GRUPO I – CLASSE V – Plenário
TC 025.994/2014-0
Natureza: Relatório de Levantamento
Órgãos/Entidades: Empresa de Tecnologia e Informações da Previdência Social; Ministério das Comunicações (vinculador); Secretaria de Logística e Tecnologia da Informação - MP; Serviço Federal de Processamento de Dados
Responsável: Identidade preservada (art. 55, caput, da Lei n. 8.443/1992)
Interessado: Identidade preservada (art. 55, caput, da Lei n. 8.443/1992)
Advogado constituído nos autos: não há.

SUMÁRIO: RELATÓRIO DE LEVANTAMENTO DE AUDITORA. IDENTIFICAÇÃO DE RISCOS RELEVANTES EM CONTRATAÇÕES DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO, SOB O MODELO DE COMPUTAÇÃO EM NUVEM. ELABORAÇÃO DE TABELA DE RISCOS, CONTROLES POSSÍVEIS E CRITÉRIOS. ELABORAÇÃO DE MATRIZ DE PROCEDIMENTOS DE AUDITORA DE COMPUTAÇÃO EM NUVEM. CIÊNCIA A DIVERSOS INTERESSADOS. LEVANTAMENTO DE SIGILO. ARQUIVAMENTO.

RELATÓRIO

Adoto como relatório, com os ajustes de forma que entendo aplicáveis, instrução elaborada no âmbito da Secretaria de Fiscalização de Tecnologia da Informação, com a qual anuíram os dirigentes daquela unidade técnica especializada:

> ***"1. Introdução***
>
> *1.1 Deliberação que originou a fiscalização*
>
> *1. A fiscalização foi autorizada pelo Acórdão 1.579/2014-TCU-Plenário, no âmbito do TC 010.866/2014-0, que trata da proposta de fiscalização formulada por esta unidade, sendo que as razões que a motivaram encontram-se descritas a seguir.*
>
> *2. A evolução tecnológica dos últimos anos e o barateamento dos recursos computacionais permitiram a exploração de um novo modelo de acesso a recursos computacionais compartilhados e de alta disponibilidade e acessibilidade: a computação em nuvem.*
>
> *3. Os benefícios oferecidos por esse novo modelo permitem o foco nas funções essenciais da organização. Além dos benefícios esperados pela terceirização em geral, o modelo traz benefícios específicos como: maior disponibilidade, flexibilidade da oferta do serviço em função de variações na demanda, menor dependência de pessoal qualificado, possível redução de vários riscos de segurança, pagamento por uso efetivo de recursos e potencial redução de custos.*
>
> *4. Todavia, diante do modelo de contratação pública, bem como, dos requisitos de segurança da informação, faz-se necessário levantar os riscos advindos de contratações sob esse modelo.*

5. Devido ao rápido crescimento da adoção dessa tecnologia no mercado privado, espera-se que, em breve, o TCU seja demandado a se manifestar sobre contratações de serviços de computação em nuvem pela Administração Pública Federal (APF).

1.2 Objetivo, escopo e metodologia

6. O objetivo deste levantamento é identificar os riscos mais relevantes em contratações de serviços de Tecnologia da Informação (TI) sob o modelo de computação em nuvem, considerando os critérios da legislação brasileira, e elaborar modelo de matriz de procedimentos e de achados para futuras fiscalizações. Para tanto, a equipe de fiscalização buscou aprofundar o conhecimento do assunto, adentrar nas peculiaridades da legislação nacional e adaptar critérios de auditoria internacionais a requisitos específicos da APF.

7. Desse modo, espera-se que o trabalho seja referência para os auditores do TCU em futuras auditorias de contratações de serviços de computação em nuvem, bem como para os gestores públicos encarregados de avaliar e, se for o caso, contratar serviços de TI segundo esse modelo.

8. Considerando que o presente trabalho trata-se de fiscalização do tipo levantamento (conforme previsto no art. 238 do Regimento Interno do Tribunal de Contas da União), a referência utilizada foi o documento Padrões de Levantamento, o qual foi aprovado pela Portaria-Segecex 15/2011.

