potenciais fornecedores para participar de reuniões com representantes do governo. Toda a realimentação dada pela indústria e pelos fornecedores foi analisada e considerada na elaboração de novas versões da estratégia de implantação de serviços em nuvem para o governo canadense.

Como orientação básica, um primeiro conjunto de serviços em nuvem foi utilizado para tratar de dados públicos, tais como informações gerais e dados abertos de agências federais e grandes conjuntos de dados gerados pela comunidade científica. O uso de dados não sensíveis foi uma estratégia de fomento ao aprendizado, com riscos minimizados.

Atualmente, os clientes do SSC na área federal já dispõem de exemplos de uso de processamento, gerenciamento e armazenamento de dados em nuvem. Mais de 20 contratos foram adjudicados até meados de 2018, com constante previsão de crescimento.

Um aspecto bastante interessante é a operação conjunta do SSC com o *Treasure Board of Canada Secretariat* para atuarem como *cloud broker*, com o objetivo de:

- Trabalhar com departamentos e agências federais no sentido de ajudá-los na obtenção de soluções adequadas para as suas necessidades.
- Prover operações e segurança consistentes.
- Prover a administração do ambiente em nuvem.
- Alavancar o poder de compra do governo canadense.

O governo canadense publicou o Plano Estratégico para Gestão e Tecnologia da Informação para o período de 2017 a 2021 [20], referendando a *Cloud Adoption Strategy* para todas as agências de governo. A última versão do *Cloud Adoption Strategy* do governo canadense foi atualizada em 2018, já com acesso por meio do sítio do *Treasure Board of Canada Secretariat*.

Assim como na documentação publicada em outros países, a *Cloud Adoption Strategy* do governo canadense destaca nos capítulos iniciais as vantagens de adoção de serviços em nuvem, tais como: desempenho melhorado dos serviços, segurança, inovação, agilidade na obtenção e entrega de recursos de TI e escalabilidade, além de definir como público-alvo:

- Supervisores de serviços de TI no governo.
- Gerentes de programas governamentais que utilizam serviços de TI ou que fornecem serviços de TI.
- Provedores na área de serviços em nuvem que atendem ao governo canadense.

O documento define a estratégia de implantação de serviços em nuvem para órgãos públicos com os seguintes objetivos:

- Adotar soluções em nuvem como opção preferencial para a entrega de serviços de TI e adotar nuvem pública como opção preferencial para implantação de soluções em nuvem no governo.
- Resguardar dados e a privacidade de cidadãos canadenses.
- Definir um conjunto de princípios para orientar CIOs na adoção de soluções em nuvem.
- Dar uma visão que permita nuvem comunitária no âmbito do governo canadense, de forma a aproximar os potenciais

compradores de serviços em nuvem no governo canadense dos provedores deste tipo de serviço, com funções de "*broker*" e avaliação de segurança sendo desempenhados pelo governo canadense.

A estratégia de implantação do governo canadense vem sendo orientada de maneira a garantir evoluções gradativas. Neste sentido, o governo publicou em 2017 documentos orientadores com aspectos sobre segurança no uso de serviços comerciais de nuvem (*Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice*) e aspectos sobre controle, acesso e propriedade de dados de governo na nuvem (*Direction for Electronic Data Residency*).

Este aspecto de constante evolução alterou alguns paradigmas das versões iniciais das orientações do governo canadense. A estratégia de implantação de serviços em nuvem se transformou em "*cloud first strategy*", definindo a nuvem como meio preferencial de entrega de serviços de TI, porém adotando a nuvem pública como solução preferencial para a implantação da nuvem do respectivo órgão federal.

Atualmente, o governo canadense define que os órgãos *Public Services and Procurement Canada – PSPC* (órgão central de compras) e *Shared Services Canada – SSC* (órgão responsável pelos serviços digitais no país) atuem como colaboradores nos processos de aquisição de serviços em nuvem por parte das agências e dos órgãos federais.

A versão mais recente do *Cloud Adoption Strategy* estabelece três grandes objetivos:

- Apoiar o balanceamento de ofertas de serviços de TI de acordo com a demanda.
- Gerenciar os riscos de forma consistente.
- Preparar a força de trabalho para atuar no ambiente em nuvem.

Apoiar o balanceamento de ofertas de serviços de TI de acordo com a demanda

De acordo com o governo canadense, a demanda de serviços de TI no país tem superado a oferta desses serviços. Isso faz com que haja uma constante necessidade de novos recursos e muitas vezes a modernização de plataformas já instaladas. O uso de ambiente em nuvem para solução das necessidades de serviços digitais permite ao governo canadense balancear constantemente a oferta de recursos de TI de acordo com a demanda.

Gerenciar riscos de forma consistente

Os riscos em ambientes em nuvem são similares aos enfrentados em ambientes de TI. O *Cloud Adoption Strategy* procura descrever de que forma esses riscos podem ser gerenciados de forma consistente, permitindo aos órgãos governamentais flexibilidade para atuarem de acordo com suas tolerâncias a riscos.

Preparar a força de trabalho para atuar no ambiente em nuvem

A agilidade em adotar soluções em nuvem pelo governo canadense está diretamente vinculada a quão rápido seus profissionais de TI podem absorver as habilidades neste ambiente. O governo canadense deixa claro que, para adotar a solução de nuvem para os serviços de TI oferecidos aos cidadãos, é necessário desenvolver talentos e habilitar seus profissionais de TI nessa área.

Modelos de Implantação do *Cloud Adoption Strategy*

O *Cloud Adoption Strategy* apresenta os modelos de implantação de nuvem (pública ou privada), considera o uso de soluções onde

não é possível adotar nuvem e, por fim, considera o uso de ambiente hibrido, onde parte dos serviços é oferecida em ambiente de nuvem pública e a outra parte dos serviços é oferecida utilizando ambiente em nuvem privada, solução apropriada quando se tem um ambiente legado que não pode ser migrado para nuvem.

Da mesma forma que nos documentos dos governos americano e inglês, a documentação do *Cloud First* no documento *Cloud Adoption Strategy* apresenta os modelos de serviços em nuvem (*SaaS – Software as a Service, PaaS – Platform as a Service e IaaS – Infrastructure as a Service*).

As orientações indicam que o governo canadense deve atuar em colaboração com os provedores no sentido de definir aspectos de segurança e níveis de confiabilidade. Cabe aos órgãos federais manter sua responsabilidade pela confidencialidade, integridade e disponibilidade dos serviços de TI e informações relacionadas que os provedores tratam. Neste contexto, a orientação do governo canadense estabelece que cabe a cada agência e departamento federal o gerenciamento de riscos levando em conta a integração de serviços em nuvem com seus respectivos ambientes de TI.

O governo canadense mantém diferentes perfis de controle para diferentes categorias de serviços em nuvem, que podem ser adaptados para cada departamento ou agência federal. Neste sentido, o governo canadense criou certificações de segurança em nuvem de forma a dar transparência para as práticas adotadas por provedores de serviços em nuvem. As certificações são conduzidas por terceiros credenciados, que devem seguir metodologias estabelecidas. Com isso, os departamentos e as agências usuárias de serviços em nuvem podem se assegurar de que os requisitos mínimos de segurança são atendidos pelos provedores.

Padrões internacionais reconhecidos, como ISO 27001, *FedRAMP* (U.*S. Federal Risk and Authorization Management Program*) e outros, são adotados para a elaboração das certificações. Com isso, os provedores

podem fazer uso desses procedimentos para comprovar ao governo canadense as evidências de atendimento a padrões de segurança.

Estabelecidas essas diretrizes, a implantação de serviços em nuvem deve observar os seguintes princípios:

- Identificar os serviços em nuvem como a principal opção de entrega de serviços quando houver o planejamento de investimentos em TI e iniciativas correlatas.
- Selecionar, com o apoio de documentação publicada pelo próprio governo canadense, os modelos preferenciais de implantação de serviços, observando a seguinte prioridade: nuvem pública, nuvem híbrida, nuvem privada e não uso de nuvem.
- Selecionar o modelo de serviço de nuvem, observando a seguinte prioridade: SaaS, PaaS e, por fim, IaaS.
- Observar a documentação publicada pelo governo canadense sobre riscos de segurança: *GC Cloud Security Risk Management Approach and Procedures*.
- Direcionar ações para o uso seguro de serviços de nuvem comercial: *Security Policy Implementation Notice (SPIN)*.
- Identificar situações particulares nos perfis de segurança, desenvolvendo ações de mitigação de riscos em conjunto com a área de segurança do governo canadense.
- Garantir acesso continuado a dados sensíveis, adotando soluções aderentes ao documento *GC Direction for Electronic Data Residency*.
- Garantir a continuidade do negócio e o gerenciamento adequado de riscos, desenvolvendo estratégias apropriadas de saída do serviço de nuvem antes da adoção do serviço.
- Considerar a portabilidade e a interoperabilidade dos

serviços por ocasião da elaboração de projetos de soluções baseadas em nuvem.

Dois aspectos importantes devem ser destacados na estratégia canadense para a implantação de serviços em nuvem em seu governo federal:

- Orientação para os *CIOs* estarem atentos à criação de uma força de trabalho especializada neste segmento, com constante capacitação de todo o pessoal, inclusive dos próprios *CIOs*.
- Criação de centros de excelência para prestar apoio aos departamentos e às agências no processo de implantação de serviços em nuvem. O objetivo é colocar especialistas do governo canadense nesses centros para prestar apoio aos projetos de implantação de serviços em nuvem nos órgãos.

A atuação do *Treasure Board of Canada Secretariat (TBS)* e do *Shared Service Canada (SSC)* é bem definida nas orientações publicadas pelo governo canadense, destacando que o SSC assume o papel de *broker* junto aos órgãos federais nas contratações de serviços em nuvem.

Nesta mesma linha de atribuição clara de responsabilidades, o governo canadense coloca o *Public Services and Procurement Canada (PSPC)*, órgão responsável por processos de compra e contratações, à disposição para atuar neste segmento em apoio aos departamentos e às agências federais, que, por sua vez, são responsáveis principalmente pelos seguintes aspectos:

- Segurança no ambiente de nuvem.
- Definição de papéis e responsabilidades para nuvem.
- Modelo de implantação e de serviço.

- Estratégia de saída de um contrato vigente.
- Atenção à continuidade do negócio.

As ações previstas no documento de orientação para implantação de serviços em nuvem do governo canadense em sua última versão (2018) apontam a criação de uma comunidade no serviço público para tratar de serviços em nuvem, denominada *Canadian Public Sector Community Cloud* (CPSCC).

O objetivo do CPSCC é disponibilizar um *framework* de serviços aos órgãos públicos, incluindo um *marketplace*, ideia semelhante ao que é implementado pelo governo britânico.

A criação do CPSCC objetiva os seguintes benefícios:

- Otimização na busca de soluções em nuvem, indicando fornecedores qualificados e soluções credenciadas pelo governo canadense.
- Economia de escala nas contratações de serviços em nuvem.
- Incentivo à colaboração entre agências de governo (compartilhamento de recursos, inclusive dados, em diferentes níveis).
- Controle adequado do crescimento do ambiente de nuvem no governo federal.

São considerados entidades públicas no Canadá, ou seja, potenciais compradores de serviços em nuvem: o governo federal, governos de províncias e territoriais, entidades municipais, universidades, escolas e hospitais. Isso aumenta significativamente o espectro de clientes e a abrangência das recomendações do governo canadense.

Em linha geral, o governo canadense tem uma atuação mais centralizadora, se comparado ao governo americano e inglês, visto que o *Shared Services Canada* (SSC) é responsável por controlar o

fornecimento de diversos serviços digitais e também por atuar como *broker* na contratação de serviços em nuvem. Considerando-se as dimensões do país e a estrutura organizacional já existente, tal estratégia torna-se mais conveniente quando se objetiva disciplinar a contratação de serviços em nuvem.

Processos de Adoção de Nuvem pelo Governo da Estônia

Um outro exemplo de implementação de nuvem governamental foi realizado pela Estônia, que demonstrou as possibilidades de uso da tecnologia para suportar um governo eletrônico de fato, no qual as fronteiras deixaram de ser os limites do país.

Para Taavi Kotka e Innar Liiv, da universidade estoniana Tallinn University of Technology, a situação e as peculiaridades da nuvem governamental da Estônia – um dos países de referência em governo digital e serviços digitais para o cidadão – requeriam requisitos distintos dos observados em outros países europeus, por conta do alto desenvolvimento digital da sociedade estoniana [21]. De fato, o governo da Estônia já vinha utilizando serviços oferecidos por provedores de nuvens públicas em larga escala desde 2009, quando lançou o *website* nacional de turismo *visitEstonia.com*, utilizando-se da nuvem da *Amazon*. Ocorre que, em 2013, o governo da Estônia resolveu realizar uma análise do uso de recursos de seus *data centers*, que concluiu que as salas de servidores espalhadas entre vários ministérios e edifícios precisavam ser consolidadas em centros mais eficientes, que atendessem a padrões de segurança estabelecidos. Esse estudo levou em consideração:

- A arquitetura de TI distribuída do estado deve permanecer – por exemplo, cada ministério/agência deve manter o papel de cliente e titular do orçamento.

- A possibilidade de livre concorrência deve permanecer.
- A qualidade dos serviços de TIC fornecidos aos ministérios/agências deve melhorar.

Dessa forma, a conclusão acabou por levar ao entendimento de que era necessária a construção de uma nuvem própria para abrigar os serviços do governo. Motivos não faltavam:

1. Era necessária a eliminação da fragmentação do parque de servidores físicos.
2. Havia a necessidade de garantir a denominada defesa cibernética de "*monumentos digitais*" *(sites* com *status* simbólico como o President.ee, o *site* do Ministério da Defesa etc.). Embora esses *sites* contenham apenas informações públicas, isso representa o simbolismo de uma nação digital que precisa ser defendida de ataques cibernéticos.
3. Era necessário que se garantissem a continuidade digital da Estônia e o seu funcionamento como Estado em qualquer situação ou emergência.
4. Era necessário garantir a confiabilidade e a qualidade dos serviços "*transfronteiriços*", porque a Estônia começava a emitir *ID digitais* para não residentes e a construir "*um Estado sem fronteiras*".
5. Soluções flexíveis e rentáveis para municípios locais precisavam ser desenvolvidas.

A implementação da política de "*governo sem papel*" levou a Estônia a uma situação em que registros essenciais, como, por exemplo, o do cadastro predial (que contém informações sobre a propriedade da terra), existissem apenas em meio digital e possuíssem valor apenas

nesse formato. A ameaça de ataques cibernéticos e uma situação na qual a Estônia fosse ocupada e perdesse sua independência acarretaram uma necessidade especial para a estratégia de adoção de nuvem governamental: a garantia da continuidade digital *independentemente das condições prevalecentes no território da Estônia*, ou seja, mais do que a preservação de conjuntos de dados críticos e soluções de TI no território da Estônia, a nuvem deveria prover uma solução na qual o Estado poderia *não ter controle sobre os data centers* localizados em seu próprio território e até mesmo possibilitar a operação de alguns serviços fora das fronteiras da Estônia.

Dessa forma, foram utilizados *data centers* dentro do país, formando uma nuvem governamental privada, cuja maior justificativa era calcada na impossibilidade da manutenção de informações confidenciais em nuvem pública internacional, devido a danos substanciais e riscos de reputação associados a vazamentos de dados.

No entanto, a utilização dessa estrutura não é mandatória. Por meio da seleção de conteúdo, o governo decide o que pode ser hospedado em uma nuvem pública e o que somente pode ser utilizado na nuvem governamental. *Sites* como President.ee, Valitsus.ee (Casa Civil) e o *website* do Ministro da Defesa, entre outros, estão em uma nuvem pública internacional. As informações nesses *sites* não são confidenciais, o que deixa o Estado mais focado na proteção de dados mais valiosos para a nação.

Outro conceito interessante criado pela Estônia refere-se à Embaixada de Dados. Para possibilitar o requisito do funcionamento mesmo em caso de ataques cibernéticos ao país, a Estônia iniciou tratativas diplomáticas com alguns países para que lhe seja possibilitada a criação de *data centers* fora do país e que possam operar com controle total da Estônia, possibilitando que o tráfego possa ser redirecionado e que o país funcione mesmo que *fora de suas fronteiras*.

Assim, temos na Estônia um modelo conceitual de nuvem governamental que se baseia em três camadas interdependentes:

1. Soluções de nuvem privada no próprio território da Estônia, que demandam a construção de *data centers* primários e secundários, envolvendo recursos do setor privado para pelo menos um terço de toda a capacidade necessária.
2. Serviços de nuvem pública fornecidos por grandes corporações multinacionais e usados com a consciência do risco de que as informações hospedadas possam vazar para terceiros.
3. Uma rede de Embaixada de Dados, composta por salas de servidores construídas fisicamente nas embaixadas estrangeiras, hospedados em *data centers* de estados amigáveis à Estônia.

Cada uma das camadas provê uma das características necessárias para implementar a estratégia de governo digital do país, trazendo consigo conceitos inovadores da utilização da tecnologia de nuvem computacional que podem ser adaptados à realidade de qualquer nação, incluindo o Brasil.

Analisando as experiências de outros países

As iniciativas de implantação de serviços em nuvem em diferentes governos são precedidas pela disseminação de orientações por parte dos respectivos governos.

Neste capítulo foram apresentados aspectos relevantes de quatro diferentes governos: Estados Unidos, Reino Unido, Canadá e Estônia. Vários outros países também possuem sua documentação e o respectivo processo de implantação de serviços em nuvem para seus órgãos públicos, mas a análise dos quatro exemplos mostra

alguns pontos de convergência e outros pontos que revelam qual é a disposição dos governos em ter maior ou menor grau de tutoria sobre os serviços em nuvem.

Como pontos em comum fica clara a disposição desses governos em estabelecer documentos de caráter orientador, em todos os níveis, para a implantação de serviços em nuvem. A atuação em oferecer soluções já customizadas ou pelo menos já credenciadas pode ser observada com grande maturidade no *G-Cloud* do governo britânico, sendo que o governo canadense aponta para o mesmo sentido ao prever a criação de um *marketplace* local para soluções em nuvem.

Destaque para o governo canadense, ao assumir a função de *broker* junto aos provedores nesse início de implantação de serviços de nuvem.

O governo americano, em suas orientações, procura ser objetivo em todos os aspectos, desde o planejamento até a seleção da solução, porém não oferece aos órgãos públicos um cardápio de soluções ou mesmo uma lista de provedores e especialistas previamente credenciados. A estrutura de *marketplace* do governo britânico já oferece as soluções em todos os níveis, incluindo especialistas e consultores, já aptos a serem contratados, e esse mesmo tipo de abordagem está sendo planejado no Canadá.

No caso específico do Canadá, o governo assume diretamente a responsabilidade de serviços digitais em diferentes níveis. Trata-se de uma estratégia interessante do ponto de vista de governança dos serviços digitais, porém pode ser um agente complicador se as dimensões do país forem muito maiores.

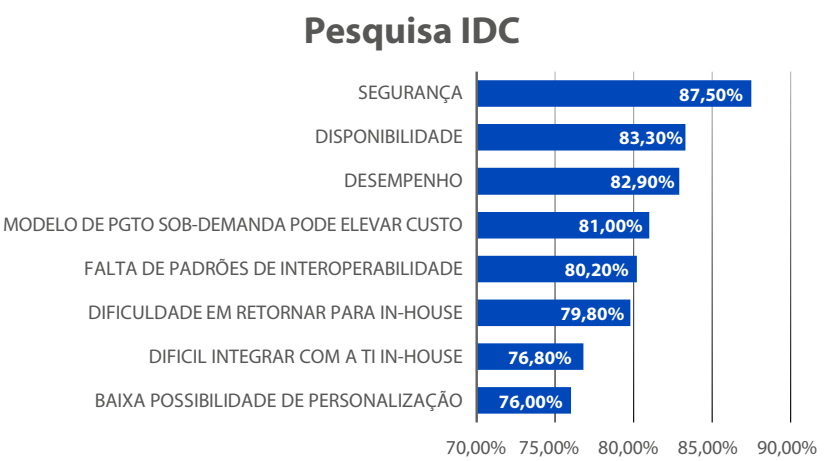
Por fim, todas as orientações, sem exceção, destacam a necessidade de capacitação das equipes de TI de seus respectivos governos, para que possam atuar de forma eficiente no segmento de serviços em nuvem.

DESMISTIFICANDO A ADOÇÃO DE SERVIÇOS EM NUVEM

Várias pesquisas demonstram um conjunto de preocupações que inibem os gestores na adoção de serviços em nuvem computacional, mesmo cientes dos benefícios que a migração traz para a organização.

No âmbito internacional, em pesquisa realizada no ano de 2009 pelo IDC [9], com a participação de 244 executivos de TI, foram levantados os principais desafios para a adoção da tecnologia de serviços em nuvem.

Figura 5. Pesquisa sobre os principais desafios para a adoção de nuvem computacional[9]



Conduzida pelo IDG (*International Data Group*) [22], em outra pesquisa com 550 executivos de TI de empresas que já adotaram ou pretendem adotar a tecnologia de nuvem computacional nos próximos três anos, foram identificadas cinco principais preocupações, tendo o *lock-in* do provedor como a mais pontuada.

No âmbito nacional e especificamente com foco na Administração Pública brasileira, uma pesquisa realizada pelo IBGP em 2018, com 44 dirigentes e assessores de órgãos de governos estaduais e do federal, identificou os principais problemas que inibiriam a adoção de serviços em nuvem computacional.

De acordo com essa pesquisa, os seis pontos de preocupação mais relevantes que inibem os gestores na adoção de serviços em nuvem são:

- Confidencialidade dos dados na nuvem pública – segurança.
- Gargalos de transferência de dados para a nuvem pública – desempenho.
- Interrupção de serviços e descontinuidade dos negócios – disponibilidade.
- Dificuldades na elaboração do termo de referência – conformidade.
- Baixa cultura organizacional para a adoção de nuvem – legitimidade.
- Imprevisibilidade do desempenho da nuvem pública – riscos.

Na sequência, vamos analisar cada um dos pontos de preocupação para, à luz das normas e dos padrões internacionais e de artigos profissionais e acadêmicos, esclarecer o que de fato seria um aspecto inibidor, qual seria a melhor prática para mitigar tal risco e o que seria considerado um "mito", muitas vezes gerado pela falta de conhecimento das tecnologias que envolvem serviços em nuvem computacional.

Figura 6. Principais preocupações com a adoção de tecnologias de nuvem computacional [22]

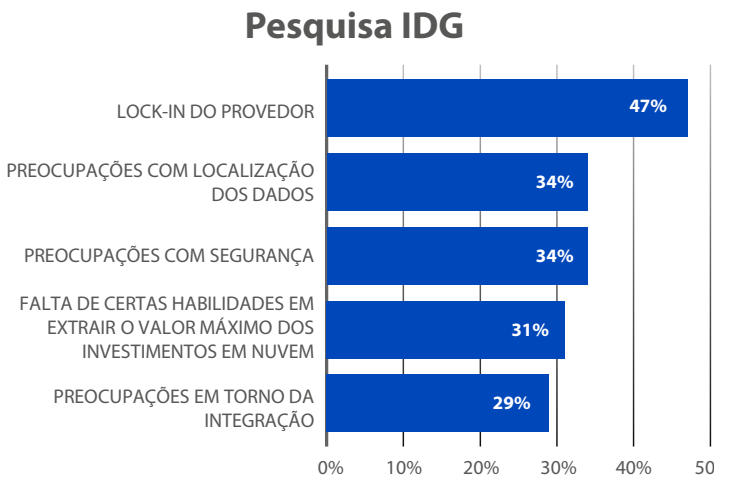
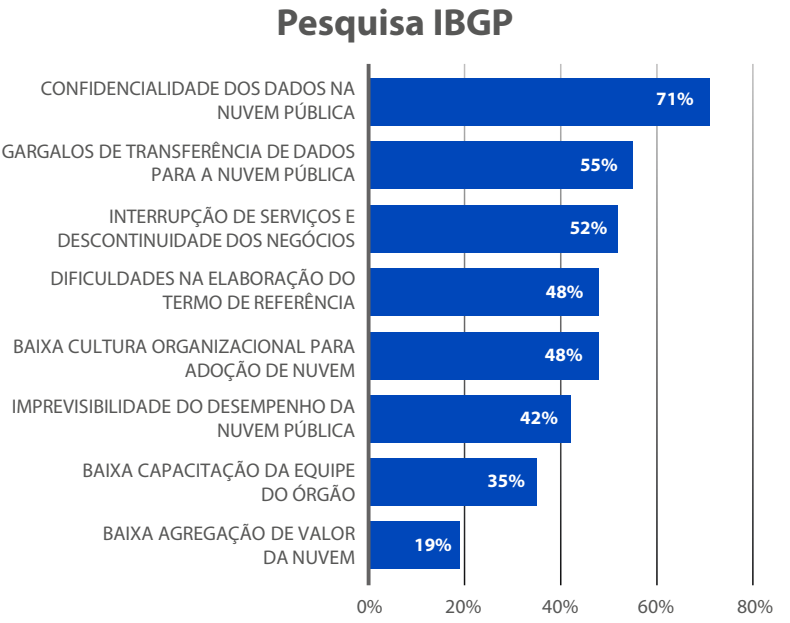


Figura 7. Principais problemas que inibiriam a adoção de serviços em nuvem



Confidencialidade dos Dados na Nuvem Pública – Segurança

Fica claro, pelas pesquisas, que os aspectos envolvendo segurança, incluindo preocupações com o vazamento de informações sigilosas, confidenciais ou estratégicas da organização, figuram como a principal justificativa para a rejeição ao uso da computação em nuvem.

Esse fenômeno não é novo, pois em várias oportunidades, em que uma nova tecnologia despontava como supridora de solução para a ineficiência das organizações, surge uma celeuma que inibe a inovação. Foi assim com a contratação de serviços de "fábrica de *software*", em que se discutiram os riscos envolvendo a segurança do código implementado por terceiros, com possibilidade de introdução de trechos maliciosos ou perda do conhecimento em casa de mudança de fornecedor. Nessa época, muito se falou sobre "*open source iniciative*", de que as organizações somente utilizassem *software* de código aberto, para evitar ações malignas ou interferências de empresas multinacionais nas atividades das organizações dependentes do uso de licenças de *software* proprietárias, como sistemas operacionais de computadores, *software* de banco de dados, suíte de aplicativos para escritório, entre outros. Se retroagirmos para o final do século passado, quando houve privatização de setor de Telecomunicações (1997), havia um alvoroço sobre o sigilo das comunicações (que seriam operadas por empresas privadas) e sobre a falta de segurança das redes de comunicação de dados.

Atualmente, não obstante a maioria dos órgãos terceirizar o processamento da folha de pagamento e muitos utilizarem serviços externos de *e-mail*, nos quais trocam informações confidenciais e estratégicas, não tem sido fácil convencer a alta administração, os gestores das áreas de negócios e, principalmente, os chefes de TI das mais diversas organizações de que os avanços na utilização de serviços em nuvem

superam em muito qualquer problema que esse risco venha a trazer.

O que muitas vezes não se analisa é que vários dos riscos que são frequentemente associados à segurança da informação na utilização de computação em nuvem já são realidade nos ambientes terceirizados da maior parte dos órgãos públicos e que eles também já foram mapeados.

A ACM – *Association for Computing Machinery* [23]– constatou que muitas das questões de segurança envolvidas na proteção de nuvens contra ameaças externas são semelhantes àquelas já enfrentadas por grandes *data centers*. Na nuvem, essa responsabilidade é dividida entre o usuário da nuvem, o fornecedor da nuvem e quaisquer fornecedores terceiros dos quais os usuários dependam para configurações de *softwares* sensíveis à segurança. Nos ambientes de *data centers* comumente encontrados nas organizações, os NOCs (*Network Operations Centers*) são operados por empresas terceirizadas, cujos funcionários obedecem a um protocolo restrito direcionados por cláusulas contratuais e SLAs fortemente calcados na segurança da informação a ser protegida, que dividem – com os responsáveis pelas unidades de infraestrutura, com os fornecedores de *softwares* e com servidores/usuários dos serviços computacionais dos órgãos – as mesmas responsabilidades pela segurança da informação institucional. Não há diferença, pois são semelhantes às estruturas nas quais repousam as recomendações sobre segurança da informação para quem já faz uso de contratos de terceirização.

O ICO (*Information Commissioner's Office*) apresenta compilações estatísticas trimestrais sobre as principais causas de incidentes de segurança de dados relatados no mundo. No último trimestre de 2017 [24], quatro das cinco principais causas, nos casos que a ICO registrou, envolviam erros humanos e falhas de processos, como: perda ou roubo de documentos, dados enviados por fax para destinatários incorretos, dados enviados por *e-mail* para destinatários incorretos, acesso a

páginas da *web* inseguras (*hacking*) e perda ou roubo de dispositivos não criptografados.

O IDG publicou, em agosto de 2018 [25], reportagem na qual são listadas recomendações importantes de ações para a proteção do ambiente tecnológico contra vazamento de dados, como registro e monitoramento, configurações do ambiente de rede, educação e configurações de direitos de acesso, em que se recomendam técnicas e ferramental que permitam leitura de *logs*, maior robustez dos sistemas de segurança, preocupações com o entendimento das ações dos usuários finais com a segurança da informação utilizada e um controle mais sistematizado de acesso privilegiado de usuários a determinados dados.

Novamente, observa-se que as abordagens recomendadas para as falhas de segurança são válidas para qualquer tipo de implementação de infraestrutura e devem constar de quaisquer contratos e SLAs que envolvam o acesso à informação do órgão, sendo essencial que se defina bem o papel que os usuários e os provedores de serviço terão em relação à segurança para que o risco de vazamento de informação possa ser gerenciado.

Outro aspecto que as organizações consumidoras de serviços em nuvem devem observar é a necessidade da criação de mecanismos para se "proteger" do provedor. Por controlar a "camada inferior" da pilha de *software*, o provedor pode "contornar" as técnicas de segurança conhecidas. Nesse caso, a organização que necessite garantir o sigilo de suas informações de maneira mais pontual deve mitigar o risco utilizando-se de tecnologias como a criptografia ou *tokenização* para tratar de preocupações de segurança de uma forma mais técnica, reduzindo a possibilidade de que eventuais vazamentos possam trazer um risco imediato a informações classificadas pelo órgão. Hoje, praticamente todos os provedores de nuvem têm o serviço de criptografia incluído em seu portfólio, das

mais diversas maneiras, como a proteção do canal de comunicação ou a criptografia de dados do lado do provedor.

A Empresa de Consultoria Gartner, em seu relatório de 2018, aborda pesquisa sobre vários aspectos da segurança na nuvem, com recomendações para o desenvolvimento de uma estratégia para migração, além de previsões para o futuro da segurança em plataformas de nuvem [26]. Segundo a empresa, o desafio não será a segurança na nuvem, mas as políticas e ferramentas para a segurança e o controle da própria tecnologia de uso da nuvem. Na maioria dos casos, será o usuário – e não o provedor de nuvem – que falhará ao gerenciar os controles utilizados para proteger os dados da organização.

A Gartner prevê ainda que, em 2022, pelo menos 95% das falhas de segurança na nuvem serão falhas do usuário contratante e sugere aos CIOs que mudem a recorrente pergunta sobre segurança ("a nuvem é segura?") para uma questão mais apropriada ("estou usando a nuvem de forma segura?") [26]. Segundo Jay Heiser, vice-presidente do Departamento de Pesquisa da Gartner, "medos exagerados podem resultar em perda de oportunidades e gastos inapropriados".

Como alertava Peter Drucker, "existem dois tipos de riscos: aqueles que não podemos nos dar ao luxo de correr e aqueles que não podemos deixar de correr".

Os riscos relacionados à segurança da informação estarão sempre presentes no uso de qualquer serviço computacional. Aprender a gerenciá-los e buscar as melhores práticas faz parte do dia a dia de qualquer organização moderna e eles não deveriam se tornar empecilhos para o atingimento dos objetivos e avanços rumo à excelência na prestação do serviço, em especial quando nos referimos aos oferecidos à nossa sociedade.

A Questão da Classificação da Informação na Legislação Brasileira

Nas organizações públicas brasileiras, um conjunto de leis, normas e acórdãos foi publicado para garantir a transparência, segurança e privacidade das informações tratadas no âmbito dos órgãos e das entidades do setor público, mas que, infelizmente, criou um ambiente de insegurança que tem inibido os gestores públicos a adotar serviços em nuvem.

O principal aspecto controverso é a classificação das informações existentes nas organizações públicas, de modo a se discernir o que seriam informações públicas e informações sigilosas. A LAI – Lei de Acesso à Informação (Lei nº 12.527/2011)[27], que assegura o direito fundamental de acesso à informação, ressalta no art. 3º "a publicidade como preceito geral e o sigilo como exceção". Então, está claro que as informações sob a guarda do Estado são públicas, devendo o acesso a elas ser restrito apenas em casos específicos e por tempo determinado. As exceções previstas na LAI[27] são:

- Informação sigilosa – aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.
- Informação pessoal – aquela relacionada à pessoa natural identificada ou identificável.

Também são abarcadas pelo sigilo as informações protegidas de acesso com base em outras leis, como os sigilos bancário, fiscal e industrial.

Uma vez que ficou esclarecido que a "transparência" é a regra e o "sigilo" é uma exceção, recorre-se ao art. 23, da Lei de Acesso a Informação[27], para identificar o que deve ser classificado como sigiloso no âmbito das organizações públicas brasileiras:

> Art. 23. São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam:
>
> I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;
>
> II - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais;
>
> III - pôr em risco a vida, a segurança ou a saúde da população;
>
> IV - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;
>
> V - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;
>
> VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;
>
> VII - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou
>
> VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.

Por outro lado, para clara identificação do que são as informações pessoais protegidas pelo sigilo da LAI[27], recorre-se à recente Lei Geral de Proteção de Dados (Lei nº 13.709/2018)[28], que determina a necessidade de proteção dos "dados pessoais" e dos "dados pessoais sensíveis", cujo significado é explicitado no art. 5º da Lei:

> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; [...].

Não há uma estatística publicada sobre o percentual de dados considerados sigilosos, mas há declarações de autoridades do governo federal que estimam serem considerados sigilosos apenas 5% dos dados armazenados nos *data centers* do governo.

A rotulação de dados como sigilosos é uma necessidade que independe do ambiente onde estejam armazenados – em nuvem ou *on-premises*. O cumprimento da lei indica o dever de providenciar a rotulação pelos órgãos/entidades do governo.

Por outro lado, sem ânimo de querer simplificar o que é sabidamente complexo, a falta de classificação dos dados não seria um impeditivo para a adoção de serviços em nuvem computacional – tanto que governos de países desenvolvidos e altamente preocupados com a segurança de suas informações já adotaram os serviços em nuvem pública ou híbrida, de modo a auferir todos os benefícios que provedores de nuvem do setor privado fornecem, incluindo menores preços.

Mesmo importantes órgãos do governo federal brasileiro também contrataram serviços de nuvem pública, tais como: TCU – Tribunal de Contas da União, MPF – Ministério Público Federal e Ministério do Planejamento, Desenvolvimento e Gestão (recentemente incorporado ao Ministério da Economia).

Para mitigarem os riscos de vazamento de informações sigilosas ou pessoais, as boas práticas indicam que não sejam migrados para

o ambiente de nuvem sistemas ou soluções que manipulem esses tipos de informação sem uma adequada solução de criptografia.

Ainda haverá um imenso conjunto de outras soluções migráveis que, certamente, poderão garantir um ganho em eficiência, eficácia, efetividade e economicidade para a administração pública brasileira. Corrobora essa afirmação o relatório-base do Acórdão TCU nº 1739/2015-Plenário[29], que levantou os riscos relevantes em contratações de serviços de tecnologia da informação, que registra as vantagens dos serviços baseados em nuvem:

> Ainda voltando-se ao tema da segurança da informação, as maciças concentrações de recursos e dados nos provedores de computação em nuvem podem representar um alvo atraente para possíveis atacantes. Porém, as defesas baseadas em nuvem tendem a ser mais robustas, escaláveis, eficientes e baratas. Há também o argumento de que a segurança torna-se fortalecida à medida que novos clientes aderem à nuvem em razão do ganho de escala. Na realidade atual, por exemplo, muitas organizações conseguem publicar rapidamente novas aplicações web utilizando sua própria infraestrutura, mas com poucos controles de segurança e de auditoria. A transferência destas soluções ou aplicações para um serviço de nuvem significa consolidar clientes dentro de uma infraestrutura que é presumidamente mantida por especialistas em segurança, com recursos consideráveis dedicados à segurança e à privacidade, pois estes são fatores fundamentais para o sucesso do provedor [grifo nosso].

Análise de Conformidade com a GSI-NC 14

Algumas normas do governo federal são publicadas com o intuito de consolidar orientações para que os gestores fiquem cientes dos

riscos a que estão expostos, mas têm causado paralisia nos gestores avessos a riscos.

É o caso da Norma GSI-NC 14, publicada em 09/03/2018[30], para estabelecer princípios, diretrizes e responsabilidades relacionados à segurança da informação para o tratamento da informação em ambiente de computação em nuvem por órgãos da administração pública federal direta e indireta.

Ao atentarmos para o objetivo da norma, fica claro que as ações necessárias para o seu cumprimento derivam diretamente de práticas e normativos exigidos não somente para o uso da nuvem pública, mas também para o tratamento da informação armazenada localmente (*on-premises*).

Práticas e políticas – tais como a Gestão de Risco de Segurança da Informação e Comunicações e a Política de Segurança de Informações e Comunicações – são insumos essenciais para a aderência não apenas à GSI-NC 14[30] com vistas à utilização da nuvem pública, mas também para a salvaguarda ante a normativos como a IN 1/2019[31], do Ministério da Economia e, ainda, como forma de desempenhar o papel designado para o contratante dos serviços no modelo de segurança compartilhada preconizado pelos provedores de nuvem pública.

Entende-se que os princípios orientadores e as diretrizes consubstanciadas na Norma GSI-NC 14[30] são plenamente alcançáveis, não devendo ser um inibidor da adoção de serviços em nuvem nas organizações submetidas a esse normativo.

No Apêndice A, é apresentada uma tabela com a análise de cada um dos incisos da GSI-NC 14[30] e a forma como acreditamos que o item poderia ser atendido, seja por uma ação ou pelo cumprimento de outra norma/política associada.

Tipos Predefinidos de Informações Sigilosas

A necessidade de proteção de dados em organizações públicas e privadas é um tema preocupante em todo o mundo. Vários casos de sucesso podem ser identificados na *internet*.

A Carnegie Mellon University, no documento *Guidelines for Data Classification*[32], define vários tipos de dados restritos com base em requisitos normativos internos. O objetivo desse guia foi dar condições de cumprimento para a Política de Segurança da Informação daquela universidade, determinando que "*todos os dados institucionais devem ser protegidos de maneira razoável e apropriada com base no nível de sensibilidade, valor e/ou criticidade que os dados têm para a universidade*". A saber:

1. Verificador de Autenticação

Um verificador de autenticação é uma informação que é mantida em sigilo por um indivíduo e é usada para provar que a pessoa é quem ela diz ser. Em alguns casos, um verificador de autenticação pode ser compartilhado entre um pequeno grupo de indivíduos. Um verificador de autenticação também pode ser usado para provar a identidade de um sistema ou serviço. Exemplos incluem, mas não estão limitados a:

- Senhas.
- Segredos compartilhados.
- Chaves privadas criptográficas.

2. Informações de saúde protegidas

As informações de saúde protegidas são definidas como "informações de saúde individualmente identificáveis", transmitidas

por meios eletrônicos, mantidas em mídia eletrônica ou transmitidas ou mantidas em qualquer outra forma ou meio. As informações de saúde protegidas são consideradas individualmente identificáveis se contiverem um ou mais dos seguintes identificadores:

- Nome.
- Endereço.
- Todos os elementos de datas (exceto ano) relacionados a um indivíduo, incluindo data de nascimento, data de admissão, data de alta, data de morte e idade exata (se acima de 89 anos).
- Números de telefone.
- Números de fax.
- Endereços de correio eletrônico.
- Números de segurança social.
- Números de registro médico.
- Números dos beneficiários do plano de saúde.
- Números de conta.
- Números de certificado/licença.
- Identificadores de veículo e números de série, incluindo o número da placa.
- Identificadores de dispositivo e números de série.
- Localizadores de recursos universais (URLs).
- Endereços de protocolo de *internet* (IP).
- Identificadores biométricos, incluindo impressões digitais e por voz.
- Imagens fotográficas de rosto inteiro e quaisquer imagens comparáveis.
- Qualquer outro número, característica ou código de identificação exclusivo que possa identificar um indivíduo.

3. Informações eletrônicas de saúde protegidas

Uma informação eletrônica de saúde protegida é definida como qualquer informação de saúde protegida que é armazenada ou transmitida por mídia eletrônica. Para efeitos desta definição, os meios eletrônicos incluem:

- A mídia de armazenamento eletrônico, como discos rígidos de computador e qualquer meio de memória digital removível e/ou transportável, como fita magnética ou disco, disco ótico ou cartão de memória digital.
- Mídia de transmissão usada para trocar informações já em mídia de armazenamento eletrônico. A mídia de transmissão inclui, por exemplo, a *internet*, uma *extranet* (usando a tecnologia da *internet* para vincular uma empresa a informações acessíveis apenas às partes colaboradoras), linhas alugadas, linhas discadas, redes privadas e o movimento físico de dispositivos eletrônicos removíveis e/ou transportáveis. Certas transmissões, inclusive de papel (via fac-símile) e de voz (via telefone), não são consideradas transmissões via mídia eletrônica, porque a informação que está sendo trocada não existe em forma eletrônica antes da transmissão.

4. Materiais controlados para exportação

Os materiais controlados para exportação são definidos como qualquer informação ou material que esteja sujeito aos regulamentos de controle de exportação dos Estados Unidos, incluindo (mas não se limitando a) Regulamentos de Administração de Exportação (EAR), publicados pelo Departamento de Comércio dos EUA, e

ITAR (*International Traffic of Arms Regulations*), publicadas pelo Departamento de Estado dos EUA.

5. Informações fiscais federais

As informações fiscais federais são definidas como qualquer retorno, informação de retorno ou informação de retorno do contribuinte que é confiada à universidade pela Receita Federal.

6. Informação do cartão de pagamento

As informações do cartão de pagamento são definidas como um número de cartão de crédito (também chamado de número de conta principal ou PAN) em combinação com um ou mais dos seguintes elementos de dados:

- Nome do titular.
- Código de serviço.
- Data de validade.
- Valor CVC2, CVV2 ou CID.
- PIN ou bloco de PIN.
- Conteúdo da tarja magnética do cartão de crédito.

7. Registros educacionais pessoais identificáveis

Os registros educacionais identificáveis pessoalmente são definidos como quaisquer registros educacionais que contenham um ou mais dos seguintes identificadores pessoais:

- Nome do aluno.
- Nome(s) do(s) pai(s) do aluno ou de outro(s) membro(s) da família.
- Número da segurança social.
- Número de estudante.

- Uma lista de características pessoais que tornariam a identidade do aluno facilmente rastreável.
- Qualquer outra informação ou identificador que torne a identidade do aluno facilmente rastreável.

8. Informações pessoais identificáveis

Para atender aos requisitos de notificação de violação de segurança, as informações pessoais identificáveis são definidas como o primeiro nome de uma pessoa ou primeiro nome e sobrenome em combinação com um ou mais dos seguintes elementos de dados:

- Número da segurança social.
- Número da carteira de motorista emitida pelo Estado.
- Número do cartão de identificação emitido pelo Estado.
- Número da conta financeira em combinação com um código de segurança, um código de acesso ou uma senha que permitiria o acesso à conta.
- Informações médicas e/ou de seguro de saúde.

9. Informações técnicas controladas

As informações técnicas controladas significam "informações técnicas com aplicação militar ou espacial que estão sujeitas a controles de acesso, uso, reprodução, modificação, desempenho, exibição, divulgação, divulgação ou disseminação".

10. Apenas para uso oficial

Os documentos e dados marcados com o rótulo de "apenas para uso oficial" são um precursor de informações não classificadas controladas.