9. Inicialmente, a equipe de fiscalização estabeleceu o escopo e o não escopo do trabalho e elaborou a matriz de planejamento para o trabalho de levantamento, contendo as seguintes questões:

Q1. O que é computação em nuvem, suas características e aplicações?
Q2. Quais são os modelos de comercialização de computação em nuvem?
Q3. Qual o quadro normativo aplicável a contratações de serviços de computação em nuvem pela APF?
Q4. Qual o panorama atual da contratação de serviços de computação em nuvem pela APF?
Q5. Quais as principais vantagens, riscos e controles quando da contratação de serviços de computação em nuvem?

10. Assim, visando aprofundar o conhecimento sobre o tema, buscou-se primeiramente melhor compreensão dos conceitos de computação em nuvem, bem como identificar suas características, classificações e aplicações. A partir dessas informações, procurou-se definir e adotar um conceito para ser utilizado no contexto da fiscalização.

11. É importante destacar que o escopo do trabalho está restrito à contratação de serviços de computação em nuvem pública (vide definição nos parágrafos 33 e 34), não incluindo a contratação de solução de TI para implantação de nuvem privada (vide parágrafos 35 e 36) e nem a de serviços na nuvem (serviços providos por ambiente de computação em nuvem; vide parágrafo 50, item 2).

12. O passo seguinte foi levantar os modelos oferecidos pelo mercado, incluindo aspectos como acordos de níveis de serviço e formas de remuneração.

13. Considerando que a maior parte das referências encontradas pela equipe são voltadas para o mercado privado dos Estados Unidos, pesquisou-se informações a respeito do quadro normativo que seria aplicável às contratações de serviços de computação em nuvem pela APF.

14. Entretanto, destaca-se que não foi escopo do trabalho analisar normativos gerais de contratações de serviços de TI, como a IN SLTI/MP 4/2014, mas apenas normativos específicos ou aspectos específicos em normativos gerais que pudessem impactar a contração de serviços de computação em nuvem, como o Decreto 8.135/2013.

15. Com relação ao panorama atual da contratação de serviços de computação em nuvem pela APF, buscou-se identificar contratações representativas já realizadas, incluindo a comparação dos benefícios esperados com os benefícios alcançados. Entretanto, os poucos exemplos encontrados são recentes e não permitem ainda aferir benefícios efetivos.

16. Como produto principal, o trabalho procurou identificar os riscos inerentes à contratação de serviços de computação em nuvem e os respectivos controles que devem ser utilizados para tratá-los. Uma vez identificados os riscos e os controles associados, a equipe elaborou tabela elencando principais riscos e controles sobre o tema, bem como modelo de matriz de procedimentos e de achados para futuras fiscalizações.

*17. A metodologia utilizada para o levantamento de informações incluiu: pesquisas a referências disponíveis na **internet**; entrevistas e envios de questionário para representantes de alguns provedores privados, como Amazon, Microsoft, Vmware e HP; reuniões telefônicas com consultores do Gartner; interação (por meio de ofícios de requisição de informações e reuniões) com gestores de algumas organizações públicas (TCU, SLTI/MP, Infraero, Serpro, Dataprev, Finep, Ministério das Comunicações, Ministério da Ciência, Tecnologia e Inovação e Petrobrás); e pesquisas no Diário Oficial da União.*

18. A interação com gestores públicos possibilitou obter conhecimento a respeito de exemplos de contratação de serviços de computação em nuvem identificados na APF, dos planos e ações dos provedores públicos (Serpro e Dataprev) e das ações estruturantes e políticas públicas de governo.

1.3 Limitações

19. Não houve restrição de acesso, omissão de informações por parte dos gestores ou outro fator que limitasse o escopo do trabalho e a profundidade da análise planejada. Entretanto, devido ao caráter recente da tecnologia, foram encontrados poucos casos concretos de uso de computação em nuvem pela APF, o que impossibilitou aferir se os benefícios esperados com o uso da tecnologia converteram-se em benefícios reais para o setor público.