Este exemplo da Carnegie Mellon University pode ser usado como uma referência para se ter uma ideia dos tipos de informação para os quais é razoável que sejam aplicados sigilos e restrições de publicação. Por outro lado, deve haver um volume grande de dados de conteúdo de cursos, informações administrativas, sistemas diversos de gestão da universidade e de prestação de serviços à comunidade acadêmica que estariam habilitados para publicação na nuvem. E é sob esse prisma que se deve analisar a classificação dos documentos e das informações no âmbito da administração pública brasileira. A aderência aos normativos protege os dados que precisam de proteção adequada, mas isso não é um impeditivo para que se possa adotar computação em nuvem e usufruir dos benefícios que a plataforma oferece.

Gargalos de Transferência de Dados para a Nuvem Pública – Desempenho

No já citado artigo *"A View of Cloud Computing"*, a ACM apresentou o que considerou serem dois riscos do uso de computação em nuvem: a transferência de dados e a imprevisibilidade de desempenho.

Em se tratando de transferência de dados, o artigo cita que, como os aplicativos vêm se tornando mais intensivos em dados e caso eles sejam distribuídos ao longo dos limites das nuvens, isso pode complicar o posicionamento e o transporte de dados. Cita ainda os custos de transferência (aproximadamente entre US$ 50 e US$ 120 por *terabyte* transferido) e que os usuários e os provedores de nuvem precisam pensar nas implicações da localização e do tráfego em todos os níveis do sistema, se quiserem minimizar os custos ou mesmo gerenciá-lo de forma adequada.

Embora a preocupação seja válida, há um certo exagero no impacto negativo real que ela pode causar na migração de serviços para a nuvem.

O padrão utilizado na nuvem pelos grandes provedores é que não há custo por transferência de dados de entrada (carga de dados do ambiente *on-premises* para o ambiente de nuvem, por exemplo), mas há cobrança para transferência de saída (dados e conteúdo entregues ao usuário do serviço na nuvem e envio dos dados de volta à infraestrutura local ou para outro provedor de nuvem ao fim do contrato) e pelo armazenamento dos dados. Assim, para que se faça uma estimativa mais precisa do custo real de um determinado serviço na nuvem, é preciso estimar o volume de dados que será entregue aos usuários mensalmente. Essa informação pode ser conseguida sem muito esforço a partir dos *logs* dos servidores *web*, com base no histórico de uso do serviço, caso já exista. Sendo um novo serviço, é preciso estimar o volume de acessos e o tamanho médio de dados que é entregue a cada requisição para, em seguida, calcular o volume mensal a ser transferido e o custo.

Assim, ao se transferir para a nuvem, por exemplo, um conjunto de imagens de tamanho total de um *terabyte*, não haverá custo para a transferência inicial, mas mensalmente será cobrado o armazenamento de 1TB de dados, adicionado ao volume de dados relativo às imagens que são baixadas pelos usuários do serviço. Ao fim do contrato, caso o conjunto de imagens seja totalmente transferido a outro provedor, é cobrada a taxa de transferência de saída relativa a 1TB.

É importante perceber que, caso as organizações utilizem a infraestrutura *on-premises*, esses custos também se aplicam, embora os gestores não façam essa contabilização de forma tão granular. Ou seja, é preciso reservar um espaço de 1TB de um *storage* e reservar a banda do *link* com a *internet* em volume suficiente para atender às requisições. Como o *storage* e o *link* são contratados para atender ao uso global pela organização, esse custo do serviço específico fica diluído ou mesmo escondido. Assim, a sensação inicial é de que o uso da nuvem trará custos adicionais quando, na verdade, haverá

um deslocamento real do custo de infraestrutura, melhor percebido apenas quando se retiram da infraestrutura local os recursos que estão sendo utilizados na nuvem.

Interrupção de Serviços e Descontinuidade dos Negócios – Disponibilidade

Os gestores de TI consultados relataram que esse tópico é uma das principais preocupações que eles têm quanto à adoção de Computação em Nuvem. Caso o provedor que hospede a infraestrutura (ou que seja apenas um serviço crítico da organização) fique indisponível, haverá perdas, tanto financeiras quanto de imagem.

Segundo a ISACA, há certa ironia nessa situação, uma vez que os produtos *SaaS* existentes estabeleceram um alto padrão a esse respeito. A pesquisa do Google tem a reputação de ser altamente disponível, a ponto de até mesmo uma pequena interrupção ser detectada pelas principais fontes de notícias. Registros de interrupções no *Amazon Simple Storage Service* (S3), no *AppEngine* e no *Gmail* viram notícias mundiais, o que, apesar da publicidade negativa, demonstra que poucas infraestruturas de TI corporativas são tão boas.

Apesar disso, contudo, sabe-se que a disponibilidade não é uma questão meramente técnica. Um provedor de nuvem pode sofrer interrupções por razões não técnicas, como a falência (sair do negócio) ou ser alvo de ação regulatória. Assim, a ISACA propôs que seja seguida a máxima da disponibilidade: "nenhum ponto único de falha", o que levaria à conclusão de que o gerenciamento de um serviço de computação em nuvem por uma única empresa seria algo a ser evitado. O argumento é que, mesmo que a empresa tenha vários *data centers* em diferentes regiões geográficas usando diferentes provedores de rede, ela pode ter sistemas comuns de infraestrutura e contabilidade de *software*, além de poderem

compartilhar características que venham a se tornar pontos de vulnerabilidade, possibilitando que seu serviço saia do ar.

Trataremos dessa preocupação sob dois prismas: disponibilidade e continuidade de negócios.

Quanto à disponibilidade – O grande poder computacional, a distribuição em dezenas de *data centers* e caminhos de conexão, a agilidade de provimento, que são características seminais da Computação em Nuvem, minimizam sobremaneira os riscos de disponibilidade. É muito provável que, para a maioria das organizações, os índices atuais de disponibilidade da infraestrutura *on-premises* sejam menores que os entregues pelos grandes provedores. Uma ação importante é tentar diminuir a chance de se contratarem pequenos provedores, empresas iniciantes com parca infraestrutura, pois isso pode impactar diretamente e indiretamente a disponibilidade, pela diminuição nas opções de contingência, como, por exemplo, replicar o serviço em outra zona de disponibilidade.

Uma pesquisa da *Right Scale*[33] mostra que as empresas que já adotaram Computação em Nuvem se utilizam, em média, de seis provedores de Nuvem diferentes. Isso não quer dizer necessariamente que há contratação de mais de um provedor de Nuvem para fornecimento de IaaS. Mas sim que, ao contratar *e-mail* corporativo, suíte de automação de escritório, entre outros aplicativos, haja uso de Computação em Nuvem pelo fornecedor, diminuindo o risco da organização contratante de se utilizar de apenas um único provedor de Nuvem para todos os seus *workloads*.

Quanto à continuidade de negócios – A Nuvem pode facilitar sua implementação, por fornecer diversas opções de contingência, mas é importante que haja um plano corporativo, discutido com a alta administração; que sejam realizados simulações e testes; e

que o plano seja atualizado para considerar a Nuvem. Em resumo, a Nuvem pode ser vista como mais uma ferramenta a ser utilizada na implementação do plano de continuidade, pela agilidade característica e pelas opções que oferece.

Dificuldades na Elaboração do Termo de Referência – Conformidade

A constante evolução tecnológica, o barateamento dos recursos computacionais e a constante redução orçamentária para investimentos em TIC estão conduzindo cada vez mais a exploração do modelo de computação em nuvem, que já traz como características intrínsecas o autoprovisionamento, a alta disponibilidade, o amplo acesso pela *internet*, a elasticidade de forma ágil e serviços remunerados conforme o demandado.

Porém, a grande preocupação dos gestores de TIC envolve questões de conformidade relacionadas a contratações de serviços em nuvem, mesmo diante dos benefícios que essas tecnologias podem trazer para a melhoria dos serviços públicos.

A partir da IN 1/2019[31], do Ministério da Economia, e da Resolução CNJ nº 182[34], do Conselho Nacional de Justiça (CNJ), são analisados alguns pontos críticos que têm inibido a adoção de serviços em nuvem em organizações públicas brasileiras.

Unidade de Medida e Forma de Comercialização

Em uma contratação baseada na arquitetura IaaS, o cliente tem controle apenas sobre itens de infraestrutura, como servidores virtuais, espaço de armazenamento, serviços de infraestrutura de rede (DNS, *load balancer* etc.), entre outros.

Ao se considerar a arquitetura IaaS, as unidades de medição desses serviços estão associadas ao provisionamento (consumo) de:

- horas de utilização de máquinas virtuais por mês;
- quantidade de GB utilizados por mês;
- quantidade de dados trafegados por mês;
- entre outros.

Para exemplificar, a tabela a seguir mostra parte do catálogo de serviços que pode ser contratado do provedor, na contratação realizada pelo TCU em 2018, relacionado ao valor máximo medido em Unidade de Serviço de Nuvem – USN.

Tabela 2. Catálogo de Serviços de Nuvem Computacional

Descrição dos serviços	Unidades	Valores máximos (em USN)
Máquina virtual Linux adquirida por meio de vCPU, reservada por um ano com pagamento *upfront*	vCPU/hora	0,32324
Máquina virtual Windows adquirida por meio de vCPU, reservada por um ano com pagamento *upfront*	vCPU/hora	0,75105
Serviço de armazenamento de blocos	Gigabyte/mês	0,95070
Serviço de armazenamento de objetos	Gigabyte/mês	0,28521
Tráfego de saída da rede	Gigabyte	0,85563
Serviço de balanceamento de carga	Unidade/hora	0,23767
Porta de conexão de fibra 10Gb/s	Unidade/hora	21,39074

Baseando-se nas diversas contratações existentes que usavam uma unidade de referência, como a Unidade de Serviço Técnico (UST), o TCU criou a USN e definiu o valor máximo em USN para os serviços que seriam mais demandados, como uma forma de

garantir que a proporção de preços entre aqueles serviços seria mantida durante toda a execução contratual.

A dimensão inicial dessas unidades deve levar em conta o consumo desses recursos no ambiente *on-premises*.

Nesta etapa, é fundamental harmonizar o ambiente *on-premises* com o ambiente na nuvem. O tipo de sistema operacional, o banco de dados, o tipo de servidor virtual, o volume de consumo de memória e de processamento devem ser conhecidos e especificados no projeto básico. Esses dados servirão para dimensionar a volumetria do serviço a ser contratado.

A forma de pagamento pelos serviços prestados é feita de acordo com o consumo, com valores medidos em horas e forma de pagamento mensal.

A composição do custo inicial padrão dos provedores pode ser definida em dólar, caso sejam utilizados provedores de outros países (AWS, Azure, Google), e depende de uma série de fatores, tais como: nível mínimo de serviço exigido, capacidade de ampliação e crescimento dos servidores provisionados, serviços de monitoramento e suporte ofertados, sistemas operacionais e interfaces (APIs) suportadas, além dos custos de entrada e saída de dados (medidos por GB).

Critérios de Segurança e Qualificação Técnica

Os temas "segurança" e "privacidade" são pontos de extrema relevância para a contratação de serviços em nuvem. Como descrito anteriormente, deve ser considerada a necessidade de conformidade com os seguintes instrumentos legais: Instrução Normativa GSI/01[54] e suas Normas Complementares (NC 14/IN01/DSIC/GSI/PR[30] e NC 19/IN01/DSIC/GSI/PR[35]), o Decreto nº 7.724[36] e o Decreto nº 7.845[37].

Os contratos devem prever cláusulas que especifiquem que os dados residam exclusivamente em território nacional, incluindo a

replicação e as cópias de segurança (*backups*), de modo que o cliente disponha de todas as garantias da legislação brasileira enquanto tomador do serviço e responsável pela guarda das informações armazenadas em nuvem. O foro brasileiro deverá ser adotado para dirimir quaisquer questões jurídicas relacionadas aos contratos firmados entre o cliente e o provedor do serviço em nuvem.

Quando aplicável, deverá ser assegurado, por meio de cláusula contratual, que as informações sob custódia do provedor de serviços em nuvem serão tratadas como informações sigilosas, não podendo ser usadas por esse provedor ou fornecidas a terceiros, sob nenhuma hipótese, sem autorização formal do cliente.

Além disso, conforme especificado no anexo da Portaria MP/STI nº 20[38], os órgãos deverão exigir, no momento da contratação de serviços em nuvem de fornecedores privados, que o ambiente do serviço contratado esteja em conformidade com a norma ABNT NBR ISO/IEC 27001:2013[39], sem prejuízo de outras exigências, objetivando mitigar riscos relativos à segurança da informação.

Quando a contratação de serviços em nuvem envolver serviços que possam comprometer a segurança nacional ou sistema estruturante, as normas indicam que as organizações direcionem a contratação de serviços de computação em nuvem junto a órgãos ou entidades de TI da Administração Pública (Serpro e Dataprev, por exemplo), invistam em uma nuvem privada ou mantenham essas soluções/sistemas em sua infraestrutura interna *on-premises*.

Portabilidade e Continuidade

Portabilidade é a capacidade que permite que as aplicações e os dados operem no mesmo modelo de serviço em nuvem, ofertado por fornecedores distintos, sem a necessidade de reescrever códigos de aplicações, converter bancos de dados, alimentar os sistemas

com informações dos usuários ou mesmo alterar características das aplicações.

Continuidade é um processo que objetiva assegurar o mínimo de impacto no negócio de um evento que possa interromper (parcial ou totalmente) um ou mais serviços de TIC.

A partir de uma análise dos conceitos apresentados, é importante firmar cláusulas contratuais, de maneira que o serviço a ser contratado permita a portabilidade de dados e aplicativos e que as informações do cliente estejam disponíveis para transferência de localização em prazo adequado e sem custo adicional, de modo a garantir a continuidade do negócio e possibilitar uma transição contratual, quando aplicável.

Outra forma de mitigar os riscos de aprisionamento e dependência técnica e contratual de um único provedor de serviços em nuvem (*lock-in*) é a elaboração de um plano de continuidade, considerando a contratação de provedores alternativos para assegurar a continuidade dos serviços no caso de interrupções (planejadas ou não) e assegurar o nível de serviços adequados, entre outros.

A seguir, são apresentadas algumas formas de evitar o *lock-in*:

- Considere provedores de infraestrutura que façam uso e tenham padrões de APIs compatíveis com a maioria dos provedores de serviços em nuvem e sejam aderentes a modelos abertos (*Open Stack*, por exemplo).
- Procure utilizar *containers* para garantir uma abordagem padronizada para a implantação das aplicações.
- Evite a utilização de banco de dados exclusivo de um provedor de serviços em nuvem.
- Utilize APIs comuns (como *NodeJS*, por exemplo).
- Use IPs fixos e nomes DNS vinculados ao órgão e não ao

provedor de serviços em nuvem.
- Utilize mais de um provedor de serviços em nuvem.

Níveis Mínimos de Serviço e Padrão de Disponibilidade

Os contratos firmados com os provedores de serviços em nuvem são, na sua maioria, contratos de adesão, como é o caso dos contratos firmados dos órgãos públicos com empresas de telefonia. Todos os provedores seguem um modelo de mercado baseado em normas, padrões e práticas internacionais, mas não deixam muita margem para adaptações específicas para atender uma organização isoladamente.

Os parâmetros de nível de serviço mais comuns que serão encontrados nos contratos dizem respeito a questões como disponibilidade, tempo de resposta, desempenho, tempo para correção de erros, capacidade, escalabilidade e políticas de segurança adotadas. No caso de descumprimento de alguns dos níveis mínimos de serviço indicados, as compensações adotadas pelos provedores costumam ser créditos em dias de serviço ou descontos no valor do faturamento seguinte.

De acordo com o anexo da Portaria MP/STI nº 20[38], na contratação de serviços em nuvem com empresas privadas, as organizações devem exigir disponibilidade de, no mínimo, 99,741% para os *data centers* onde os serviços estarão hospedados e a comprovação poderá ser aceita por meio de certificação TIA 942 TIER II.

Vale abrir um espaço para esclarecer o que seria a certificação TIER, adotada mundialmente pelos principais *data centers* e desenvolvida pelo instituto americano *Uptime Institute*, com o objetivo de mensurar o nível da infraestrutura de um local destinado ao funcionamento de um centro de processamento de dados (CPD).

- TIER I: *data center* básico que possui componentes internos não redundantes e uma rota de alimentação externa (energia e conexão de dados) não redundante, servindo ao ambiente crítico. Essa infraestrutura inclui um espaço dedicado para os sistemas de TI; um sistema UPS (*no-break*), para lidar com falhas momentâneas no fornecimento de energia; um equipamento dedicado de refrigeração; e um sistema gerador, para proteger as funções de TI de falhas prolongadas no fornecimento de energia. A disponibilidade para o TIER I é de 99,671%.
- TIER II: este *data center* possui componentes internos redundantes e uma rota de distribuição de alimentação externa (energia e conexão de dados) não redundante, servindo ao ambiente crítico. As redundâncias encontram-se nos geradores, sistemas UPS (*no-break*), sistemas de refrigeração e tanques de combustível. Esses componentes podem ter seu funcionamento interrompido, seguindo um plano de manutenção, por exemplo, sem a necessidade de desligar qualquer um dos equipamentos críticos de TI. A disponibilidade para o TIER II é de 99,741%.
- TIER III: trata-se de um *data center* paralelamente sustentável que possui componentes de capacidade redundantes e múltiplas rotas independentes de distribuição (energia e conexão de dados) que servem ao ambiente crítico. Apenas uma rota de distribuição é necessária para servir ao ambiente crítico em qualquer momento. A interrupção de qualquer componente nas rotas de distribuição não impacta os equipamentos do ambiente crítico. A disponibilidade para o TIER III é de 99,982%.
- TIER IV: é um *data center* tolerante a falhas e composto por vários sistemas fisicamente independentes e isolados, componentes redundantes e múltiplas rotas independentes de

> alimentação (energia e conexão de dados) ativas simultaneamente, servindo ao ambiente crítico. Sistemas complementares e rotas de distribuição estão compartimentalizados, ou seja, fisicamente isolados um do outro, para prevenir que qualquer incidente impacte simultaneamente os sistemas ou as rotas de distribuição e alimentação. Pelas suas características, a disponibilidade para o TIER IV é de 99,99%.

Com o objetivo de garantir e monitorar o atendimento aos níveis mínimos de serviço, o contrato deve prever a auditoria de registros ou *logs* pelos clientes, além de prover acesso às estatísticas de qualidade do serviço.

Utilização de POC – Prova de Conceito

A prova de conceito é um instrumento que auxilia os órgãos na verificação das condições de execução dos serviços que serão prestados pelo provedor. Para fazer uso da POC, deve haver previsão explícita no projeto básico da contratação e esta não deve ser utilizada no momento do planejamento da contratação, mas sim na fase externa da licitação, para avaliar se o serviço ofertado atende aos requisitos definidos no projeto básico.

Para o TCU[40], as "*provas de conceito não devem ser utilizadas na fase interna da licitação (planejamento da contratação), uma vez que não se prestam a escolher solução de TI e a elaborar requisitos técnicos, mas a avaliar, na fase externa, se a ferramenta ofertada no certame atende às especificações técnicas definidas no projeto básico ou no termo de referência*".

Para a avaliação da POC, devem ser definidos um escopo mínimo de um ambiente que será montado pelo provedor de serviços e um rol de atividades que devem ser executadas por

ele. A validação final da POC irá comprovar o atendimento ou não dos requisitos técnicos e o cumprimento dos padrões mínimos de desempenho descritos.

A contratação com *broker* ou diretamente com o provedor

Um *broker* é uma entidade que gerencia o uso, o desempenho e a entrega de serviços de nuvem e negocia relacionamentos entre provedores e consumidores de nuvem. O *broker* posiciona-se entre o consumidor e o provedor de nuvem e pode ajudar o consumidor de nuvem a diminuir a complexidade de escolher e gerenciar múltiplos serviços de provedores. Um consumidor de nuvem pode exercer as atividades de *broker* se tiver, em sua equipe, pessoas qualificadas para o relacionamento direto com um provedor.

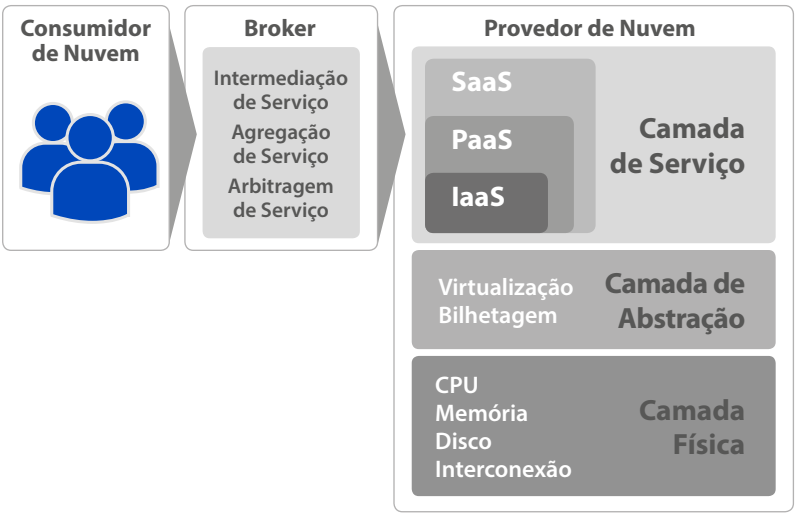
Em geral, um *broker* pode fornecer serviços em três categorias, podendo atuar em mais de uma simultaneamente:

- intermediação de serviço;
- agregação de serviços;
- arbitragem de serviço.

As primeiras licitações de serviços em nuvem na Administração Pública Federal (TCU, MP) foram estruturadas para contratar um *broker*; nesse caso, uma empresa de TI que tivesse conhecimento na implementação de serviços em nuvem e que representasse um ou mais provedores de nuvem pública.

Na prática, o *broker* especificado nas licitações brasileiras aproxima-se mais da definição do Gartner do que do NIST, na medida em que viabiliza principalmente a terceirização da configuração e gestão de serviços na nuvem (customização dos serviços), mas não oferece agregação e nem arbitragem dos serviços.

Figura 8. Arquitetura incluindo o *broker*



A utilização do *broker* não é obrigatória na relação entre o consumidor da nuvem e o provedor de serviços; porém, se for insuficiente o nível de maturidade das equipes de TI das organizações consumidoras de serviços em nuvem, o *broker* assumirá o papel de facilitador tanto da implantação quanto da gestão dos serviços, recomendando-se a sua contratação. Essa contratação se torna determinante quando o termo de referência envolver a contratação simultânea de dois ou mais provedores de nuvem, pois o nível de complexidade se eleva exponencialmente.