20. Durante a execução do trabalho, foi possível realizar reuniões com apenas quatro grandes provedores privados. Outros dois não responderam o contato inicial feito pela equipe de auditoria. Além disso, foi enviado um questionário para os provedores com os quais a equipe se reuniu e somente um deles enviou suas respostas. Desse modo, considera-se que a análise do mercado brasileiro ficou prejudicada.

2. Características principais de computação em nuvem

21. Este capítulo apresenta algumas definições a partir de publicações técnicas e estudos acadêmicos sobre computação em nuvem, além de abordar os potenciais benefícios da computação em nuvem.

2.1 Conceituação de computação em nuvem

*22. Das muitas definições encontradas para computação em nuvem, a definição do **National Institute of Standards and Technology** (NIST), agência governamental não-regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos, tem sido amplamente utilizada:*

> *Computação em nuvem é um modelo que permite acesso ubíquo, conveniente e sob demanda, através da rede, a um conjunto compartilhado de recursos computacionais configuráveis (por exemplo: redes, servidores, armazenamento, aplicações e serviços), que podem ser rapidamente provisionados e disponibilizados com o mínimo de esforço de gerenciamento ou de interação com o provedor de serviços. (Tradução livre)*

*23. No entanto, esta não é uma única e completa definição do termo. Existe uma infinidade de definições, que por sua vez relatam entendimentos diversos. Uma rápida pesquisa no site de buscas do Google para o termo "**cloud computing**" retornou cerca de 176.000.000 resultados, o que já transmite a ideia de crescente importância do tema e sua abrangência.*

24. O Gartner define computação em nuvem como "um estilo de computação no qual capacidades de TI escaláveis e elásticas são entregues como um serviço a clientes externos, utilizando tecnologias de Internet".

*25. Já o CIO.com, site subsidiário do **International Data Group** (IDG) que concentra publicações sobre tendências de tecnologia da informação, apresenta uma definição concisa que foi estabelecida*

*pela empresa de consultoria Accenture: "o provisionamento dinâmico de capacidades de TI (**hardware**, **software** ou serviços) por terceiros, através de uma rede".*

*26. Desta maneira, o CIO.com, em seu artigo intitulado "**Cloud Computing Definitions and Solutions**", defende que computação em nuvem é:*

> *Um modelo, não uma tecnologia. Neste modelo de computação, todos os servidores, redes, aplicações e outros elementos relacionados a data centers são disponibilizados para a TI e para os usuários finais através da Internet, de maneira que a TI compra somente o tipo e a quantidade de serviços computacionais que realmente são necessários. O modelo em nuvem difere das terceirizações tradicionais à medida em que os clientes não entregam seus próprios recursos de TI para gerência de terceiros. Ao invés disso, eles se conectam à "nuvem" para ter serviços de infraestrutura, ou serviços de software, lidando com a "nuvem" da mesma maneira que eles fariam com um data center interno ou um computador que tivesse as mesmas funções. (tradução livre)*

*27. O **International Data Corporation** (IDC), provedor de consultoria e serviços estratégicos de marketing para os mercados de Tecnologia da Informação e Telecomunicações, estabelece distinção entre dois conceitos: "Computação em Nuvem (**Cloud Computing**)" e "Serviços na Nuvem (**Cloud Services**)". De acordo com o blog IDC Exchange, "Serviços na Nuvem" são quaisquer tipos de serviços, produtos e soluções, voltadas a negócios ou ao consumidor final, utilizados em tempo real através da **Internet**. "Computação em nuvem", por sua vez, é um modelo emergente de desenvolvimento, implantação e entrega de TI, permitindo a entrega em tempo real de produtos, serviços e soluções através da Internet. Ou seja, a computação em nuvem é o ambiente de TI que dá suporte ao desenvolvimento, consumo e entrega dos serviços na nuvem.*

*28. Assim, computação em nuvem é um termo que remete a grupos de recursos computacionais acessíveis por rede, flexíveis, provisionados por demanda e de maneira autônoma pelo demandante. Os serviços disponibilizados através da computação em nuvem são flexíveis porque os recursos e processamento disponíveis podem ser ajustados dinamicamente de acordo com as necessidades, sem a obrigatoriedade de envolvimento da equipe de TI do cliente. Desta maneira, cria-se um modelo de computação independente de **hardware**, capaz de absorver crescimentos futuros ou ajustar-se a novas demandas, ainda que inferiores às inicialmente projetadas.*

*29. A definição do **National Institute of Standards and Technology** (NIST) pode ser considerada atualmente como a mais generalista e completa. As demais definições podem ser vistas como especializações, em maior ou menor grau, da determinada pelo NIST, e todas elas somente podem ser completamente compreendidas a partir do estabelecimento de um conjunto mínimo de características, ou atributos, de computação em nuvem, listados a seguir.*

2.2 Características essenciais de computação em nuvem

30. O NIST também descreve, de maneira abrangente, cinco características essenciais de computação em nuvem (tradução livre):

1) ***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.*
2) ***Acesso amplo pela rede** ("**broad network access**"): os recursos da nuvem estão disponíveis para acesso pela rede por diferentes dispositivos (tais como: estações de trabalho, tablets e smartphones) através de mecanismos padrões.*
3) ***Compartilhamento através 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.

4) ***Rápida elasticidade**: 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.*

5) ***Serviços medidos por utilização** ("**measured service**"): os serviços de computação em nuvem automaticamente controlam e otimizam a utilização de recursos, através 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.*

2.3 Modelos de computação em nuvem (ou tipos de computação em nuvem)

*31. Existem vários modelos de computação em nuvem, que servem como dimensões combináveis entre si para balizar o projeto, implantação, e aquisição de nuvens. Os modelos mais difundidos atualmente são os definidos pelo NIST, descritos pelo **Cloud Security Alliance** (CSA):*

1) ***Modelo baseado na forma de implantação**: a nuvem pode ser pública, privada, híbrida, ou comunitária;*

2) ***Modelo baseado na arquitetura dos serviços disponibilizados pela nuvem**: a arquitetura pode ser Infraestrutura como Serviço (**Infrastructure as a Service -** IaaS), Plataforma como Serviço (**Platform as a Service -** PaaS), **Software** como Serviço (**Software as a Service** - SaaS).*

2.3.1 Modelo de nuvem de acordo com a forma de implantação

32. A nuvem pode ser implantada e utilizada de maneiras diferentes, dependendo das necessidades de uso e de negócio. Considerando as formas de implantação, existem quatro categorias distintas, de acordo com o NIST e CSA: Nuvem Pública, Nuvem Privada, Nuvem Comunitária e Nuvem Híbrida.

*33. **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, gerenciamento e operação podem ser de uma empresa, uma instituição acadêmica, uma organização do governo, ou de uma combinação desses.*

*34. Os serviços mais conhecidos e populares de nuvem estão em nuvens públicas, como o Hotmail, Dropbox, Google Apps e Icloud. Serviços institucionalmente contratados na nuvem pública, normalmente, mas não obrigatoriamente, são acessados pelos usuários corporativos através da **Internet**. Desta maneira, estes serviços são terceirizados para os provedores de nuvem, e, portanto, a infraestrutura computacional associada aos mesmos também é terceirizada. A nuvem pública oferece economia de escala, mas pode apresentar riscos de segurança que necessitam ser avaliados.*

*35. **Nuvem Privada**: A infraestrutura de nuvem privada está disponível para uso exclusivo por uma única organização. Sua utilização, gerenciamento e operação podem ser feitos pela própria organização, terceiros, ou por uma combinação dos dois, e pode estar localizada em suas dependências ou fora delas. No entanto, o cliente terá controle sobre sua localização geográfica, o que a faz tornar atrativa para dados ou sistemas com restrições de acesso ou que são de missão crítica.*

36. A nuvem privada, portanto, tem sua elasticidade reduzida. A economia de custos associada também é menor que a de uma nuvem pública, mas pode mitigar alguns riscos de segurança.