O fluxo a ser registrado no termo de referência seria: o órgão decidirá o serviço a ser migrado ou criado na nuvem computacional e passará essas informações para o *broker*, que intermediará a configuração e publicação no(s) provedor(es) de serviços. Essa intermediação acontecerá durante todos os momentos em que o consumidor necessitar de alguma ação sobre o(s) provedor(es) de

serviços, seja ela acréscimo de espaço de armazenamento, incremento de processamento, migração de dados e outros serviços.

Baixa Cultura Organizacional para Adoção de Nuvem – Legitimidade

Embora a computação em nuvem exista há mais de dez anos, desde que a AWS começou a oferecer seus serviços em 2006, as empresas brasileiras e, em especial, as organizações de governo demoraram a reconhecer e avaliar o valor estratégico de um posicionamento na nuvem.

A demora na adoção se deu por diversos motivos. Como os provedores de nuvem não tinham *data center* no Brasil, havia uma chance de se encontrar maior latência na comunicação de rede entre o provedor e os usuários nacionais. Essa questão inviabilizava a migração de alguns serviços e aplicações. Não ter *data center* no Brasil significava também que a legislação aplicável seria a de outro país e isso trouxe receios, inicialmente, e impôs restrições, posteriormente, quando normativos específicos foram publicados, a exemplo da NC 14 do GSI/PR, cuja primeira versão data de janeiro de 2012[30].

A AWS foi a primeira a ter *data center* em território brasileiro e sua operação iniciou-se em dezembro de 2011. A Microsoft Azure iniciou as operações em solo nacional em junho de 2014, e a Google, em setembro de 2017, citando os três maiores provedores de nuvem.

Ainda em 2013, um incidente – no qual se descobriu que a NSA americana havia espionado comunicações da então presidente Dilma Rousseff – trouxe mais preocupações acerca da privacidade na comunicação e no armazenamento de dados no âmbito do governo brasileiro, aumentando o clima de desconfiança quanto a migrar dados da infraestrutura local para provedores de nuvem.

Em 2016, houve a promulgação da EC 95[1], que estabeleceu que os gastos realizados naquele ano virariam um teto por 20 anos,

corrigido apenas pela inflação anual. Essa EC fez com que houvesse uma corrida das organizações de governo para executar, ainda em 2016, compras de ativos de TI (licenças de *software*, equipamentos), cuja renovação estava próxima. Em 2017, com os estoques cheios de servidores, elementos de rede, *storages*, assim como de licenças e subscrições de sistemas, várias organizações postergaram a adoção de nuvem para meses e anos posteriores.

Ou seja, embora o conhecimento em relação à importância da Computação em Nuvem tenha aumentado a partir da instalação de *data centers* dos grandes provedores em solo nacional, pelos motivos citados, não houve contratações relevantes e em volume suficiente para que se criasse uma comunidade de prática, no âmbito do governo brasileiro, e isso resultou em uma baixa cultura organizacional em relação à nuvem.

No âmbito de uma dissertação de mestrado em Computação em Nuvem[53], uma pesquisa realizada em junho de 2018 com 311 servidores públicos de TI comprova essa realidade da administração pública brasileira. De acordo com a pesquisa, 48% das organizações responderam que o uso de nuvem era importante ou muito importante para as atividades-fim da organização. Mas apenas 15% das organizações haviam contratado Computação em Nuvem, o que mostra um descompasso entre a percepção de importância e a real adoção.

Quando perguntados qual era o prazo em que previam realizar uma contratação que viabilizasse a adoção da nuvem, 9% relataram que estimavam contratar em até um ano, e 20%, entre um e dois anos. Além disso, 43% dos respondentes relataram ter tempo de experiência em nuvem menor que um ano. Esses sinais indicam que a adoção continuará lenta, ainda, caso a cultura organizacional continue baixa em relação à nuvem e caso as organizações do governo brasileiro não iniciem ações efetivas que viabilizem a mudança do quadro.

Imprevisibilidade do Desempenho da Nuvem Pública – Riscos

Em se tratando de previsibilidade de desempenho, o artigo da ACM[23] descreve que, com base na experiência e nos experimentos realizados pelos autores, várias máquinas virtuais (VMs) podem compartilhar CPUs e memória principal surpreendentemente bem na nuvem, mas que o compartilhamento de rede e de E/S de disco é mais problemático. Como resultado, diferentes instâncias do EC2 (serviço de fornecimento de VMs da AWS) variaram mais em seu desempenho de E/S do que no desempenho da memória principal. Encontrou-se um desvio-padrão de desempenho de apenas 4% para memória, mas de 16% para gravação em disco, o que demonstra o problema de interferência de E/S entre máquinas virtuais.

Outro estudo[41] mediu o desempenho de processamento de um modelo de máquina virtual da AWS, instanciando mais de mil VMs do mesmo modelo em diferentes zonas de disponibilidade (e, portanto, em diversos *data centers* de vários países) e em diferentes horários e dias da semana. O resultado é que se encontrou uma variação de até 30%, que se atribuiu às diferentes versões de processador disponíveis em cada *data center*.

De fato, não há como garantir que haja exatamente o mesmo desempenho ao se executar uma mesma VM em horários diferentes, e isso deve ser levado em consideração. Dependendo da arquitetura e do tamanho da infraestrutura local, esse fenômeno pode já estar acontecendo no ambiente *on-premises* em algumas organizações. Ele está relacionado não apenas com a carga da infraestrutura como um todo em dado momento, que pode variar de acordo com as características das aplicações que se utilizam da infraestrutura simultaneamente, mas também com estratégias de consolidação de servidores, utilizadas para melhorar a eficiência do uso da infraestrutura

do ponto de vista do provedor, economizando energia elétrica, ao permitir desligar servidores físicos não utilizados, o que também tem um apelo de sustentabilidade. Uma variável relacionada é a heterogeneidade dos modelos e das gerações de processadores disponíveis na infraestrutura, visto que o artigo encontrou ser o modelo de processador o fator mais importante para o desempenho. Caso haja mudanças de VM entre servidores físicos com gerações diferentes de processador, haverá também variação no desempenho.

Um ponto importante a se considerar é que a variabilidade de desempenho é uma característica da nuvem pública, uma vez que ela é baseada em grandes centros de dados (o que proporciona a heterogeneidade de processadores), que são compartilhados por muitos usuários (o que facilita a migração de VMs entre servidores físicos, quando se considera um período de tempo mais longo, da ordem de dias ou semanas). Não se pode deixar de levar em conta, por outro lado, que a agilidade no provimento e a elasticidade, somadas ao pagamento por uso, diminuem o impacto negativo (ou mesmo perceptível) dessa variabilidade. Ou seja, é possível se alocar uma ou mais VMs para um serviço na nuvem, monitorar o seu desempenho e, caso necessário, aumentar a quantidade de recursos (e de VMs!) rapidamente, em minutos. Com a elasticidade, é possível fazer isso automaticamente e garantir que os recursos alocados estejam em uso pleno, mas sem impactar o nível de serviço prestado ao usuário.

ESTRATÉGIAS DE ADOÇÃO DE NUVEM COMPUTACIONAL

Nesta seção, veremos algumas estratégias utilizadas para a adoção de nuvem computacional que auxiliarão os órgãos superiores de gestão, as instâncias de controle e as organizações públicas a utilizarem, mais rapidamente, os benefícios da adoção de serviços em nuvem com menores riscos. De igual modo, veremos um modelo de decisão para auxiliar a definir qual infraestrutura (*on-premises* ou na nuvem) executará os novos *workloads*, sejam novos sistemas, sejam evoluções de sistemas legados.

- 0% Cloud – A decisão é por não se utilizar da nuvem como forma de provimento de soluções de TI. Embora seja difícil visualizar uma operação de TI que não se utilize de nenhum sistema em nuvem atualmente, essa estratégia vai na linha de usar o mínimo possível, restringindo-se apenas ao uso de sistemas de mercado que sejam providos exclusivamente na nuvem.
- 100% Cloud – Essa é uma decisão inversa à anterior, em que toda a infraestrutura de *hardware* e *software* é mantida e operada na nuvem pública. Empresas *startups* (empresas novas que já nascem com um foco em receber investimentos para crescer rapidamente) podem se utilizar dessa estratégia, de forma que possam focar seus esforços apenas no negócio para o qual foram criadas. Considerando-se

os investimentos já realizados pela administração pública brasileira, por meio de seus órgãos e suas agências, essa dificilmente será a estratégia adotada.

- *Cloud First* – Estratégia adotada pelo governo americano em 2011 e pelo governo inglês, que determina que, sempre que houver uma alternativa similar (em custo, funcionalidades) disponível na nuvem, essa deve ser a forma de provimento escolhida. Ou seja, primeiro vê-se se é possível fazer na nuvem. Caso não seja possível ou adequado, implementa-se *on-premises*. É comum se estabelecerem metas de quantidade de serviços a serem executados na nuvem ou de percentual do orçamento anual a ser dispendido na nuvem, como uma forma de determinar o ritmo da adoção, que se intenciona seja um ritmo sustentado.
- Experimentação – É uma decisão de se adotar nuvem como forma de provimento, mas prioriza-se o aumento da maturidade da organização como pré-requisito para um maior avanço. Estuda-se e contrata-se nuvem (principalmente nos modelos de IaaS e PaaS) e iniciam-se projetos experimentais em diversas áreas como uma forma de dominar a nova plataforma antes de uma ida com mais volume.
- Caso a caso – Decide-se ir para a nuvem, mas a decisão sobre cada *workload* é tomada caso a caso. Normalmente, não há metas estabelecidas e a maturidade no uso da nuvem virá em um tempo maior que nas estratégias de *cloud first* e experimentação, na maioria dos casos. Por exemplo, pode-se decidir utilizar um serviço de *e-mail* corporativo ou de pacote de aplicativos de automação

de escritório na nuvem simplesmente porque a oferta do momento mostrou-se mais vantajosa de que a alternativa *on-premises*.

Após a organização decidir adotar nuvem e dependendo da estratégia que adotar, a cada novo *workload* pode ser necessário usar um modelo de decisão para identificar qual é a melhor forma de provimento (considerando-se que a estratégia não foi 100% *cloud*).

Um modelo de decisão é um *framework* estruturado, que recebe informações de entrada e indica como saída quais são as opções de provimento que melhor se adequam, de acordo com o perfil da organização. Ele pode ser utilizado para selecionar os sistemas e serviços que serão criados ou migrados para a nuvem, trazendo objetividade ao processo de seleção e priorização.

Acelerando a Adoção de Nuvem no Governo Brasileiro

A tecnologia que envolve os serviços em Nuvem Computacional está disponível por mais de 10 anos e tem demonstrado uma gama de benefícios para os órgãos de governo e, indiretamente, para os cidadãos que dependem de serviços públicos de qualidade. Tal tecnologia já adquiriu um alto nível de maturidade no âmbito de empresas privadas, mas, apesar disso, no âmbito do governo brasileiro, ainda se percebe um ritmo de adoção lento, principalmente por questões que envolvem segurança e desconhecimento da tecnologia envolvida.

Seguindo tendências e boas práticas de países que já vêm adotando serviços em Nuvem Computacional para governo, entende-se que os órgãos/entidades do governo brasileiro, nas esferas federal, estadual/distrital e municipal, devem rapidamente iniciar

ações aceleradoras que catalisem a adoção de serviços em Nuvem Computacional.

A partir de inspiração no modelo proposto por Vivek Kundra, CIO do governo americano em 2011[17], propõem-se ações que envolvam, principalmente, trabalhos em comunidade, compartilhamento de boas práticas e debates sobre problemas/riscos identificados. A ação conjunta dos gestores de TI do governo brasileiro dará agilidade, eficiência, eficácia e economicidade aos serviços prestados à sociedade.

Propõem-se, de modo não exaustivo, cinco ações catalizadoras que podem rapidamente ser implementadas pelo governo brasileiro, acelerando a adoção de serviços em Nuvem Computacional, para se auferirem, em curto espaço de tempo, os benefícios dessa tecnologia.

1. Desenvolver modelos de adoção de serviços em nuvem para governo

Ao desenvolverem e divulgarem modelos e boas práticas relacionados a serviços em nuvem, os órgãos de governo disponibilizam referências e casos de sucesso que desmistificam os problemas que envolvem a contratação e o uso das tecnologias envolvidas, agilizando a adoção dos serviços e mitigando riscos de falhas e questionamentos por órgãos de controle interno e externo.

O incentivo à criação de comunidades de prática e à manutenção de *sites* de conteúdo especializado poderá alavancar a publicação de processos, roteiros e modelos que auxiliem os órgãos de menor maturidade.

Outra medida relevante seria o registro, nesses *sites* especializados, dos "Casos de Negócios de Órgãos de Governo", de modo que essas informações compiladas se transformassem numa biblioteca de modelos para apoiar outros órgãos/entidades em seus processos de

adoção de serviços em nuvem. Essa biblioteca de casos de negócios conteria detalhes dos processos de planejamento da contratação, seleção de fornecedores e gestão contratual, organizados por tipo de serviço, conforme tabela padronizada.

Desse modo, um órgão que decidisse adotar determinado serviço em nuvem procuraria na biblioteca um caso de negócio de escopo ou propósito similar, reduzindo enormemente o esforço burocrático decorrente de processos envolvendo a justificativa, análise de riscos, licitação, gestão contratual etc.

É certo que a padronização de processos de trabalho não dirime todos os problemas inerentes à abordagem de computação em nuvem, mas à medida que os órgãos públicos e o mercado fornecedor amadurecerem, essas dificuldades tenderão a se reduzir rapidamente, tornando esses serviços comuns, como luz, água e telefonia.

2. Criar um ambiente seguro e confiável

As questões que envolvem segurança da informação são as mais impactantes na adoção de serviços em nuvem, pois os órgãos/entidades do setor público têm deixado para segundo plano a classificação de seus dados quanto ao nível de confidencialidade e, como consequência, temem não conseguir identificar adequadamente quais dados são passíveis de armazenamento em ambiente de empresas privadas.

A Lei nº 12.527/2011[27], que assegura o direito fundamental de acesso à informação, determina "*a publicidade como preceito geral e o sigilo como exceção*". Além disso, há certo consenso em que apenas um pequeno percentual dos dados da administração pública é sigiloso. Apesar disso, o receio de ser questionado pela terceirização da guarda de dados sigilosos tem-se imposto a qualquer benefício decorrente da adoção de serviços em nuvem computacional.

Entende-se, por outro lado, que um ambiente seguro deva existir em qualquer situação, seja no armazenamento de dados em *site* local (*on-premises*), seja em armazenamento de dados em nuvem computacional de terceiros. Para isso, os órgãos de gestão superior (OGS) do governo brasileiro deveriam padronizar processos de classificação de informações, disponibilizar *softwares* de criptografia de dados e desenvolver métodos de gestão de riscos que orientem os gestores no desenvolvimento de um ambiente seguro e confiável para os dados dos órgãos/entidades públicas, independentemente de sua localização.

Para o governo americano, também cioso de garantir a confidencialidade de suas informações governamentais, *"a transição para o ambiente de computação em nuvem terceirizada é, em muitos aspectos, um exercício de gerenciamento de riscos"*[17].

O adequado gerenciamento de riscos envolve identificar, avaliar e mitigar os riscos em todo o ciclo de vida das informações, implementando os controles de segurança e privacidade disponíveis e garantindo os benefícios esperados com as soluções de computação em nuvem.

A criação de um ambiente de segurança transparente entre provedores e consumidores da nuvem permitirá a elevação da maturidade e da capacidade dos órgãos do governo em sua postura de segurança de dados.

No âmbito do governo americano, o primeiro passo nesse processo foi o Programa Federal de Gerenciamento de Risco e Autorização (FedRAMP), iniciado em 2010, com o objetivo de "*definir requisitos para controles de segurança de computação em nuvem, incluindo verificação de vulnerabilidades e monitoramento de incidentes, registros e relatórios*".

No escopo desse programa, o governo americano priorizou uma lista das principais ameaças de segurança, acompanhando-a sistemática e periodicamente, com uma equipe de especialistas

em segurança, de modo a garantir que controles e medidas de segurança apropriados fossem implementados para mitigar as ameaças identificadas.

No Brasil, esse acompanhamento poderia ser realizado pelo Centro de Tratamento de Incidentes de Redes do Governo (CTIR-Gov), órgão subordinado ao Departamento de Segurança de Informação e Comunicações (DSIC), do Gabinete de Segurança Institucional da Presidência da República (GSI/PR). O CTIR-Gov tem como finalidade o atendimento aos incidentes em redes do governo (domínios gov.br, jus.br, leg.br, mil.br, mp.br e def.br).

Num segundo momento, o governo americano determinou ao NIST a publicação de orientações técnicas de segurança, voltadas para o monitoramento contínuo de soluções de computação em nuvem, consistentes com a estrutura de seis etapas do gerenciamento de riscos[42], considerando os possíveis "benefícios de segurança" e as "potenciais vulnerabilidades".

Benefícios de segurança do uso de serviços de computação em nuvem incluem:

- a capacidade de concentrar recursos em áreas de grande preocupação, à medida que serviços de segurança mais gerais são assumidos pelo provedor de nuvem;
- força potencial da plataforma resultante de maior uniformidade e homogeneidade, resultando em melhoria na garantia de informações, resposta de segurança, gerenciamento do sistema, confiabilidade e capacidade de manutenção;
- melhor disponibilidade de recursos por meio de recursos de escalabilidade, redundância e recuperação de desastres;
- resiliência melhorada a demandas imprevistas de serviço;

- aprimoramento de recursos de *backup* e recuperação, políticas, procedimentos e consistência;
- capacidade de alavancar serviços em nuvem alternativos para melhorar a postura geral de segurança, incluindo a dos *data centers* tradicionais.

Potenciais vulnerabilidades associadas aos modelos de serviço e implantação de computação em nuvem seriam:

- a complexidade inerente do sistema de um ambiente de computação em nuvem e a dependência da exatidão desses componentes e das interações entre eles;
- a dependência do provedor de serviços para manter a separação lógica em um ambiente de múltiplos inquilinos (por exemplo, não exclusivo do modelo de computação em nuvem);
- a necessidade de garantir que a organização retenha um nível apropriado de controles para obter consciência situacional, pesar alternativas, definir prioridades e efetuar mudanças na segurança e na privacidade que sejam do interesse da organização.

Enfim, para o governo americano, as principais considerações de segurança incluem a necessidade de:

- definir cuidadosamente os requisitos de segurança e privacidade durante o estágio inicial de planejamento no início do ciclo de vida de desenvolvimento de sistemas;
- determinar até que ponto os contratos de serviços negociados são necessários para atender aos requisitos de segurança;

- determinar as alternativas de uso de contratos de serviços negociados ou modelos de implantação de computação em nuvem que ofereçam maior supervisão e controle sobre segurança e privacidade;
- avaliar até que ponto os ambientes de computação do lado provedor e do lado cliente atendem aos requisitos de segurança e privacidade da organização;
- continuar a manter práticas de gerenciamento de segurança, controles e responsabilidade sobre a privacidade e a segurança de dados e aplicativos.

Certamente, as ações implementadas pelo governo americano melhoraram a confiança no uso de serviços em nuvem e ajudaram as agências do governo a auferir os benefícios do serviço com baixos riscos de segurança.

3. Simplificar os processos de aquisição de serviços em nuvem

O processo de aquisição do governo brasileiro, à luz da Instrução Normativa nº 1/2019 [31], do Ministério da Economia, já está bem consolidado e amadurecido, mas quando o objeto de aquisição se refere a "serviços em nuvem computacional", há uma paralisia entre os gestores públicos. Várias podem ser as causas, mas eleva substancialmente a inércia na adoção de nuvem computacional, em órgãos do governo, a falta de um modelo simplificado de contratação que envolva IaaS (Infraestrutura como Serviço), PaaS (Plataforma como Serviço) e SaaS (Software como Serviço).

A determinação para que os órgãos e as entidades do Poder Executivo Federal optem por serviços em nuvem computacional quando necessitarem "*criar, ampliar ou renovar infraestrutura de*

centro de dados", inserida no item 4.1 da IN 1/2019[31], pode não ser suficiente se permanecer complexa a contratação desses tipos de serviços.

Além dos benefícios mundialmente aceitos e validados, outra grande vantagem em contratar serviço de nuvem é que o governo passa a adotar a abordagem "aprovar uma vez, usar com frequência e pagar por consumo", o que, pela legislação atual, significa a renovação de contratos por até 60 meses.

O desenvolvimento de modelos de termos de referência para serviços baseados em nuvem com certeza simplificaria a adoção desses serviços, principalmente em órgãos de menor maturidade.

Recomenda-se que tais modelos sejam criados por grupos de trabalho multidisciplinares, com representantes de vários órgãos e várias especialidades, principalmente membros das áreas de controle e jurídico. Sempre que houver possibilidade técnica e quando for economicamente vantajoso, os modelos serão formatados como casos de negócios, para que os órgãos públicos possam rapidamente migrar para tecnologias de nuvem.

É importante ressaltar que todo o esforço em nível federal auxiliará sobremodo os governos estaduais e municipais na simplificação de seus processos aquisitivos, impulsionando a participação em serviços em nuvem, proporcionando inovação aos serviços públicos, aumentando o tamanho do mercado e criando maior eficiência em função da elevação da escala, com a consequente redução dos gastos públicos.

Outra iniciativa de grande impacto e apoio à adoção de serviços em nuvem é a implementação de um processo de "credenciamento de provedores de nuvem" por órgãos de gestão superior (OGS). Tal habilitação prévia garantiria agilidade e segurança aos órgãos/entidades governamentais, que ficariam livres de discussões técnicas

sobre acordos de níveis de serviço, portabilidade, padrões de segurança, disponibilidade e outras características inerentes à contratação de empresas fornecedoras do serviço.

Quanto maior for o número de provedores de nuvem habilitados para o governo, mais rápidos serão os processos de aquisição, menores serão os preços dos serviços e maiores serão as possibilidades de prestação de serviços de qualidade. Ressalte-se que também poderá ser criado credenciamento por faixa de volume, deixando as faixas de menor volume para empresas privadas 100% brasileiras, que buscam escala para crescer e se estabelecer no mercado nacional e internacional.