*37. **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, gerenciamento e 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 destas organizações, ou fora delas.*

*38. **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.*

39. É possível utilizar esta abordagem para valer-se dos benefícios dos modelos público e privado, e ao mesmo tempo minimizar os riscos e custos advindos de cada modelo, ou quando existem necessidades distintas associadas a determinados tipos de usuários ou de dados.

40. Os conceitos de nuvem pública, privada, comunitária e híbrida podem ter variações em outros modelos de implantação. Contudo, os tipos são frequentemente apresentados em escalas que variam desde nuvem privada em um extremo à nuvem pública no outro.

41. Dentro destas variações, vale a pena, ainda, abordar o conceito de nuvem privada virtual. Segundo o Gartner, quando um provedor de serviços utiliza recursos de nuvem pública para criar e fornecer nuvens privadas, o resultado é uma nuvem privada virtual, ou seja, uma nuvem pública sem compartilhamento de recursos, onde os recursos são acessados por uma conexão de rede privada. Os provedores de nuvem pública já estão explorando maneiras de oferecer serviços de nuvem privada virtual.

42. No entanto, há muitas dúvidas em torno da delimitação entre um termo e outro, e sua divisão não tem sido consensual nem absoluta. O CSA define algumas características que auxiliam a diferenciar os tipos de nuvem, resumidos na tabela abaixo:

*Tabela 1 - Comparativo de características de nuvem pública, privada, privada virtual e híbrida, baseado no quadro "**Cloud Computing Models**" do CSA*

Tipo de Nuvem	***Gerenciada por***	***Propriedade da Infraestrutura***	***Localização da Infraestrutura***	***Forma de acesso e consumo***
Pública	*Terceiros*	*Terceiros*	*Fora das dependências*	*Compartilhado*
Virtual privada	*Organização ou terceiros*	*Organização ou terceiros*	*Fora das dependências*	*Dedicado*
Privada	*Organização ou terceiros*	*Organização ou terceiros*	*Dentro das dependências*	*Dedicado*
Híbrida	*Tanto organização como terceiros*	*Tanto organização como terceiros*	*Tanto dentro como fora das dependências*	*Tanto dedicado como compartilhado*

2.3.2 Modelo de nuvem de acordo com a arquitetura dos serviços disponibilizados pela nuvem

43. Esta classificação baseia-se no conceito de arquitetura em camadas hierárquicas, onde os serviços da camada superior são providos pela camada inferior subsequente.

44. O NIST distingue entre três principais categorias, a saber:

*45. **Software como um Serviço (Software as a Service** - SaaS): São as aplicações do fornecedor executadas em uma infraestrutura de nuvem (conforme as cinco características de computação em nuvem), disponíveis 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. Para este último, há a possível exceção de restritas configurações de aplicação, específicas a usuário.*

*46. **Plataforma como um Serviço (Platform as a Service** - PaaS): O recurso fornecido ao consumidor são linguagens de programação, bibliotecas, serviços e ferramentas de suporte ao desenvolvimento de aplicações, para que o consumidor possa implantar, na infraestrutura da nuvem, aplicativos criados ou adquiridos por ele. O consumidor não gerencia nem controla a infraestrutura subjacente da nuvem (rede, servidores, sistema operacional, banco de dados ou armazenamento), mas tem controle sobre as aplicações implantadas e possivelmente sobre as configurações do ambiente que hospeda as aplicações.*

*47. **Infraestrutura como um Serviço (Infrastructure as a Service** - IaaS): É o provisionamento de processamento, armazenamento, comunicação de rede e outros recursos de computação fundamentais pelo fornecedor, nos quais o consumidor pode instalar e executar **softwares** em geral, incluindo sistemas operacionais e aplicativos. O consumidor não gerencia nem controla a infraestrutura subjacente da nuvem, mas tem controle sobre os sistemas operacionais, espaço de armazenamento, e aplicativos instalados, e possivelmente possui controle limitado sobre alguns componentes de rede (como **firewalls**).*

48. A divisão de responsabilidades pela administração de TI entre fornecedor e cliente varia entre os três tipos, IaaS, PaaS e SaaS:

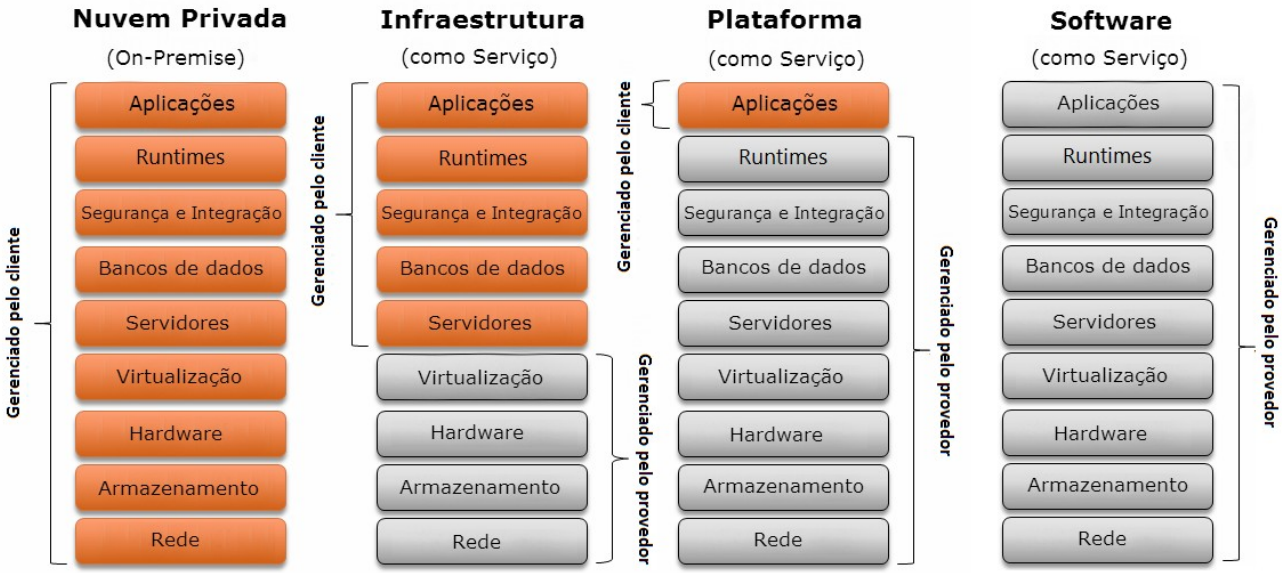

Figura 1 - Divisão de responsabilidades entre cliente e fornecedor de nuvem (adaptada de Matt Hester´s WebLog)

49. A tabela abaixo traz uma relação não-exaustiva de exemplos de segmentos e de provedores de computação em nuvem pública. Demonstra-se, assim, que existem soluções em nuvem similares às tradicionais, com capacidade e interfaces familiares para os usuários da TI convencional.

Tabela 2 - Exemplos de segmentos e provedores de nuvem pública. Fonte: TheMetisFiles

Nuvem pública	*Segmentos*	*Exemplos*
***Software** como Serviço (SaaS)*	*Comunicação e colaboração*	*Cisco Webex, Microsoft Lync, IBM Lotusphere*
	Produtividade de escritório	*Google Apps, Microsoft Office 365*
	Gestão de relacionamento com o cliente (CRM)	*Salesforce.com, PerfectView CRM Online, AccountView CRM Online*
	Sistema integrado de gestão empresarial (ERP)	*NetSuite, Exact Online, Twinfield, SAP Business ByDesing, Infor*
	***Supply chain management** (SCM)*	*Descartes, Ariba, Ketera, JDA Software*
Plataforma como Serviço (PaaS)	*Desenvolvimento de aplicações específicas*	*Salesforce Force.com, SaaSPlaza, SAP Business ByDesign*

	Desenvolvimento de aplicações genéricas	*Google App Engine, Microsoft Azure*
Infraestrutura como Serviço (IaaS)	*Computação*	*Amazon EC2, JitScale, Rackspace, Uniserver, Microsoft Azure, Google Compute Engine*
	*Armazenamento e **backup***	*EMC, Symantec, RainStor, Amazon S3*

2.4 Delimitação dos conceitos

50. Sabendo-se que os modelos permeiam-se (por exemplo: pode-se ter uma nuvem privada que provê IaaS, ou uma nuvem pública provendo SaaS), é necessário, ainda, diferenciar os conceitos de nuvem, serviços na nuvem, computação em nuvem e serviços de computação em nuvem:

*1) **Nuvem** (cloud): De acordo com o site whatiscloud.com, uma nuvem:*

> *refere-se a um ambiente distinto de TI projetado com o propósito de provisionar recursos de TI escaláveis e mensuráveis, com fronteiras delimitadas e acessados remotamente. O termo originou-se como uma metáfora à Internet, a qual é, em sua essência, uma rede de redes provendo acesso remoto a um conjunto de recursos de TI descentralizados. (tradução livre)*

*2) **Serviços na nuvem** (**cloud services**): A partir da definição do IDC, deriva-se que são quaisquer serviços e soluções entregues e consumidos em tempo real, localizados na nuvem e acessados remotamente, comumente pela **Internet**, tais como serviços de compras, bancos, colaboração, etc. Os consumidores não estão explicitamente comprando "computação em nuvem", mas "serviços na nuvem" providos por ambientes de computação em nuvem;*

*3) **Computação em nuvem** (**cloud computing**): De acordo com o IDC, é "o ambiente de TI – envolvendo todos os elementos da "pilha" de TI e produtos de rede (e serviços de suporte) – que permite o desenvolvimento, entrega e consumo de serviços na nuvem", de maneira escalável e elástica. Envolve um **framework** e vocabulário voltados ao domínio de TI;*

*4) **Serviços de computação em nuvem** (**cloud computing services**): são serviços que abrangem o provimento de computação em nuvem, com todas suas características.*

51. Diante dessa diferenciação, é importante destacar que, para os fins deste trabalho, o escopo está limitado somente à contratação de serviços de computação em nuvem (item 4 acima), conforme o conceito e as características do NIST. Assim, não fazem parte do escopo a contratação de solução de TI para implantação de nuvem privada e nem a contratação de serviços na nuvem (item 2 acima).

52. Além disso, quaisquer análises sobre contratações de serviços de computação em nuvem variam de acordo com as nuances dos dois modelos: modelo baseado na forma de implantação e modelo baseado na arquitetura dos serviços disponibilizados pela nuvem (vide definição no parágrafo 31). Por exemplo, nuvens privadas apresentam riscos reduzidos relativos à segurança da informação, porém maiores no que concerne à escalabilidade e elasticidade, quando comparadas a nuvens públicas.

53. Assim, como é possível fornecer serviços de computação em nuvem associados a qualquer modelo de nuvem, faz-se necessário estabelecer uma linha divisória conceitual, e, dentre os vários degraus para prestação de serviços de computação em nuvem, não há dúvidas de que os serviços associados a uma nuvem pública representam o maior grau de terceirização.

54. Deste modo, no escopo deste trabalho, serão adotados os serviços de computação em nuvem pública como a base para o levantamento de riscos e controles, observadas as características elencadas pelo NIST.

55. Por fim, destaca-se que existem ainda outros conceitos relacionados à computação em nuvem, frequentemente citados em sítios comerciais e na literatura, mas que não dizem respeito diretamente à sua definição e características, como os conceitos de virtualização, automação, orquestração e ***collocation****. Maiores esclarecimentos sobre tais conceitos encontram-se no anexo III deste trabalho.*

2.5 Principais vantagens da adoção de computação em nuvem

56. Diversas fontes de informação sobre computação em nuvem listam suas potenciais vantagens, havendo grande interseção entre elas. No entanto, a importância relativa de cada vantagem é sensível às particularidades do sistema sendo utilizado em nuvem (sobretudo em função de sua classificação entre IaaS, PaaS ou SaaS) e das prioridades da entidade contratante desses serviços.

57. Descreve-se a seguir as principais vantagens da adoção de computação em nuvem, decorrentes da definição adotada neste trabalho (seção 2.1).