4. Estabelecer padrões de computação em nuvem

Para o governo americano [17], o estabelecimento de padrões foi fator preponderante para a adoção bem-sucedida e para a entrega de serviços de computação em nuvem, uma vez que a padronização possibilitou a portabilidade dos serviços entre os provedores de nuvem, permitindo que as agências de governo daquele país tivessem independência de fornecedores e pudessem aproveitar melhores condições de preço e, ainda, de funcionalidades inovadoras dos serviços oferecidos. Para o governo americano, os padrões também foram essenciais para garantir que as nuvens tivessem uma plataforma interoperável, na qual os serviços fornecidos por diferentes provedores trabalhassem juntos.

No Brasil, não há um órgão com a mesma característica e capacidade do NIST (*National Institute of Standards and Technology*), que é responsável pela definição de padrões para o governo americano e colabora com os CIOs dos órgãos públicos americanos. Por isso, o governo brasileiro, a exemplo de vários outros países, adota os padrões publicados pelo NIST na maioria das vezes sem qualquer adaptação.

É importante ressaltar que o NIST realiza várias outras atividades que também são muito importantes para o bem-sucedido programa americano de adoção de serviços em nuvem, a saber:

- O NIST realiza *workshops* de engajamento para identificar e priorizar necessidades.
- O NIST gera, avalia e revisa periodicamente um roteiro de computação em nuvem.
- O NIST executa um projeto tático de *Standards Acceleration to Jumpstart Adoption of Cloud Computing* – SAJACC (Aceleração de Padrões para Incentivar a Adoção de Computação em Nuvem), que desempenha um papel importante na validação das principais especificações de nuvem e no compartilhamento de informações, para aumentar a confiança na tecnologia de computação em nuvem antes que os padrões formalizados estejam disponíveis.

Assim, mesmo que o Brasil continue adotando os padrões americanos, algum órgão ou entidade brasileira deverá exercer o papel de liderança na priorização, tradução, adaptação, capacitação e divulgação desses padrões para o governo brasileiro.

5. Estabelecer uma sólida base de governança de TI

A definição de uma "Estratégia Nacional para Nuvem Computacional" deverá ser o primeiro passo no processo de migração para tecnologias de nuvem no âmbito do setor público, a exemplo do que ocorreu em 2011 no governo americano.

Os órgãos de gestão superior (OGS) deverão desempenhar um papel preponderante em todo esse processo, assumindo a

responsabilidade de identificar e resolver problemas de nuvem em todos os níveis: liderando o processo, induzindo comportamentos desejáveis em órgãos públicos e mobilizando fornecedores na prestação de serviços inovadores com preços competitivos. À medida que as questões impactantes amadureçam e se estabilizem, os OGS poderão voltar a focar suas prioridades em pontos mais abrangentes.

Para gerir de forma eficaz as questões de governança pública de TI em longo prazo, a Presidência da República e o Congresso Nacional precisam estabelecer uma política de Estado voltada para garantir a eficiência do governo e a melhoria dos serviços públicos, que não podem ficar restritos ao mandato de um governo ou à administração temporária de OGS.

Uma alternativa mais rápida seria a publicação da "Estratégia Nacional para Nuvem Computacional", de forma a estabelecer clara e inequivocamente o que deverá ser migrado para os serviços em nuvem computacional (e o que não poderá migrar), definindo papéis, responsabilidades, metas e recursos para órgãos, comitês e gestores, além de clarificar a estrutura hierárquica de tomada de decisão entre os partícipes desse processo.

No governo americano, medidas similares minimizaram a burocracia desnecessária, capacitaram os órgãos no cumprimento de metas ambiciosas de adoção de serviços em nuvem e estabeleceram uma clara responsabilidade pelos resultados almejados.

A exemplo do governo americano, alguns órgãos brasileiros poderiam ter seus papéis e suas responsabilidades aprimorados para auxiliar na proposta da "Estratégia Nacional para Nuvem Computacional":

- O Instituto Nacional de Tecnologia da Informação (ITI) lideraria o programa de Nuvem do Governo e colaboraria com CIOs dos órgãos e das entidades dos setores

públicos federais, estaduais e municipais, negociaria com especialistas do setor privado e manteria contatos com organismos internacionais para identificar e priorizar padrões e diretrizes de computação em nuvem, atuando com papel similar ao do *National Institute of Standards and Technology – NIST*, do governo americano.

- A Secretaria Especial de Desburocratização, Gestão e Governo Digital, do Ministério da Economia, e o Conselho Nacional de Justiça (CNJ) desenvolveriam normas, roteiros, processos e guias para a aquisição de serviços em nuvem para o governo, bem como orientariam a adoção da nuvem por todo o governo, identificando tecnologias de nuvem de última geração e compartilhando casos de negócios relativos aos processos de licitação e modelos reutilizáveis. Ambos atuando com papel similar ao do Conselho Federal de CIOs do governo americano – o Ministério da Economia no âmbito do Poder Executivo Federal e o CNJ no âmbito do Poder Judiciário.
- O GSI (Gabinete de Segurança Institucional) monitoraria problemas de segurança operacional relacionados à nuvem, atuando com papel similar ao do *Department of Homeland Security – DHS*.
- O TCU acompanharia a implementação da Estratégia Nacional, caso ela se tornasse uma política de governo, com metas e compromissos estabelecidos, atuando de forma similar à do *General Accountability Office* (GAO), órgão americano de controle externo, que publicou relatórios bienais acerca dos resultados e das dificuldades de implementação do *Cloud First* americano.
- Os órgãos públicos seriam responsáveis por avaliar suas

estratégias de contratações para considerar totalmente as soluções de computação em nuvem.

Principalmente pela inércia dos OGS em ultrapassar as trincheiras dos mitos culturais e ritos nostálgicos que envolvem a contratação de serviços de tecnologia da informação, ainda há muito a ser feito para que os cidadãos recebam serviços de melhor qualidade, suportados com tecnologias modernas e acessíveis. Mas, felizmente, não há grande complexidade envolvida, pois bastam vontade, compromisso e envolvimento de todas as partes interessadas.

Outros serviços – tais como: "desenvolvimento de soluções por fábrica de *software*", "segurança da informação de maneira geral", "suporte técnico local" etc. – já foram considerados complexos e até inadequados para a terceirização, posto que envolviam atividades que "só poderiam ser realizadas por servidores de carreira". Hoje, são serviços amplamente terceirizados, sem qualquer indicativo de riscos irremediáveis.

Por isso, consideramos que a desmistificação dos serviços em nuvem computacional passa por um processo ágil de contratação, para começar logo e pequeno, para depois evoluir rápido e de forma constante.

Contribuindo com essa aceleração da adoção de serviços em nuvem computacional, detalhamos – na sequência – a proposta do "Processo Primeira Nuvem".

O Processo Primeira Nuvem

Este guia orientador contempla as principais atividades que as áreas de TI devem seguir para auferir os benefícios que a nuvem computacional poderá trazer para a eficiência, eficácia e economicidade dos órgãos públicos.

O nome "Primeira Nuvem" indica que o órgão ainda não adquiriu maturidade para a condução de projetos de adoção de serviços em nuvem computacional e pretende iniciar com um caso de negócio mais simples, mas buscando o rápido amadurecimento.

As atividades previstas no guia orientam o gestor público a seguir um caminho mais simples e bem pavimentado de boas práticas. O resultado almejado é um contrato de serviço em nuvem bem gerido e que apresenta ganhos de qualidade e segurança, com potencial redução de custos em médio e longo prazos.

Um órgão/entidade do setor público que já esteja utilizando serviços em nuvem também poderá usar o Processo Primeira Nuvem em outro caso de negócio ou que envolva outros tipos de serviço.

No detalhamento das fases, serão oferecidos exemplos e modelos que auxiliem os órgãos públicos no entendimento e na execução das atividades.

O Processo Primeira Nuvem é dividido em três fases:

- Fase 1 – Preparação do Projeto para Serviços de Nuvem.
- Fase 2 – Gerenciamento dos Serviços em Nuvem Computacional.
- Fase 3 – Acompanhamento Estratégico do Projeto de Adoção de Nuvem.

Fase 1 – Preparação do Projeto para Serviços de Nuvem

Para Vivek Kundra, CIO do Governo Barack Obama, a "computação em nuvem fornece três fontes principais de valor: eficiência, agilidade e inovação"[17], pontos extremamente importantes para os órgãos do governo brasileiro que pretendem entregar melhores serviços públicos.

Os ganhos de eficiência na utilização de serviços em nuvem podem ocorrer pela utilização maciça de tecnologias de virtualização, flexibilidade na alocação e desalocação de recursos computacionais e, principalmente, com a redução dos custos com mão de obra especializada. A natureza de alguns custos mudará de investimento em infraestrutura de *hardware* e *software* (*CapEx*) para um modelo de serviços em nuvem com pagamento por consumo (*OpEx*), a depender do modelo de implantação em nuvem que está sendo usado.

A opção por serviços em nuvem dá agilidade aos usuários de TI, considerando-se a possibilidade de aumentar/diminuir a capacidade de processamento de determinados serviços. Exemplos de longos *upgrades* de sistemas, demorados processamentos de análise de dados, entre outros, podem ter o tempo de execução diminuído mediante o acréscimo de memória, processamento ou armazenamento de dados, que serão decrescidos após a conclusão dos serviços.

Os órgãos públicos, por meio de projetos de inovação, podem experimentar tecnologias disponíveis no ambiente da nuvem – a exemplo de Aprendizado de Máquina, *Deep Learning* e Internet das Coisas (IOT) –, avaliando os benefícios e o valor agregado, tudo isso dentro do mesmo contrato de serviços em nuvem e pagando por consumo.

A primeira fase envolve a criação do projeto para a adoção de serviços em nuvem computacional, focando na migração de algumas soluções e na possibilidade de experimentar tecnologias inovadoras disponíveis no portfólio do provedor de nuvem.

O projeto poderá ser conduzido pela área de TI, de governança ou de planejamento do órgão. O mais importante é que o setor responsável pelo projeto tenha legitimidade perante a alta administração e boa interlocução com as áreas de negócios.

Etapa 1.1 – Elaborar projeto para adoção de serviços de nuvem

Atividade 1.1.1 – Criar equipe de nuvem

A criação de uma equipe de nuvem é muito importante para o desenvolvimento e a condução do projeto para a Primeira Nuvem, o qual chamaremos "Projeto Primeira Nuvem". A dedicação dos membros dessa equipe permitirá a internalização de conceitos e boas práticas, bem como a convergência de ações de TI que podem ser implementadas de forma melhor por meio da adoção de serviços em nuvem computacional.

Recomenda-se a alocação de pelo menos duas pessoas, mesmo que em tempo parcial, mas – havendo maior disponibilidade de pessoal – seria interessante a alocação de membros da área de TI com conhecimento em infraestrutura, segurança da informação e licitações/contratos, posto que esses assuntos têm consumido muito do esforço das equipes de nuvem. Também deve ser enfatizada a participação de representantes das áreas de negócios, que seriam mais favorecidas com os serviços em nuvem, considerando-se que, atualmente, cada vez mais representantes dessas áreas estão envolvidos nas decisões de TI.

Atividade 1.1.2 – Capacitar a equipe de nuvem e gestores e técnicos envolvidos no projeto

Todos os participantes da equipe de nuvem devem ter capacitação técnica para conduzir o Projeto Primeira Nuvem. Além deles, é importante convidar para participar dos cursos outros funcionários da TI, representantes das áreas de negócios que serão favorecidas com os novos serviços, representantes da área jurídica e da área de licitações, além da relevante participação de membros da alta administração.

Essa capacitação envolve saber o que é (e o que não é) computação em nuvem, estabelecer uma terminologia comum entre os interlocutores do órgão e, principalmente, desmistificar a adoção desse tipo de serviço nos aspectos de segurança, SLA, licitação, governança etc.

Cursos específicos sobre segurança das informações em ambiente de nuvem computacional e sobre contratação de serviços em nuvem são importantes para acelerar a implantação do serviço.

Enfim, uma equipe de nuvem preparada dá, ao órgão, maior agilidade na implementação de serviços em nuvem, maior capacidade para negociar SLAs e maior segurança para o gerenciamento da mudança e dos riscos inerentes ao processo de adoção de serviços em nuvem.

Atividade 1.1.3 – Preparação da justificativa e escopo do projeto

A preparação da justificativa deve se pautar no conjunto de benefícios que os serviços em nuvem trazem para os órgãos públicos, assim como focar nos objetivos do planejamento estratégico de TI dos órgãos que serão favorecidos com a adoção desses serviços e, ainda, na possibilidade de adoção de tecnologias inovadoras disponíveis no portfólio de serviços do provedor de nuvem.

Ganha-se muito tempo se, desde o início, houver o envolvimento da alta administração, que deve apresentar informações sobre suas expectativas quanto aos serviços em nuvem: quais melhorias são esperadas para os serviços atuais, que negócios finalísticos almejam implementar ou alavancar e qual é o nível de riscos que aceitam ter no Projeto Primeira Nuvem.

O escopo do projeto deve fornecer orientações gerais para a adoção da nuvem, incluindo postura quanto à segurança e privacidade de dados, políticas de manutenção e localização de

dados, descrição do nível de maturidade da equipe de TI e da cultura das áreas de negócios quanto a inovações tecnológicas etc.

É importante registrar no projeto que as atividades envolvem um "ciclo evolutivo de maturidade em nuvem", em que se busca fazer o que é certo, mas ciente dos riscos de erros para, rapidamente, corrigi-los e amadurecer. Neste ciclo, o Projeto Primeira Nuvem permitiria a adoção rápida e simples da nuvem, trazendo maturidade para a equipe de TI e para todas as áreas da organização. Depois, um segundo ciclo implementaria outro projeto com funcionalidades mais complexas e maiores desafios, mas, por outro lado, maiores benefícios para o órgão e seus clientes.

Recomenda-se, ainda, registrar no escopo do projeto que haverá a aplicação de um modelo de decisão simplificado (alto valor agregado x baixo risco inerente x custos compatíveis) para escolher as soluções (*workloads*) piloto para migração para nuvem, explicitando que será vedada a seleção de *workloads* que apresentem óbices de segurança da informação ou sejam contraindicados por apresentarem problemas de interdependência de dados ou sistemas.

Atividade 1.1.4 – Estimar os ganhos financeiros, negociais ou sociais do projeto

Para estimativa dos ganhos financeiros, recomenda-se inferir sobre a economia que será auferida com a mudança de abordagem de aquisição de bens relativos à infraestrutura "*on-premises*" orçada pelo pico, para a abordagem de "pagamento por consumo", por meio da contratação de serviços na nuvem. Ou seja, se em média usam-se apenas 50% dos processadores alocados a um serviço na infraestrutura *on-premises* – por exemplo, 60 dos 120 processadores alocados –, devem-se usar como custo estimado do processamento na nuvem apenas 60 processadores

similares. Mas deve-se usar como base de comparação o custo dos 120 processadores *on-premises* (considerando-se que eles não podem ser alocados a outros *workloads* para garantir a disponibilidade nos momentos de pico), somado ao custo estimado com energia, espaço físico e pessoal para garantir que esses processadores estejam disponíveis. Caso você ache 50% um número muito baixo, a média encontrada no governo americano foi de 30% (em 2011!). É preciso medir o uso da nossa infraestrutura real para identificar qual é o percentual de ociosidade. Embora não seja fácil estimar o custo proporcional do espaço físico utilizado e do pessoal necessário, ele tem de ser citado na motivação e pode ser utilizado como argumento pró-nuvem caso o valor do custo da nuvem fique próximo, mas um pouco acima.

Os ganhos relativos aos negócios podem ser identificados pela expectativa de melhoria nos serviços relacionados às atividades finalísticas do órgão.

Mas os ganhos mais relevantes do Projeto Primeira Nuvem estão relacionados à internalização da tecnologia de serviços em nuvem, à flexibilidade que traz para gestão de TI (incluindo a possibilidade de realocar parte da equipe para atuações mais nobres que a simples operação de tecnologia) e à agilidade na introdução de tecnologias emergentes e disruptivas.

Atividade 1.1.5 – Identificar os riscos associados ao projeto

A identificação dos riscos do projeto tem o objetivo de atuar fortemente no atingimento dos resultados esperados, seja por meio da redução da probabilidade de ocorrências indesejadas, seja pela redução dos impactos ao projeto, caso ocorram.

Alguns dos riscos comuns, relacionados com a adoção de Computação em Nuvem, são:

- Baixo engajamento do pessoal que gerencia a infraestrutura *on-premises* – Embora este seja um comportamento esperado, é importante mapear o impacto no projeto, uma vez que, na contratação e implementação de IaaS, informações precisas da operação de *data center* são de suma importância.
- Indefinição acerca das ações suficientes para atender aos requisitos de segurança da informação – Um dos principais receios na adoção de nuvem é criar-se um passivo para o gestor de TI caso alguma obrigação normativa seja descumprida. É importante mapear esse risco e abrir uma frente de discussão sobre a abordagem inicial com a nuvem para que a segurança seja tratada de forma adequada e não seja um impeditivo ao uso da plataforma.
- Governança e gestão de custos, desde a orçamentação até a execução contratual – Principalmente no caso de migração de serviço (ou de infraestrutura) existente para a nuvem, é preciso contextualizar o momento da migração em meio aos ciclos de renovação de ativos (servidores, armazenamento, licenciamento, subscrições), de forma a não incorrer em duplicidade de compra. Isso pode significar uma redução de volume na renovação de infraestrutura com a consequente alocação, para o projeto de nuvem, do valor referente à redução. Em relação à governança, é preciso mitigar o risco de exaurimento precoce do orçamento contratual, dada a nova dinâmica de pagamento por uso, que precisa ainda ser aculturada nas organizações.

Esteja atento à probabilidade de que esses riscos ocorram na sua organização (além de outros riscos inerentes ao uso de

novas tecnologias) e implemente uma resposta para cada risco encontrado em acordo com o processo de gestão de riscos em vigor na organização.

Atividade 1.1.6 – Estimar os prazos do projeto

A criação de uma Estrutura Analítica do Projeto (EAP) permitirá a decomposição hierárquica do trabalho a ser executado pela equipe de nuvem, detalhando em tantas atividades quantas sejam necessárias para se alcançarem os objetivos e se cumprir o escopo do projeto. Em cada nível descendente da EAP, deve-se ter registrado um nome que bem caracterize a atividade, os entregáveis, os prazos, os responsáveis, os riscos e os fatores críticos de sucesso.

O prazo do projeto deve ser compatível com a expectativa da alta administração, com a maturidade da equipe e com a quantidade de membros alocados integralmente ao projeto.

Inspirado no artigo da ISACA "Governança da nuvem: perguntas que os conselhos diretores precisam fazer" (43), listamos alguns questionamentos a serem feitos na análise do tempo necessário à implantação de um Projeto Primeira Nuvem de um órgão:

- A implantação de computação em nuvem entrará em conflito com a cultura do órgão?
- Faltam habilidades necessárias nas equipes do órgão?
- Processos relacionados à nuvem entrarão em conflito com processos estabelecidos?
- A estrutura organizacional prejudica a efetividade ou eficiência do uso da nuvem?

Atividade 1.1.7 – Apresentar projeto à alta administração

Ter o patrocínio da alta administração do órgão é um fator crítico de sucesso para a adoção de nuvem, pois isso ajuda a diminuir as resistências internas e a aumentar os recursos disponíveis à empreitada. Caso a alta administração não seja acessível, mas a área de TI tenha autonomia de gestão, tanto estratégica quanto financeira, é possível propor a adesão como um projeto de inovação ou mesmo como parte de um novo serviço a ser disponibilizado.

Quando viável, a apresentação do projeto à alta administração deve ser precedida de um estudo sobre as expectativas dos membros e sobre as perspectivas do órgão. Desse modo, a equipe de nuvem deverá identificar quais seriam os principais objetivos com a adoção de serviços em nuvem, tais como:

- Melhorar os produtos e serviços atuais.
- Desenvolver novos produtos ou serviços.
- Aumentar a produtividade.
- Reduzir custos.
- Superar barreiras geográficas.

Etapa 1.2 – Escolher os *workloads* candidatos à migração para nuvem

Atividade 1.2.1 – Levantamento das soluções passíveis de migração para nuvem

Para o Projeto Primeira Nuvem, não há necessidade de levantamento exaustivo de sistemas, soluções ou negócios passíveis de migração para nuvem computacional, pois, no primeiro "Ciclo Evolutivo de Maturidade em Nuvem", são mais importantes a

capacitação da equipe de nuvem e das demais partes interessadas e o aculturamento na plataforma.

Assim, recomenda-se que sejam selecionados *workloads* (sistemas, soluções, infraestrutura etc.) que permitam esse aprendizado, que permitam avaliar a eficácia da tecnologia e a comparação de custos, riscos e benefícios envolvidos.

Boas práticas recomendam "Estratégia *Rehost* (*Lift and Shift*)", que significa escolher soluções autocontidas, com pouca ou nenhuma dependência com outros ativos da infraestrutura *on-premises*, e migrá-la para o ambiente de nuvem, de modo que sua migração permita uma adequada avaliação do processo e comparação das tecnologias disponíveis. Outros exemplos de *workloads* que podem ser escolhidos para compor o primeiro ciclo são *backups* de arquivos com prazo longo de retenção, ambientes de desenvolvimento e testes, *hotsites* independentes.

Entrevistas com representantes das áreas de negócios darão uma boa visão de soluções candidatas que tenham alto valor agregado e baixo risco de migração.

Atividade 1.2.2 – Análise das soluções candidatas a migração para nuvem

Para cada solução selecionada recomenda-se que seja realizada uma análise técnica dos impactos relativos à migração, desenvolvendo-se um modelo funcional da solução no novo ambiente com base na arquitetura tecnológica da nuvem.

É importante que seja realizada uma análise dos riscos de migração, de forma que contemple os processos e fluxos de negócios que poderão ser interrompidos e afetados.

Deverão ser excluídos da lista de *workloads* candidatos as soluções que apresentem dados com restrição de acesso, confidencialidade

ou qualquer óbice relativo à segurança da informação. Não se recomenda trazer ao Projeto Primeira Nuvem complexidade que envolva essas questões.

Também deverão ser excluídos os *workloads* que sejam interligados com outros sistemas que não serão migrados, pois a interdependência entre uma solução local e outra na nuvem poderá trazer riscos e complexidades não desejáveis na primeira fase do "Ciclo Evolutivo de Maturidade em Nuvem". Por exemplo, ao se criarem na nuvem ambientes de desenvolvimento, dando-se autonomia aos desenvolvedores e desalocando-se os ambientes *on-premises* que ficam ociosos boa parte do tempo, é preciso verificar se as dependências (base de dados de desenvolvimento, conjuntos de arquivos, entre outros) também estarão disponíveis, se é necessária mudança de nomes e de endereços físicos e lógicos etc.

Atividade 1.2.3 – Estimar custos para migração de cada *workload* candidato

Considerando-se que um Projeto Primeira Nuvem envolve atividades iniciais de montagem da infraestrutura em nuvem e preparação da equipe de nuvem, recomenda-se segmentar os custos iniciais de preparação para a migração para nuvem, dos custos com a migração de *workloads* candidatos.

Focando na preparação do órgão para migração para um ambiente em nuvem computacional, relacionamos alguns exemplos de custos, inspirados em guias da CSCC[10]:

- Custo de desenvolvimento de habilidades de computação em nuvem – resume-se a treinamento da equipe de nuvem, de TI, de licitações/contratos e das demais áreas

envolvidas, principalmente as áreas de negócios dos *workloads* candidatos.

- Ferramentas/serviços/processos adicionais – são custos de serviços ou ferramentas para otimizar os trabalhos das equipes de nuvem, como o custo de licenciamento de um orquestrador de nuvem, ferramenta que automatiza a criação de serviços em um ou mais provedores de nuvem, evitando que a equipe conheça em detalhes as interfaces dos provedores.
- Gerenciamento de serviços – refere-se às atividades de monitoramento dos serviços de nuvem prestados pelo *broker*/provedor.

Quando o foco está no *workload* candidato, os custos dependem da característica da solução e dos objetivos da migração para nuvem, porém podemos apresentar alguns exemplos inspirados em guias da CSCC[10]:

- Custos contínuos do serviço em nuvem – são os custos inerentes aos serviços de nuvem após a implantação, como o custo de armazenamento de dados, de uso de servidores virtuais, de transferência de dados.
- Redesenho de aplicativos – serviço técnico, implementado por fornecedor (*broker*, fábrica de *software*) ou pela equipe interna, que adapta a aplicação a ser migrada às tecnologias disponíveis no provedor de nuvem contratado.
- Implantação e teste de aplicativos.
- Manutenção e administração de aplicativos.
- Integração de aplicativos.

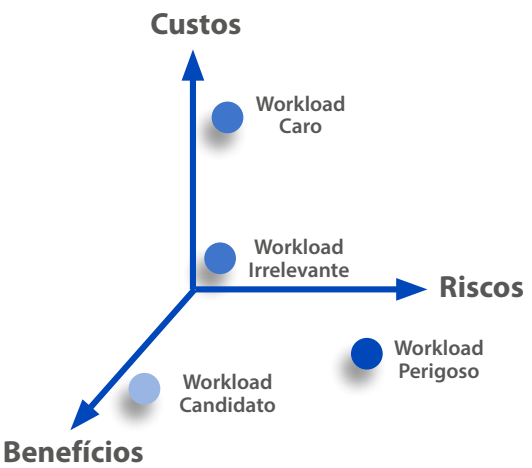
É importante realizar um bom exercício de estimativa de custos e registro da memória de cálculo, mas sempre lembrando que esses valores servirão, principalmente, para a escolha de *workloads* para a migração.

Atividade 1.2.4 – Aplicar modelo de decisão simplificado na escolha de *workloads*

Considerando-se que o resultado do levantamento de soluções candidatas à migração poderá identificar um número relativamente grande de *workloads*, recomenda-se aplicar um modelo de decisão simplificado, priorizando-se aqueles que entregam mais benefícios com baixo risco e menos custos.

A figura a seguir apresenta possíveis tipificações de *workloads* em relação aos benefícios, riscos e custos de migração para o ambiente de nuvem computacional.

Figura 9. Tipificação de *workloads* em relação aos benefícios, riscos e custos de migração



Aplicando-se análise quanti-qualitativa de benefícios, riscos e custos da migração de workloads para nuvem computacional encontram-se combinações que podem ser expressas em quatro tipos básicos:

- workload caro – aquele que apresenta altos custos de migração para nuvem, que não são compensados pelos benefícios para a organização.
- workload perigoso – aquele que apresenta alto risco de migração para nuvem, independentemente dos benefícios que possa trazer para a organização.
- workload irrelevante – aquele que apresenta baixo benefício para organização se migrado para a nuvem.
- workload candidato – aquele que apresenta alto benefício, baixo risco e razoáveis custos de migração para o ambiente de nuvem computacional.

Assim, as melhores soluções para migração (*workload* candidatos) são aquelas que entregam maiores resultados em seus processos de negócios, apresentam os menores riscos e dispendem os menores custos para migração para o ambiente de nuvem. As soluções caras, perigosas e irrelevantes devem ser descartadas nos processos de seleção de *workloads*.

Os benefícios que o *workload* entrega ao negócio devem ser apurados a partir de registros contábeis ou por meio de entrevistas aos responsáveis pelas áreas de negócios envolvidas. Esses benefícios podem representar o aumento de receitas ou a redução de despesas, mas também podem expressar a melhoria dos serviços públicos para os cidadãos ou benefícios de cunho social.

Os riscos envolvidos, por outro lado, devem ser medidos de modo mais amplo e aprofundado, pois envolvem impactos ao negócio. As

soluções candidatas que suportam negócios críticos não devem ser priorizadas, pois a mudança de ambiente de processamento pode gerar problemas como interrupção dos serviços, lentidão, perda de dados etc. Vários outros riscos tecnológicos podem envolver a migração para serviços em nuvem; por isso, cabe à equipe de nuvem antecipar esses problemas e identificar ações paliativas e mitigadoras.

Os custos estimados de migração para a nuvem são importantes, pois a falta de recursos pode inviabilizar a conclusão do projeto, mas devem-se sopesar os custos contra os benefícios com a migração. Um projeto orçamentário bem desenhado pode encantar a alta administração e angariar recursos extras para a migração de mais *workloads* já na primeira fase do Ciclo Evolutivo de Maturidade em Nuvem.

Uma vez estimados os valores relativos a benefícios e custos, bem como o nível de exposição a riscos para cada *workload,* elabora-se uma planilha estabelecendo-se um peso para os riscos: alto, médio e baixo. O peso depende diretamente do apetite a riscos da alta administração. Os valores atribuídos ao peso dos riscos elevarão os valores dos benefícios na situação inversa: quanto mais "alto o risco", menor o "peso do risco".

A tabela a seguir apresenta um exemplo no qual foram atribuídos peso 3 para risco baixo, peso 2 para risco médio e peso 1 para risco alto.

Tabela 3. Exemplo de análise de riscos

***Workload* candidato**	**Benefício (A)**	**Peso do risco (B)**	**Custos (C)**	**Valor final A x B - C**
X	10.000,00	Alto (1)	100,00	9.900,00
Y	3.000,00	Baixo (3)	100,00	8.900,00
Z	2.000,00	Médio (2)	400,00	3.600,00

Valores em R$ mil.

Outra maneira mais simples seria a exclusão de *workloads* com nível de risco alto ou médio, ficando para a primeira fase do ciclo somente aqueles de baixo risco para a migração. Nesse caso, o valor final é apurado com base nos benefícios menos os custos associados à migração.

Qualquer que seja a alternativa escolhida, o valor final resultante será classificado em ordem decrescente, para que a alta administração possa decidir qual é o valor orçamentário que será disponibilizado para o projeto e, por consequência, quantos e quais *workloads* serão migrados.

Ao valor de migração de *workloads* serão acrescidos os custos fixos relacionados à preparação para migração para um ambiente em nuvem computacional.

Atividade 1.2.5 – Contratar serviços de nuvem computacional

Definido o orçamento e escolhidos os *workloads* que serão migrados, chega a fase de contratação dos serviços para a Primeira Nuvem, que contempla:

- Planejar a contratação.
- Elaborar a análise de viabilidade técnica.
- Identificar a melhor estratégia que envolva *broker*/provedor.
- Definir padrões de segurança, desempenho, interoperabilidade e portabilidade necessários.

A tabela a seguir apresenta um conjunto de ações e atividades que podem ser utilizadas para apoiar o planejamento da contratação.

Tabela 4. Ações e atividades para o planejamento das contratações

Ações	Atividades
Realizar análise de viabilidade	- Mapear os benefícios do *workload* escolhido em comparação com a hospedagem *on-premises*. - Analisar os custos envolvidos entre o ambiente *on-premises* e o serviço de nuvem: manutenção, integração, gerenciamento, recursos humanos, sustentação da aplicação e outros.
Avaliar o impacto	- Analisar a criticidade do serviço para a organização. - Mapear o impacto da migração em relação à disponibilidade, ao desempenho, à segurança, à conformidade, à necessidade de respostas e à escalabilidade, entre outros.
Analisar a criticidade da aplicação	- Avaliar aspectos relacionados à continuidade dos serviços, à criticidade dos dados armazenados e aos requisitos de latência.
Considerar o ambiente de TI existente	- Identificar estratégias para garantir que o serviço migrado continuará a cumprir os padrões existentes. - Validar o impacto do modelo de suporte operacional vigente com o adotado na nuvem. - Identificar estratégias para interoperar as informações nos dois ambientes, caso seja necessário. - Prospectar no mercado as melhores relações "custo x benefício" baseadas no modelo de negócio atual.
Buscar conformidade com os requisitos legais	- Observar as orientações dos marcos regulatórios brasileiros e os acórdãos do TCU. - IN 1/2019 (Ministério da Economia)[31], para o Poder Executivo Federal. - Resolução CNJ/182 [34], para o Poder Judiciário. - Norma GSI-NC 14/IN01/DSIC/GSIPR[30]. - Norma GSI-NC 19/IN01/DSIC/GSIPR[35].

Ações	Atividades
Analisar riscos	Identificar os principais riscos relativos: - ao orçamento; - à indisponibilidade do serviço; - à confidencialidade e à integridade dos dados; - às necessidades de mudanças; - à segurança; - à gestão contratual; - à dependência do fornecedor; e - às falhas na execução contratual.

Os requisitos de segurança que devem constar do projeto básico para a contratação dos serviços envolvem (mas não se limitam a):

- cumprimento estatutário de leis, regulamentos e normas governamentais;
- requisitos de proteção dos dados, privacidade e confidencialidade, protegendo contra o acesso acidental e intencional à informação;
- integridade para garantir que os dados sejam autorizados, completos e precisos;
- políticas de acesso para determinar onde os dados podem ser armazenados e quem pode acessar os locais físicos;
- requisitos de transparência, controles de segurança e gerenciamento que viabilizem o monitoramento de maneira apropriada e independente.

Podem ser acrescidos serviços de suporte administrativo e treinamento técnico, abordando tópicos como as horas diárias de suporte principal, os tempos de escalonamento de problemas, a resolução de problemas recorrentes e os métodos de envio de mensagens de problemas.

Devem ser definidos os papéis do contratante, do(s) provedor(es) e do *broker*, se houver, garantindo a responsabilidade pela configuração dos serviços e a segregação de funções com complementariedade de ações. O foco na independência de provedores será um relevante fator crítico de sucesso.

Devem ser incluídos parâmetros claros de nível de serviço (SLAs) envolvendo: segurança, continuidade de operações e qualidade de serviço que atendam às suas necessidades individuais. Também devem ser explicitadas as métricas de medição e monitoramento dos serviços, bem como as consequências por descumprimento dos níveis de serviço estabelecidos.

Devem ser definidas as ações referentes ao fim de contrato e a outros casos de substituição de provedor.

A partir do levantamento realizado, deve-se elaborar um projeto básico, considerando o atendimento às características essenciais dos serviços em nuvem e todos os requisitos levantados junto às áreas intervenientes, de modo a realizar uma pesquisa de preços de mercado.

Com o resultado da pesquisa de mercado, analisam-se os preços médios informados e as sugestões encaminhadas para revisão do projeto básico e encaminhamento às demais instâncias da organização.

Com o processo aprovado, efetua-se a licitação para seleção da melhor proposta.

Fase 2 – Gerenciamento dos serviços em nuvem computacional

Normalmente, a responsabilidade pelo gerenciamento dos serviços em nuvem computacional é da área de TI das organizações; porém, os problemas que decorrem da migração desses serviços para um ambiente de nuvem pública também envolvem terceiros, seja o *broker* ou o(s) provedor(es) de nuvem. Nestes casos, os acordos de

nível de serviço são os parâmetros que regulam o bom andamento das atividades relacionadas ao novo ambiente de TI em nuvem.

Etapa 2.1 – Migrar *workloads* candidatos para nuvem

Atividade 2.2.1 – Treinar equipe técnica nas ferramentas de gerenciamento dos serviços

A primeira atividade no processo de migração para o ambiente de nuvem é o treinamento e a capacitação da equipe técnica nas ferramentas disponíveis no ambiente de nuvem do(s) provedor(es) e na ferramenta de orquestração, caso haja.

O nível de preparação da equipe técnica da organização contratante depende das responsabilidades que lhes foram atribuídas. Se houver opção por um *broker*, boa parte das atividades já será executada pelos profissionais da empresa contratada com essa função.

Havendo impacto nos processos de suporte ao cliente (*service desk*), essas equipes técnicas devem ser preparadas e habilitadas para dar atendimento a partir do ambiente em nuvem.

Além disso, a equipe de nuvem responsável pelo Projeto Primeira Nuvem e pelo monitoramento das atividades de adoção dos serviços em nuvem computacional também deverá participar dos treinamentos que a capacite no cumprimento de suas tarefas.

Atividade 2.2.2 – Preparar e configurar os serviços de nuvem

A configuração dos serviços de nuvem deve ser executada pela equipe técnica diretamente ou por orientação formal ao(s) provedor(es) de nuvem. Caso um *broker* tenha sido contratado, recomenda-se que a equipe técnica acompanhe e valide essas atividades.

Atividade 2.2.3 – Realize uma prova de conceito (POC)

Projetos que envolvem novas tecnologias, principalmente mudança de ambiente de TI, requerem a realização de muitos testes. Portanto, é recomendável a realização de POCs para testes da infraestrutura de nuvem antes da efetiva migração. Para montagem das POCs, entende-se por importante o envolvimento de uma equipe composta pelos seguintes especialistas:

- Tecnologia da Informação – arquitetos, administradores de sistemas, administradores de bancos de dados, desenvolvedores sêniores de recursos de suporte ao cliente (*service desk*).
- Áreas de Negócios – representantes das áreas envolvidas com as soluções a serem migradas e demais partes interessadas.

Apesar dos serviços de nuvem pública fornecerem benefícios como provisionamento e escalabilidade rápidos, é importante que as organizações realizem testes usando um conjunto de dados representativos dos dados de produção. Também é importante reconhecer que os dois ambientes não serão idênticos (mesmo utilizando-se virtualização), o que pode gerar diferenças entre o ambiente "*on-premises*" e o ambiente do POC na nuvem. Essas diferenças devem ser avaliadas e documentadas.

Uma vez que todos os testes tenham sido concluídos e todas as partes interessadas tenham manifestado o "de acordo" quanto às funcionalidades do *workload* no novo ambiente, as atividades de migração podem ter início.

Atividade 2.2.4 – Preparar e migrar os *workloads* para a nuvem

A partir da preparação do ambiente de nuvem, bem como da realização da POC e de testes, devem ser negociadas as datas de migração dos *workloads* com as áreas intervenientes, provedor(es) e *broker*, quando for o caso.

A preparação e a migração envolvem atividades técnicas que devem ser desenvolvidas e/ou acompanhadas pela equipe técnica. Para a transferência de grande volume de dados de produção para o ambiente de nuvem, recomenda-se negociar com o(s) provedor(es) a entrega em dispositivos de armazenamento móveis para carga diretamente em seus *sites*.

Atividade 2.2.5 – Homologar os *workloads* na nuvem, envolvendo as áreas demandantes

A homologação de um novo serviço de nuvem requer a mesma disciplina que a implementação de um serviço *on-premises*. Para o CSCC [(10)], os responsáveis pela homologação do *workload* devem garantir que as seguintes atividades sejam concluídas com sucesso:

- Verificar, em ambiente de teste, se o serviço em nuvem fornece a funcionalidade adequada.
- Verificar se todos os processos funcionam conforme o esperado.
- Verificar as atividades de recuperação de dados, formatação, migração e função de recursos de ETL (extrair, transformar e carregar).
- Verificar a integração com sistemas de gerenciamento e monitoramento.

- Assegurar que o *service desk* possa solucionar dúvidas e problemas rapidamente.
- Verificar o gerenciamento de identidade e acesso no novo ambiente de nuvem.
- Comparar o tempo que as atividades de recuperação de dados e do sistema levam para concluir no novo serviço de nuvem *versus* seu estado atual.

Atividade 2.2.6 – Comunicação de incidentes, gerenciamento de mudanças e recuperação de desastres

No contrato de serviço com o(s) *broker*/provedor(es), deve estar previsto um processo de comunicação de incidentes e respostas. Cada incidente deve ter uma gravidade atribuída, de modo que reflita o impacto e a urgência e um tempo de resposta. Como encaminhamento, é preciso definir quais são o próximo nível de comunicação e a alçada para a solução. Devem estar definidas as situações em que um incidente no ambiente de nuvem necessita ser comunicado ao suporte de TI da organização contratante e vice-versa.

A infraestrutura na nuvem deve estar incluída nos processos existentes da organização, como o gerenciamento de mudanças e a recuperação de desastres. A criação destes processos está relacionada com a gestão operacional de TI da organização e a adoção de computação em nuvem apenas deveria atualizá-los. Caso eles não existam atualmente, é importante criá-los para aumentar a maturidade da gestão da TI da organização e devem-se incluir todos os serviços críticos prestados pela organização, incluindo os serviços em nuvem.

Deve estar clara a definição das responsabilidades do(s) provedor(es), do *broker* e das áreas da organização contratante envolvidas com a gestão de mudanças e com a recuperação de desastres (TI, negócios, comunicação etc.).

Etapa 2.2 – Gerenciar serviços, benefícios, riscos e custos

Atividade 2.2.1 – Gerenciar os custos, os benefícios, a percepção de qualidade dos serviços

A equipe de nuvem, a partir das estimativas e métricas estabelecidas no Projeto de Primeira Nuvem, avaliará os custos dispendidos com a infraestrutura consumida no ambiente de nuvem, bem como os valores dispendidos com os *workloads* migrados.

Os benefícios serão medidos pelos resultados auferidos com a migração, seja pela redução de custos ou elevação de ganhos – financeiros ou sociais. O tempo para avaliação dos benefícios pode ser muito extenso; então, uma projeção a partir da curva de tendência poderá ser utilizada.

A qualidade dos serviços prestados pela solução após a migração deve ser medida a partir da percepção de seus usuários. Para isso, podem ser utilizadas pesquisas qualitativas e/ou o levantamento do número de chamados ao suporte técnico (*service desk*). Os resultados devem ser comparados com as avaliações prévias à migração.

Atividade 2.2.2 – Monitorar riscos, segurança, desempenho e SLA

O gerenciamento do ambiente em nuvem é diferente do tradicional gerenciamento de ativos, uma vez que as características (como provisionamento de recursos e escalabilidade rápida) requerem ações de alocação/desalocação para a redução do consumo e, por consequência, dos custos no novo ambiente.

Para CSCC[10], deve haver mudança de mentalidade nas organizações contratantes, de forma a reorientar o foco para pensar em "serviços" em vez de "ativos". As organizações que fizerem com

sucesso essa transição gerenciarão efetivamente o sistema em direção a métricas de saída (por exemplo, SLAs), em vez de métricas de entrada (por exemplo, número de servidores).

Nessa nova abordagem, as organizações devem monitorar ativamente os SLAs e responsabilizar o(s) provedor(es) e/ou o *broker* (quando for o caso) pelas falhas detectadas. As organizações não devem abrir mão de monitorar as ameaças ou falhas de segurança ocorridas em seu ambiente de nuvem, analisando a efetividade das camadas de proteção e da eficiência de seus provedores de serviço.

As organizações devem rastrear as taxas de uso/consumo para garantir que as tarifas cobradas correspondam aos serviços efetivamente prestados e que não excedam os valores disponíveis em orçamento. Para isso, podem ser desenvolvidas ferramentas de monitoramento de desempenho e medição de consumo para captura direta dessas importantes informações, de forma independente dos sistemas do(s) *broker*/provedor(es).

As organizações contratantes devem considerar o aumento do escopo dos serviços fornecidos pela nuvem à medida que os mercados amadurecem (por exemplo, passar de soluções IaaS para soluções PaaS e SaaS), bem como as tecnologias disponibilizadas pelo(s) provedor(es), como: Internet das Coisas (IoT), Inteligência Artificial (AI) etc.

Fase 3 – Acompanhamento estratégico do Projeto Primeira Nuvem

Para a CIO do governo americano na administração Trump [19], a adoção dos serviços em nuvem computacional normalmente falha quando "as organizações compram soluções sem a identificação adequada dos requisitos e dos resultados pretendidos".

Desse modo, o acompanhamento dos resultados alcançados torna-se fundamental para a retroalimentação do próximo "Ciclo

Evolutivo de Maturidade em Nuvem". As informações do primeiro ciclo auxiliarão no planejamento do segundo ciclo e na definição de objetivos e metas mais desafiadoras.

Nessa fase, a equipe de nuvem exerce um importante papel, pois utilizará todas as informações colhidas no acompanhamento das fases anteriores do projeto.

Etapa 3.1 – Avaliar os resultados do projeto

Atividade 3.1.1 – Levantar problemas identificados na fase 2

Os problemas registrados e coletados pela equipe de nuvem durante as fases anteriores do projeto devem ser compilados e classificados por categorias de riscos, de modo a viabilizar nova avaliação dos riscos a que o projeto está exposto.

Atividade 3.1.2 – Levantar a efetividade dos serviços do(s) provedor(es) e do *broker*

Com base nos registros do gestor de contrato, devem ser apuradas as falhas de cumprimento dos SLAs, bem como os problemas de desempenho dos *workloads* migrados, principalmente sob o ponto de vista do usuário final.

Atividade 3.1.3 – Levantar os custos dispendidos com a migração

Devem ser apurados todos os custos dispendidos com a migração e o processamento dos *workloads* para o ambiente de nuvem. Mais uma vez, a categorização é importante, por possibilitar o redimensionamento para o próximo ciclo.

Atividade 3.1.4 – Analisar ciclos de renovação de infraestrutura *(hardware e software)*

À luz do Plano Diretor de Tecnologia da Informação, recomenda-se verificar a possibilidade de realocar parte do orçamento previsto para contratação de infraestrutura *on-premises*, plataformas de sistemas e licenças de *software*, passando a contratá-los como serviços em ambiente de nuvem computacional.

Atividade 3.1.5 – Elaborar relatório de conclusão do projeto

Por fim, recomendam-se a elaboração do relatório de conclusão do projeto e a apresentação dos resultados à alta administração, com indicação dos próximos passos na Estratégia de Adoção de Serviços em Nuvem Computacional.

Sugerimos certificar-se de abordar os seguintes aspectos:

- Satisfação do usuário – O nível de satisfação dos usuários é um importante critério de sucesso – se os usuários estiverem satisfeitos, as novas implementações serão bem-sucedidas.
- Custos – Indicativo sobre a redução/elevação dos custos com hospedagem e manutenção em ambiente de nuvem, em comparação com os custos em ambiente *on-premises*.
- Resolução de problemas – Tempo médio entre o relato de um *bug* e a resolução do problema pelo *broker* e/ou pelo(s) provedor(es) de nuvem.
- Segurança – A percepção do nível de segurança pelos usuários do sistema, pela área de negócios e pelos membros da equipe de TI. As falhas em segurança devem ser

analisadas e relatadas, com a clarificação das causas e as ações reparadoras.

- Recuperação de desastres – Os testes de recuperação de desastres também têm importância diferenciada e devem ter seus relatos detalhados.
- Monitoramento e relatórios – É importante resumir os principais relatórios de controle do ambiente de nuvem, com gráficos evolutivos das medidas de desempenho e incidência de falhas.

O Projeto Primeira Nuvem deve ser concebido como um processo iterativo, com ciclos que se sucedem em uma espiral, em que cada novo ciclo é melhor (mais maduro) que o anterior, pois se baseia nas experiências adquiridas e, portanto, inicia-se de um patamar mais alto que o anterior. Assim, ao final da atividade 3.1.5, que finaliza a fase 3 do processo, pode-se executar novamente a fase 1, adaptando as atividades à nova realidade da organização pública.

Por exemplo, como a equipe de nuvem já estará criada, a análise deverá verificar se ela tem o tamanho e as capacidades adequadas ao novo ciclo e, caso não tenha, deverá ajustá-la em quantidade e no perfil dos profissionais, assim como elaborar um plano de treinamento para mantê-la atualizada.

A estimativa de benefícios, prazos e custos será baseada nas circunstâncias em que a organização se encontre, assim como de forma a considerar as novas ofertas de serviços em nuvem que foram lançadas ou melhoradas desde que o planejamento anterior foi realizado.

Haverá nova rodada de escolha de *workloads*, que podem ser implementados no contrato vigente ou em uma nova contratação. Essa decisão tem vários fatores a serem considerados, como o tempo restante da vigência contratual, o saldo contratual, a viabilidade da

prorrogação de vigência, entre outros. Sucessivamente, as etapas e atividades do Projeto Primeira Nuvem podem ser executadas de forma diferente em cada novo ciclo, a depender dos resultados do ciclo anterior, das lições aprendidas, da estratégia organizacional e das ofertas do mercado de nuvem pública.

CONCLUSÃO

A computação em nuvem pública, cuja oferta comercial iniciou-se em 2006, é uma plataforma de oferta de serviços de TI que tem características que auxiliam na redução de vários problemas de infraestrutura, na medida em que fornece fácil acesso aos recursos de TI por meio da *internet*, dentro de uma interface padronizada, com rápido provimento, elasticidade de recursos computacionais e pagamento por consumo.

Mas o uso de nuvem pública também traz riscos inerentes, que devem ser gerenciados adequadamente. Os mais citados são a perda de confidencialidade dos dados e outros riscos associados à segurança da informação, o aprisionamento (*lock-in*) pelo fornecedor e o descontrole dos gastos.

Um gestor público responsável não pode se omitir à identificação e ao controle dos riscos inerentes aos serviços em nuvem computacional, mas também não pode ficar alheio aos benefícios que esses serviços trazem às suas organizações. É necessário ter cuidado para não ficar paralisado, postergando a adoção de nuvem, tendo como justificativa os mitos que acentuam os impactos negativos e desconsideram as vantagens no uso dessa tecnologia.

Alguns países, como EUA, Reino Unido, Canadá e Estônia, já implementaram políticas públicas nacionais para incentivar, regulamentar e acompanhar a adoção de nuvem pública por suas agências de governo. O modelo americano, o *Cloud First*, é bastante icônico

e pode servir como referência para o governo brasileiro, como um roteiro para uma adoção de nuvem sustentada em nível nacional.

O CIO americano à época (2011), Vivek Kundra, fez um levantamento da infraestrutura nacional e evidenciou ociosidade de recursos, comprados para atender aos picos eventuais de uso, além de esforços repetidos, na medida em que várias agências adquiriam diferentes soluções para atenderem aos mesmos propósitos, sem que houvesse uma conjunção de esforços. A partir dessas constatações e frente às ofertas de computação em nuvem pública no mercado americano, foram criadas orientações de uso, definidos padrões técnicos para melhorar a interoperabilidade e portabilidade, foi publicado um guia de compras que definiu atributos a serem considerados nas contratações e foram estabelecidas metas, principalmente a de cada agência migrar um serviço para a nuvem pública em até 12 meses e mais dois serviços em até 18 meses. O GAO, similar do TCU para o governo americano, acompanhou a evolução da implementação do *Cloud First* bianualmente, fazendo um registro das principais dificuldades encontradas e emitindo orientações. Em 2018, o modelo foi atualizado para o *Cloud Smart*, com uma mudança de foco para atender prioritariamente a três pilares: segurança, aquisição e habilidades necessárias da força de trabalho.

Assim, com vários países desenvolvidos fazendo uso cada vez maior de nuvem para suportar e melhorar os serviços oferecidos à sociedade, por qual motivo o governo brasileiro tem demorado tanto para aderir à nova plataforma? A resposta é que não há um motivo único, mas diversos fatores.

Apenas em 2011 é que um provedor de nuvem pública iniciou a operação com *data center* em solo brasileiro, a AWS. Antes, para se usar dos serviços de nuvem pública, era preciso contratá-los para uso em *data centers* estrangeiros, principalmente americanos, e muitos

workloads não eram compatíveis com a latência de redes muito maiores que as encontradas nas operações em solo brasileiro. Em 2013, ocorreu o escândalo envolvendo a NSA americana, em que foi revelado que os EUA estavam tendo acesso indevido a comunicações de diversos chefes de Estado, entre eles a então presidente Dilma Rousseff. Ainda em 2013, foi editado o Decreto 8.135 (revogado em dezembro de 2018), que estabelecia que as comunicações de rede e os consequentes armazenamento e recuperação de informações dos órgãos da APF deveriam ser realizados por órgãos ou empresas da própria APF. Esses fatos contribuíram para gerar um clima de insegurança em relação à adoção de computação em nuvem pública com um receio exacerbado de responsabilização pelos órgãos de controle. Como complemento, em 2016, a EC 95[1] (que instituiu um teto de gastos da administração pública por 20 anos) motivou uma antecipação dos procedimentos de compra de infraestrutura de *hardware* e *software* das organizações públicas, aumentando os estoques de ativos de TIC e, consequentemente, aumentando o receio de se adotar a nuvem pública e ser questionado por estar duplicando gastos para os mesmos propósitos. Apenas a partir de 2017, com as contratações do TCU, da ETICE, do MPF e do então Ministério do Planejamento, é que se quebrou a inércia e os gestores passaram a se sentir mais confiantes.

Os sobressaltos não são infundados, merecem atenção e ações adequadas de mitigação de riscos, mas eles não podem paralisar as organizações públicas e postergar indefinidamente o alcance dos benefícios do uso de computação em nuvem para organizações de governo.

É importante a comparação com outros governos para termos uma referência compatível com a nossa realidade e não exagerarmos apenas nos riscos e impactos negativos. Como tomadores de decisão no âmbito da administração pública, é necessário que

façamos uma análise imparcial, com foco na melhoria dos serviços ao cidadão – usuário dos serviços públicos.

O conteúdo deste livro foi organizado de forma a dar uma visão geral da plataforma, dos benefícios, dos riscos e das experiências de outros países. Um ponto fundamental é a desmistificação dos principais impactos negativos que podem advir da adoção de nuvem. O termo 'desmistificação' foi empregado pois as análises mostram que há informações, ações e tecnologias disponíveis que minimizam esses impactos, quando não os eliminam.

Após apresentar uma visão mais realista da adoção de nuvem pública por organizações do governo brasileiro e de quais são as ações necessárias para se adequar ao que a legislação nacional exige, foi esboçado um processo para a rápida adoção de serviços em nuvem como contribuição para o governo brasileiro.

O Processo Primeira Nuvem foi criado com base nas melhores práticas internacionais, considerando-se os aspectos característicos de organizações de governo em relação à gestão de pessoas, à gestão de contratações e ao relacionamento com a alta administração, fatores fundamentais em qualquer processo de adoção de novas tecnologias.

É esperado que a leitura deste livro contribua com a melhoria dos serviços públicos dos órgãos públicos brasileiros, permita a criação de comunidades de prática no âmbito governamental e, enfim, incentive o compartilhamento de conhecimento e a troca de experiências.

Essa troca de informações e casos de sucesso é imprescindível para acelerar o uso da nuvem no governo brasileiro de forma sustentada, gerenciando os riscos e recebendo os benefícios, com foco no usuário dos serviços de governo: o cidadão brasileiro.

Divulgue este livro com outros profissionais de sua rede de relacionamento, e – sobretudo – conte com o nosso apoio.

AUTORES

Breno Costa

Doutorando em Informática pela Universidade de Brasília (UnB). Mestre em Computação Aplicada pela UnB com o tema: Migração de Sistemas Legados do Governo para a Nuvem. Possui 22 anos de experiência na área de TI. É servidor do Tribunal de Contas da União (TCU) desde 2008 e atual Diretor de Relacionamento com Clientes. Contribuiu para a especificação e contratação de serviços multinuvem do TCU e participa das definições e decisões relativas à fiscalização e gestão do contrato.

Geraldo Loureiro

Mestre em Gestão do Conhecimento e da Tecnologia da Informação pela Universidade Católica de Brasília e especialista em Auditoria pela Universidade de São Paulo. Como funcionário do Banco do Brasil S.A., gerenciou equipes de Desenvolvimento de Sistemas e de Auditoria Interna, bem como exerceu a função de Diretor da BB Tecnologia e Serviços. Tem passagem pelo Governo Federal como Diretor de Sistemas e Informação na CGU, quando recebeu 7 prêmios nacionais e internacionais com o Portal da Transparência do Governo Federal. Foi fundador do Capítulo Brasília da ISACA, entidade na qual ocupou o cargo de Presidente por 2 mandatos. Atualmente, é Diretor do Instituto Brasileiro de Governança Pública, empresa que fundou com o objetivo de melhorar os processos de governança do setor público brasileiro.

Antônio Ésio Salgado

Graduação em Engenharia Elétrica pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-RJ 1980) e Mestrado em Eletrônica e Telecomunicações pelo

Instituto Nacional de Pesquisas Espaciais (INPE, 1985). Servidor Público Federal do Instituto Nacional de Pesquisas Espaciais – MCTIC/INPE desde 02/1982, Tecnologista Sênior, atualmente Coordenador de Tecnologia da Informação (COCTI/INPE). Colaborador das equipes de desenvolvimento e especificação de novos modelos de urnas eletrônicas nos projetos conduzidos pelo TSE. Professor Assistente II no Depto. de Informática da Universidade de Taubaté – UNITAU desde 02/1992, disciplinas Redes de Computadores I e II.

Carlos Augusto da Silva

Graduado em Engenharia Civil (UFAM), Especialização em Melhorias de Processo de *Software* (UFLA), MBA Executivo em Gestão de Operações de Serviços (UNB) e Pós-Graduação em Finanças – Gestão de Riscos (FGV). Cursos nas áreas de Auditoria Interna, Controles Internos e Gestão de Pessoas (BB). Exerceu funções de gestão no Banco do Brasil, onde atuou como Coordenador de Auditoria Interna. Atualmente, é Sócio e Diretor do IBGP.

Fernanda Haddad

Servidora pública federal do Ministério da Economia, Analista em Tecnologia da Informação, com ampla experiência em governança e gestão de TIC, contratações de bens e serviços de TIC. Palestrante e consultora na área de contratações de soluções de TI para organizações públicas, disseminando as boas práticas da IN 01/2019 e de legislações correlatas.

Lorena Brasil Cirilo Passos

Mestre em Informática pela Universidade de Brasília (UnB). Desde 2006, é Servidora do Tribunal de Contas da União (TCU), onde exerce o cargo de Diretora de Infraestrutura de TI. Atualmente, é Gestora do Contrato de Serviços Multinuvem do TCU.

Lucio Melre da Silva

Mestre em Gestão do Conhecimento e Tecnologia da Informação pela Universidade Católica de Brasília. Pós-graduado em análise de sistemas e metodologia do ensino superior. Graduado em Direito, Engenharia Civil e Matemática. Servidor de carreira do Superior Tribunal de Justiça, onde exerce o cargo de Analista Judiciário – Informática. Atua na área de Tecnologia da Informação há mais de 30 anos. Atual Diretor da Secretaria de Tecnologia da Informação do Tribunal Regional Federal da 1ª Região. Exerceu funções de gestor em tecnologia da informação em diversos órgãos do Poder Judiciário, dentre eles o Conselho Nacional de Justiça, Supremo Tribunal Federal, Superior Tribunal de Justiça e Conselho da Justiça Federal.

Renato Melo

Mestre em Administração pela PUC Minas. Especialista em Finanças pelo IBMEC-MG (CBA e MBA). Diretor da Blanka Consultoria, atua como instrutor de cursos relacionados ao Setor Público. Exerce atualmente o cargo de Gerente-Geral do Conselho Federal de Química, com passagens como Gerente Financeiro do CAU/BR e Gerente Financeiro do CREA/MG.

Rodrigo Carvalho

Pós-Graduado em Engenharia de *Software* pela Universidade de Brasília. Servidor do Superior Tribunal de Justiça, com mais de 20 anos de experiência na área de TI, atuou em diversos cargos de direção. Como Secretário de Tecnologia da Informação e Comunicação, realizou a primeira implantação de SaaS no Superior Tribunal de Justiça. Atualmente está em exercício no Conselho Nacional de Justiça, atuando na Corregedoria Nacional de Justiça.

APÊNDICE A

Análise dos incisos da GSI-NC 14

Princípios e Diretrizes

Incisos da GSI-NC 14[30]	Ações de conformidade
5.1.1 A prevalência dos direitos e das garantias fundamentais no tratamento das informações pessoais.	Ao elaborar o Termo de Referência (TR) respeitar à Política de Acesso à Informação e à Lei nº 13.709/2018 (proteção aos dados pessoais)[28].
5.1.2 As diretrizes estabelecidas em sua Política de Segurança da Informação e Comunicações (POSIC) e normas complementares.	Revisar a Política de Segurança da Informação e Comunicação (POSIC) do órgão, respeitando o estabelecido nas GSI-NC 01 – Gestão de Segurança da Informação e Comunicações na APF[44], GSI-NC 03 – Diretrizes para a elaboração de Política de Segurança da Informação e Comunicações na APF[45], verificando sua aderência à nuvem e acrescentando no Termo de Referência (TR) a exigência do cumprimento desses requisitos.
5.1.3 As diretrizes relativas à sua Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC).	Em tempo de execução contratual, avaliar os riscos associados a cada uma das cargas de trabalho de acordo com a GSI-NC 04 – Gestão de Riscos de Segurança da Informação e Comunicações na APF[46] e ABNT NBR ISO/IEC 27005:2011 – Gestão de Riscos de Segurança da Informação[51].
5.1.4 As informações tratadas em ambiente de computação em nuvem devem passar por um processo de GRSIC.	Para cada uma das cargas de trabalho (*workloads*), deve ser executado processo definido de acordo com a GSI-NC 04 – Gestão de Riscos de Segurança da Informação e Comunicações na APF[46] e ABNT NBR ISO/IEC 27005:2011 – Gestão de Riscos de Segurança da Informação[51].

Incisos da GSI-NC 14[30]	Ações de conformidade
5.1.5 As diretrizes relativas à sua Gestão de Continuidade nos aspectos relacionados à Segurança da Informação e Comunicações (SIC).	Verificar se os mecanismos de gestão de continuidade de negócios estão aderentes à GSI-NC 06 – Gestão de Continuidade de Negócios na APF[48] e ABNT NBR ISO 22313:2015 – Gestão de Continuidade de Negócios[52], verificando sua aderência à nuvem. Avaliar, para cada carga de trabalho, a necessidade de implementar mecanismos previstos pela Gestão de Continuidade.
5.1.6 As legislações vigentes para contratação de solução de tecnologia da informação.	Elaborar o Termo de Referência de acordo com o definido na IN 1/2019[31], Resolução CNJ Nº 182[34] ou equivalente.
5.1.7 As legislações vigentes relativas à Gestão de Segurança da Informação e Comunicações.	As definições do Termo de Referência e as ações em tempo de execução devem estar aderentes ao definido nas GSI-NC 01 – Gestão de Segurança da Informação e Comunicações na APF[44] e ABNT NBR ISO/IEC 27001:2013 – Sistema de Gestão de Segurança da Informação[39].
5.1.8 As diretrizes para implementação de controles de acesso relativos à SIC.	Os controles de acesso à informação hospedada na nuvem pública devem seguir o preconizado nas normas GSI-NC 07 – Implementação de Controles de Acesso na APF[49] e ABNT NBR ISO/IEC 27001:2013 – Sistema de Gestão de Segurança da Informação[39].
5.1.9 A prevalência da legislação brasileira sobre qualquer outra.	Deve haver cláusula explícita no Termo de Referência e no contrato estabelecido com a definição de "prevalência da legislação brasileira sobre qualquer outra".

Tratamento da Informação

Incisos da GSI-NC 14[30]	Ações de conformidade
5.2.1 Informação sem restrição de acesso: pode ser tratada a critério do órgão ou da entidade da APF em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. *5.2.2 Informação sigilosa: como regra geral, deve ser evitado o tratamento em ambiente de computação em nuvem, conforme disposições a seguir:* *5.2.2.1. Informação classificada: é vedado o tratamento em ambiente de computação em nuvem.* *5.2.2.2. Conhecimento e informação contida em material de acesso restrito: é vedado o tratamento em ambiente de computação em nuvem.* *5.2.2.3. Informação com restrição de acesso prevista em legislação vigente: a critério do órgão ou da entidade da APF, pode ser tratada em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. O órgão ou a entidade da APF deve adotar medidas que assegurem a disponibilidade, integridade, confidencialidade e autenticidade (DICA).* *5.2.2.4. Documento preparatório: a critério do órgão ou da entidade da APF, pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. O órgão ou a entidade da APF deve adotar medidas que assegurem a DICA.*	Assim como no ambiente *on-premises*, na nuvem pública, o estabelecido na política de classificação de informação do órgão deve ser seguido. Para cada carga de trabalho candidata ao uso da nuvem pública, deverá ser feita avaliação do nível de classificação dos dados. Caso haja alguma restrição de acesso, deve-se criptografá-los e, se impossível ou oneroso, deve-se desqualificar a carga de trabalho para migração.

Incisos da GSI-NC 14[30]	Ações de conformidade
5.2.2.5. Documento preparatório que possa originar informação classificada deve ser tratado conforme o item 5.2.2.1. *5.2.2.6. Informação pessoal relativa à intimidade, vida privada e imagem: a critério do órgão ou da entidade da APF, pode ser tratada em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. O órgão ou a entidade da APF deve adotar medidas que assegurem a DICA.*	
5.3 Deve ser assegurado que dados, metadados, informações e conhecimento, produzidos ou custodiados por órgão ou entidade da APF, bem como suas cópias de segurança, residam em território brasileiro.	No termo de referência, deve ser estabelecida a necessidade de que o provedor mantenha *data center* em território brasileiro.
5.4 Os dados, metadados, as informações e o conhecimento, produzidos ou custodiados por órgão ou entidade da APF, referentes aos itens 5.2.2.3, 5.2.2.4 e 5.2.2.6, devem residir exclusivamente em território brasileiro.	No termo de referência, deve ser estabelecida a necessidade de que o provedor mantenha *data center* em território brasileiro, de modo que esse tipo de informação possa ser armazenado em território brasileiro.

Incisos da GSI-NC 14[30]	Ações de conformidade
5.5 Na adoção de serviços de computação em nuvem, o órgão ou a entidade da APF deve assegurar que sejam definidos em instrumento contratual ou similar: *5.5.1 Requisitos que garantam a DICA das informações tratadas em ambiente de computação em nuvem.* *5.5.2 Processo de comunicação e tratamento de incidentes de segurança em redes computacionais, considerando as exigências da legislação vigente.* *5.5.3 Requisitos necessários para a realização de auditorias.* *5.5.4 Que os dados, metadados, as informações e o conhecimento, tratados pelo provedor, não poderão ser fornecidos a terceiros e/ou usados por este provedor para fins diversos do previsto no referido instrumento contratual ou similar, sob nenhuma hipótese, sem autorização formal do órgão ou da entidade da APF.* *5.5.5 Requisitos necessários para a continuidade de negócio.* *5.5.6 Requisitos necessários para os casos de cancelamento, descontinuidade, portabilidade e renovação do referido instrumento contratual ou similar, bem como substituição de ambiente, que visem à eliminação e/ou à destruição definitiva dos dados, metadados, das informações e do conhecimento.*	Devem fazer parte do instrumento contratual a necessidade de assinatura de acordo de confidencialidade e também a necessidade de comprovação, por parte do provedor, da existência de um plano de continuidade de negócios em acordo com a norma vigente GSI-NC 06 – Gestão de Continuidade de Negócios na APF[48]. Além disso, em relação ao Plano de Comunicação e Tratamento de Incidentes, deve haver aderência às normas GSI-NC 05 – Criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais[47] e GSI-NC 08 – Gerenciamento de Incidentes de Segurança em Redes de Computadores[50].

Incisos da GSI-NC 14[30]	Ações de conformidade
5.6 É vedado o tratamento de informação em ambientes de computação em nuvem não autorizados pela Alta Administração do respectivo órgão ou entidade da APF.	Apenas soluções homologadas pelo órgão poderão ser utilizadas no ambiente da nuvem pública, ou seja, os serviços contratados devem estar de acordo com a política de utilização dos recursos de TI.

Responsabilidades

Incisos da GSI-NC 14[30]	Ações de conformidade
6.1 A Alta Administração de cada órgão ou entidade da APF, no âmbito de suas competências, é responsável pela segurança das informações tratadas em ambiente de computação em nuvem, em conformidade com as orientações contidas nesta norma e legislação vigente.	Assim como no ambiente *on-premises*, o gestor de segurança da informação deve participar ativamente das avaliações e eventuais reformulações de práticas e políticas de segurança da informação que visem a abarcar o ambiente da nuvem pública. É necessário que este perfil seja parte do comitê encarregado da implantação de serviços em nuvem pública no órgão.
6.2 O Gestor de Segurança da Informação e Comunicação do órgão, no âmbito de suas atribuições, é responsável pelas ações de implementação da gestão de risco de segurança das informações tratadas em ambiente de computação em nuvem.	Como já citado anteriormente e de acordo com a GSI-NC 04 – Gestão de Riscos de Segurança da Informação e Comunicações na APF[46], o gestor de segurança da informação é o responsável pela gestão de risco de segurança das informações, independentemente de onde elas estejam armazenadas. Portanto, deve participar ativamente da implantação de serviços em nuvem pública.

APÊNDICE B

Lista de Serviços em Nuvem

A seguir, são listados exemplos de serviços de nuvem disponíveis para um consumidor de nuvem computacional, conforme definições do NIST[6].

Serviços de SaaS:

- *E-mail* e produtividade no escritório: aplicativos para *e-mail*, processamento de texto, planilhas, apresentações etc.
- Faturamento: serviços de aplicativos para gerenciar o faturamento do cliente com base no uso e nas assinaturas de produtos e serviços.
- *Customer Relationship Management* (CRM): aplicativos de CRM que variam de aplicativos de *call center* à automação da força de vendas.
- Colaboração: ferramentas que permitem aos usuários colaborar em grupos de trabalho, dentro de empresas e entre empresas.
- Gerenciamento de conteúdo: serviços para gerenciar a produção e o acesso ao conteúdo para aplicativos baseados na *web*.
- Gerenciamento de documentos: aplicativos para gerenciar documentos, impor fluxos de trabalho de produção de documentos e fornecer espaços de trabalho para grupos ou empresas para localizar e acessar documentos.
- Finanças: aplicativos para gerenciar processos financeiros que vão desde o processamento de despesas e faturamento até o gerenciamento de impostos.

- Recursos humanos: *software* para gerenciamento de recursos humanos dentro das empresas.
- Vendas: aplicativos projetados especificamente para funções de vendas, como precificação, rastreamento de comissões etc.
- Redes sociais: *software* social que estabelece e mantém uma conexão entre usuários que estão ligados a um ou mais tipos específicos de interdependência.
- *Enterprise Resource Planning* (ERP): sistema integrado baseado em computador usado para gerenciar recursos internos e externos, incluindo ativos tangíveis, recursos financeiros, materiais e recursos humanos.

Serviços de PaaS:

- *Business Intelligence*: plataformas para criação de aplicativos, como *dashboards*, sistemas de relatórios e análise de dados.
- Banco de dados: serviços que oferecem soluções de banco de dados relacional escaláveis ou *datastores* escaláveis não relacionais.
- Desenvolvimento e teste: plataformas para o desenvolvimento e teste de ciclos de desenvolvimento de aplicativos, que se expandem e se contraem conforme a necessidade.
- Integração: plataformas de desenvolvimento para construção de aplicativos de integração na nuvem e dentro da empresa.
- Implantação de aplicativos: plataformas adequadas para desenvolvimento de aplicativos de uso geral. Esses serviços fornecem bancos de dados, ambientes de tempo de execução de aplicativos da *web* etc.

Serviços de IaaS:

- *Backup* e recuperação: serviços para *backup* e recuperação de sistemas de arquivos e armazenamentos de dados brutos em servidores e sistemas *desktop*.
- Computação: recursos do servidor para executar sistemas baseados em nuvem que podem ser provisionados e configurados dinamicamente conforme o necessário.
- *Content Delivery Networks* (CDNs): tecnologia de armazenamento de conteúdo e arquivos para melhorar o desempenho e o custo de entrega de conteúdo em sistemas baseados na *web*.
- Gerenciamento de serviços: serviços que gerenciam plataformas de infraestrutura em nuvem. Essas ferramentas geralmente oferecem recursos que os provedores de nuvem não fornecem ou se especializam no gerenciamento de determinadas tecnologias de aplicativos.
- Armazenamento: capacidade de armazenamento massivamente escalável que pode ser usada para aplicativos, *backups*, arquivamento e armazenamento de arquivos.

REFERÊNCIAS

(1) BRASIL. PRESIDÊNCIA DA REPÚBLICA. "Emenda Constitucional nº 95, de 15/12/2016". Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Emendas/Emc/emc95.htm. Acesso em: 20/abril/2019.

(2) UNITED STATES OF AMERICA. "Cloud Computing Definitions and Solutions", CIO.com, setembro/2009. Disponível em: https://www.cio.com/article/2424886/cloud-computing-definitions-and-solutions.html. Acesso em: 20/abril/2019.

(3) UNITED STATES OF AMERICA. INDEPENDENT DIRECTORS COUNCIL. "Defining 'Cloud Services'- An IDC update", IDC Exchange, Setembro/2009. Disponível em: http://blogs.idc.com/ie/?p-422.

(4) UNITED STATES OF AMERICA. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. "The NIST Definition of Cloud Computing", NIST Special Publication 800-145, NIST - National Institute of Standards and Technology, setembro/2011. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. Acesso em: 20/abril/ 2019.

(5) UNITED STATES OF AMERICA. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. "NIST Cloud Computing Standards Roadmap", NIST Special Publication 500-291, Version 2, NIST - National Institute of Standards and Technology, julho/2013. Disponível em: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909024. Acesso em: 20/abril/ 2019.

(6) UNITED STATES OF AMERICA. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. "Cloud Computing Reference Architecture", NIST - National Institute of Standards and Technology, setembro/2011. Disponível em: https://www.nist.gov/publications/nist-cloud-computing-reference-architecture. Acesso em: 20/abril/ 2019.

(7) "Right Scale Cloud Comparison Tool", Flexera. Disponível em: https://www.rightscale.com/cloud-comparison-tool. Acesso em: 20/abril/ 2019.

(8) BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. "Acórdão TCU 588/2018 - Plenário", TCU – Tribunal de Contas da União, 2017, fonte: https://contas.tcu.gov.br/sagas/SvlVisualizarRelVotoAcRtf?codFiltro=SAGAS-SESSAO-ENCERRADA&seOcultaPagina=S&item0=615513. Acesso em: 20/abril/2019.

(9) UNITED STATES OF AMERICA. INDEPENDENT DIRECTORS COUNCIL. ENTERPRISE PANEL. "Bringing Cloud Into the Enterprise", IDC Enterprise Panel, IDC - INDEPENDENT DIRECTORS COUNCIL, 2009. Disponível em: https://www.eiseverywhere.com/file_uploads/86cde4f4bf015bb8cd2153ea7e0287ff_Day_1_815am_Frank_Gens_Bringing_Cloud_into_the_Enterprise.pdf. Acesso em: 20/abril/2019.

(10) UNITED STATES OF AMERICA. CLOUD STANDARDS CUSTOMER COUNCIL. "Practical Guide to Cloud Computing Version 3.0", CSCC - Cloud Standards Customer Council, dezembro/2017. Disponível em: https://www.omg.org/cloud/deliverables/practical-guide-to-cloud-computing.htm. Acesso em: 20/abril/2019.

(11) UNITED STATES OF AMERICA. INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. "IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud", ISACA, 2011. Disponível em: https://www.isaca.org/chapters2/kampala/newsandannouncements/Documents/IT%20contro%20objectives%20for%20Cloud%20computing.pdf. Acesso em: 20/abril/2019.

(12) UNITED STATES OF AMERICA. INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. "IT Governance and the Cloud: Principles and Practice for Governing Adoption of Cloud Computing", ISACA Journal. Vol. 5, 2011. Disponível em: https://www.isaca.org/Journal/archives/2011/Volume-5/Pages/IT-Governance-and-the-Cloud-Principles-and-Practice-for-Governing-Adoption-of-Cloud-Computing.aspx. Acesso em: 20/abril/2019.

(13) EUROPEAN UNION. EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY. "Cloud Computing Benefits, risks and recommendations for information security – 2.0 ", ENISA - European Network and Information

Security Agency, dezembro/2012. Disponível em: https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security. Acesso em: 20/abril/2019.

(14) AMAZON WEB SERVICES. "Otimização de custo", AWS – Amazon Web Services, página de site, 2019. Disponível em: https://aws.amazon.com/pricing/cost-optimization/. Acesso em: 20/abril/2019.

(15) AMAZON WEB SERVICES. "Calculadoras de custo total de propriedade (TCO) da AWS", AWS – Amazon Web Services, página de site, 2019. Disponível em: https://aws.amazon.com/tco-calculator/. Acesso em: 20/abril/2019.

(16) UNITED STATES OF AMERICA. CARNEGIE MELLON UNIVERSITY. SOFTWARE ENGINEERING INSTITUTE. "12 Risks, Threats, & Vulnerabilities in Moving to the Cloud", SEI - Software Engineering Institute - Carnegie Mellon University, março/2018. Disponível em: https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html. Acesso em: 20/abril/2019.

(17) UNITED STATES OF AMERICA. WHITE HOUSE. "Federal Cloud Computing Strategy", Vivek Kundra, U.S. Chief Information Officer, The White House, fevereiro/2011. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf. Acesso em: 20/abril/2019.

(18) UNITED STATES OF AMERICA. UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE. "Cloud Computing: Additional Opportunities and Savings Need to Be Pursued", GAO - United States Government Accountability Office, setembro/2014. Disponível em: https://www.gao.gov/products/GAO-14-753. Acesso em: 20/abril/2019.

(19) UNITED STATES OF AMERICA. OFFICE OF THE FEDERAL CHIEF INFORMATION OFFICER. "Federal Cloud Computing Strategy: From Cloud First to Cloud Smart", Office of the Federal Chief Information Officer. Disponível em: https://cloud.cio.gov/strategy/. Acesso em: 20/abril/2019.

(20) CANADA. TREASURY BOARD OF CANADA SECRETARIAT. "Government of Canada Strategic Plan for Information Management and Information Technology 2017 to 2021", TREASURY BOARD OF CANADA SECRETARIAT / Government of Canada, 2017. Disponível em: https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/strategic-plan-2017-2021.html#toc8-1-2. Acesso em: 20/abril/2019.

(21) ESTONIA. TALLINN UNIVERSITY OF TECHNOLOGY. "Concept of Estonian Government Cloud and Data Embassies", Tallinn University of Technology, 2015. Disponível em: https://link.springer.com/chapter/10.1007%2F978-3-319-22389-6_11. Acesso em: 20/abril/2019.

(22) INTERNATIONAL DATA GROUP. "2018 Cloud Computing Research - Executive Summary", IDG - International Data Group, 2018. Disponível em: https://www.idg.com/tools-for-marketers/2018-cloud-computing-summary/. Acesso em: 20/abril/2019.

(23) UNITED STATES OF AMERICA. ASSOCIATION FOR COMPUTING MACHINERY. "A View of Cloud Computing", Communications of the ACM - vol. 53 nº 4, ACM - Association for Computing Machinery, abril/2010. Disponível em: https://dl.acm.org/citation.cfm?id=1721672. Acesso em: 20/abril/2019.

(24) UNITED KINGDOM. UK INFORMATION COMMISSIONER'S OFFICE. "Data security incident trends", ICO - UK Information Commissioner's Office. Disponível em: https://ico.org.uk/action-weve-taken/data-security-incident-trends/. Acesso em: 20/abril/2019.

(25) BRASIL. INSTITUTO DE DESENVOLVIMENTO E GESTÃO. "4 formas de prevenir o vazamento de dados", Revista CIO, IDG, agosto/2018. Disponível em: https://cio.com.br/4-formas-de-prevenir-o-vazamento-de-dados/. Acesso em: 20/abril/2019.

(26) GARTNER. "Is the Cloud Secure?", Smarter With Gartner, Gartner, março/2018. Disponível em: https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/. Acesso em: 20/abril/2019.

(27) BRASIL. PRESIDÊNCIA DA REPÚBLICA. "Lei nº 12.527/2011", Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 20/abril/2019.

(28) BRASIL. PRESIDÊNCIA DA REPÚBLICA. "Lei nº 13.709/2018", Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 20/abril/2019.

(29) BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. "Acórdão TCU 1739/2015 – Plenário", TCU – Tribunal de Contas da União, 2015. Disponível em: https://contas.tcu.gov.br/etcu/ObterDocumentoSisdoc?seAbrirDocNoBrowser=true&codArqCatalogado=9145724. Acesso em: 20/abril/2019.

(30) BRASIL. PRESIDÊNCIA DA REPÚBLICA. GABINETE DE SEGURANÇA INSTITUCIONAL. "Norma Complementar nº 14/IN01/DSIC/GSIPR", Brasil, março/2018. Disponível em: http://dsic.planalto.gov.br/assuntos/editoria-c/documentos-pdf-1/portaria-09-gsi-de-9-de-marco-de-2018-nc-14-in01-computacao-em-nuvem.pdf/view. Acesso em: 20/abril/2019.

(31) BRASIL. MINISTÉRIO DA ECONOMIA. "Instrução Normativa nº 01", Ministério da Economia, abril/2019. Disponível em: http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/70267659/do1-2019-04-05-instrucao-normativa-n-1-de-4-de-abril-de-2019-70267535. Acesso em: 20/abril/2019.

(32) UNITED STATES OF AMERICA. CARNEGIE MELLON UNIVERSITY. INFORMATION SECURITY OFFICE. "Guidelines for Data Classification", Information Security Office - Carnegie Mellon University, maio/2018. Disponível em: https://www.cmu.edu/iso/governance/guidelines/data-classification.html. Acesso em: 20/abril/2019.

(33) RIGHTSCALE INC. "Get the RightScale State of the Cloud Report", RightScale Inc., 2019. Disponível em: https://www.rightscale.com/lp/state-of-the-cloud. Acesso em: 20/abril/2019.

(34) BRASIL. CONSELHO NACIONAL DE JUSTIÇA. "Resolução CNJ Nº 182", Brasil, outubro/2013. Disponível em: http://www.cnj.jus.br/atos-normativos?documento=1874. Acesso em: 20/abril/2019.

(35) BRASIL. PRESIDÊNCIA DA REPÚBLICA. GABINETE DE SEGURANÇA INSTITUCIONAL. "Norma Complementar nº 19/IN01/DSIC/GSI/PR", Brasil, julho/2014. Disponível em: http://dsic.planalto.gov.br/legislacao/nc_19_SISTEMAS_ESTRUTURANTES.pdf. Acesso em: 20/abril/2019.

(36) BRASIL. PRESIDÊNCIA DA REPÚBLICA. "Decreto nº 7.724", Brasil, maio/2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Decreto/D7724.htm. Acesso em: 20/abril/2019.

(37) BRASIL. PRESIDÊNCIA DA REPÚBLICA. "Decreto nº 7.845", Brasil, novembro/2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Decreto/D7845.htm. Acesso em: 20/abril/2019.

(38) BRASIL. MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO. SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO. "Portaria MPDG/STI nº 20", Brasil, junho/2016. Disponível em: https://www.governodigital.gov.br/documentos-e-arquivos/legislacao/Portaria%20MP-STI%20no%2020%20de%2014%20de%20junho%20de%202016.pdf/view. Acesso em: 20/abril/2019.

(39) BRASIL. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. "Norma ABNT NBR ISO/IEC 27001:2013", ABNT - Associação Brasileira de Normas Técnicas, 2013. Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=306580. Acesso em: 20/abril/2019.

(40) BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. "Acórdão TCU 2059/2017 – Plenário", TCU – Tribunal de Contas da União, 2017. Disponível em: https://contas.tcu.gov.br/etcu/ObterDocumentoSisdoc?seAbrirDocNoBrowser=true&codArqCatalogado=13414290&codPapelTramitavel=58061318. Acesso em: 20/abril/2019.

(41) INTERNATIONAL CONFERENCE ON CLOUD COMPUTING TECHNOLOGY AND SCIENCE. "Towards Performance Prediction for Public Infrastructure Clouds", IEEE 5th International Conference on Cloud Computing Technology

and Science, dezembro/2013. Disponível em: https://ieeexplore.ieee.org/document/6753834. Acesso em: 20/abril/2019.

(42) UNITED STATES OF AMERICA. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. "Guide for Applying the Risk Management Framework to Federal Information Systems. Revision 1", Special Publication 800-37, NIST - National Institute of Standards and Technology, fevereiro/2010. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final. Acesso em: 20/abril/2019.

(43) UNITED STATES OF AMERICA. INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. "Cloud Governance: Questions Boards of Directors Need to Ask", ISACA, 2013. Disponível em: http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/cloud-governance-questions-boards-of-directors-need-to-ask.aspx. Acessado em: 20/abril/2019.

(44) BRASIL. PRESIDÊNCIA DA REPÚBLICA. GABINETE DE SEGURANÇA INSTITUCIONAL. "Norma Complementar nº 01/IN01/DSIC/GSIPR", Brasil, outubro/2008. Disponível em: http://dsic.planalto.gov.br/legislacao/nc_1_normatizacao.pdf. Acesso em: 20/abril/2019.

(45) BRASIL. PRESIDÊNCIA DA REPÚBLICA. GABINETE DE SEGURANÇA INSTITUCIONAL. "Norma Complementar nº 03/IN01/DSIC/GSIPR", Brasil, junho/2009. Disponível em: http://dsic.planalto.gov.br/legislacao/nc_3_psic.pdf. Acesso em: 20/abril/2019.

(46) BRASIL. PRESIDÊNCIA DA REPÚBLICA. GABINETE DE SEGURANÇA INSTITUCIONAL. "Norma Complementar nº 04/IN01/DSIC/GSIPR", Brasil, fevereiro/2013. Disponível em: http://dsic.planalto.gov.br/legislacao/nc_04_grsic.pdf. Acesso em: 20/abril/2019.

(47) BRASIL. PRESIDÊNCIA DA REPÚBLICA. GABINETE DE SEGURANÇA INSTITUCIONAL. "Norma Complementar nº 05/IN01/DSIC/GSIPR", Brasil, agosto/2009. Disponível em: http://dsic.planalto.gov.br/legislacao/copy_of_nc_05_etir.pdf. Acesso em: 20/abril/2019.

(48) BRASIL. PRESIDÊNCIA DA REPÚBLICA. GABINETE DE SEGURANÇA INSTITUCIONAL. "Norma Complementar nº 06/IN01/DSIC/GSIPR", Brasil, novembro/2009. Disponível em: http://dsic.planalto.gov.br/legislacao/nc_6_gcn.pdf. Acesso em: 20/abril/2019.

(49) BRASIL. PRESIDÊNCIA DA REPÚBLICA. GABINETE DE SEGURANÇA INSTITUCIONAL. "Norma Complementar nº 07/IN01/DSIC/GSIPR", Brasil, julho/2014. Disponível em: http://dsic.planalto.gov.br/legislacao/nc_07_revisao_01.pdf. Acesso em: 20/abril/2019.

(50) BRASIL. PRESIDÊNCIA DA REPÚBLICA. GABINETE DE SEGURANÇA INSTITUCIONAL. "Norma Complementar nº 08/IN01/DSIC/GSIPR", Brasil, agosto/2010. Disponível em: http://dsic.planalto.gov.br/legislacao/copy_of_nc_8_gestao_etir.pdf. Acesso em: 20/abril/2019.

(51) BRASIL. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. "Norma ABNT NBR ISO/IEC 27005:2011", ABNT - Associação Brasileira de Normas Técnicas, 2011. Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=89327 . Acesso em: 20/abril/2019.

(52) BRASIL. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. "Norma ABNT NBR ISO 22313:2015", ABNT - Associação Brasileira de Normas Técnicas, 2015. Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=345105. Acesso em: 20/abril/2019.

(53) COSTA, Breno Gustavo Soares da. Uma proposta de migração de sistemas legados do governo para a nuvem. 2018. [110] f., il. Dissertação (Mestrado Profissional em Computação Aplicada)—Universidade de Brasília, Brasília, 2018. Disponível em http://repositorio.unb.br/handle/10482/34321. Acesso em: 24/maio/ 2019.

(54) BRASIL. PRESIDÊNCIA DA REPÚBLICA. GABINETE DE SEGURANÇA INSTITUCIONAL. "Instrução Normativa Nº 1 GSI/PR", Brasil, junho/2008. Disponível em: http://dsic.planalto.gov.br/legislacao/in_01_gsidsic.pdf. Acesso em: 20/abril/2019.

São inegáveis os benefícios da adoção da Nuvem Computacional para as organizações públicas; porém, há de se sopesar o nível dos riscos aceitáveis na migração da plataforma. A vantagem é que a decisão não precisa ser no sentido de "tudo ou nada", pois é possível (e recomendável) a migração paulatina da infraestrutura, dos sistemas e dos aplicativos. A migração seletiva faz com que seja aproveitado o máximo de benefícios do ambiente de Nuvem Computacional com o mínimo de riscos.
Os mais relevantes benefícios apontados por organizações nacionais e internacionais em relação à utilização do ambiente de Computação em Nuvem são:

- Aumento da produtividade da equipe de TI.
- Melhoria da experiência do cidadão.
- Acesso a recursos avançados e redução dos ciclos de inovação.
- Flexibilidade na disponibilização de serviços, conforme os picos de demanda.
- Benefício para as organizações públicas de pequeno porte.
- Redução do tempo para a implementação.

Os autores buscam, na literatura existente, nos modelos de outros países e nas suas vastas experiências pessoais, a desmistificação da adoção de serviços em Nuvem Computacional nas organizações públicas, esclarecendo conceitos e padrões, apontando benefícios e riscos, assim como desenvolvendo uma proposta de processo de adoção do serviço de Computação em Nuvem para as organizações públicas brasileiras.