58. As vantagens de nuvem decorrem essencialmente de benefícios de escala: ao consolidar centros de processamento de dados (CPDs) isolados em um pool de recursos computacionais compartilhados em nuvem, reúne-se um conjunto maior de recursos o que permite reduzir seus custos unitários, melhorar seu aproveitamento, balanceando as demandas por serviços de diversos clientes, o que otimiza o nível de uso dos recursos e divide os custos fixos em uma maior base de usuários.

59. Segundo estudo da IDC, as principais vantagens do uso de computação em nuvem são:

1) ***Redução de custos de infraestrutura e serviços de TI****. O benefício mais significativo vem de hospedar aplicações em infraestrutura em nuvem devido à redução de custos de capital (****capital expenditure*** *- Capex) e custos operacionais (****operacional expenditure*** *- Opex).*

2) ***Otimização da produtividade da equipe de TI****. A mudança para o uso de IaaS, ao acelerar o desenvolvimento e a implantação de aplicações, bem como automatizar o seu gerenciamento, torna a equipe de TI mais produtiva e capaz de melhorar o suporte de operações de missão crítica.*

3) ***Melhoria da produtividade do usuário final****. Os usuários finais beneficiaram-se de menor indisponibilidade do serviço e recuperação mais rápida, reduzindo o tempo de inatividade em 72% e economizando expressivos recursos de cada aplicativo por ano.*

4) ***Aumento de benefícios do negócio****. Muitas das empresas estão empregando soluções em nuvem para possibilitar novos modelos de negócios e suportar aplicações de geração de receita, atingindo um maior número de usuários/clientes.*

*60. Outras vantagens também são apontadas pela Isaca na publicação "****Controls and Assurance in the Cloud: Using*** *COBIT 5":*

1) ***Melhorar capacidade de resposta****. Computação em nuvem fornece serviços flexíveis e escaláveis que podem ser implementados rapidamente para fornecer às organizações a capacidade de responder a mudanças de requisitos e a períodos de picos.*

2) ***Ciclo mais rápido de inovação****. No ambiente de nuvem, a inovação é tratada muito mais rápido do que dentro da empresa. O gerenciamento de patches e atualizações para novas versões tornam-se mais flexíveis.*

3) ***Redução do tempo para implementação****. Computação em nuvem oferece poder de processamento e capacidade de armazenamento de dados conforme a necessidade, quase em tempo real.*

4) ***Resiliência****. Computação em nuvem pode fornecer um ambiente altamente resiliente e reduzir o potencial de falha e o risco de* ***downtime****.*

*61. Segundo análise da ENISA (****European Network and Information Security Agency****), os ganhos de escala refletem-se também na área de segurança:*

> ***Segurança e os benefícios de escala**: de forma simples, todos os tipos de medidas de segurança são mais baratos quando implementados em larga escala. Portanto, um mesmo valor de investimento em segurança permite adquirir uma melhor proteção. Isso inclui todos os tipos de medidas defensivas, tais como filtragem, gerenciamento de atualizações, o **hardening** das instâncias de máquinas virtuais e **hypervisors** etc. Outros benefícios de escala 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. (tradução livre)*

62. Como a segurança é um dos elementos diferenciadores de mercado, os principais fornecedores de nuvem competem com propostas abrangentes e robustas de segurança, possivelmente superando o padrão de segurança em data centers próprios dos clientes, que possuem menos recursos disponíveis de segurança a serem amortizados sobre uma menor base de usuários. Dentre essas vantagens de segurança na nuvem, destacam-se:

1) *maior resistência a ataques contra a disponibilidade de serviços (**distributed denial of service** - DDoS) devido à maior capacidade do provedor de nuvem para realocar dinamicamente os recursos de filtragem, **traffic shaping**, autenticação, criptografia etc.*

2) *vantagens para auditoria e perícia: o uso de virtualização em computação em nuvem, permite fornecer imagens dedicadas para a perícia forense de máquinas virtuais, acessíveis sem precisar desconectar a infraestrutura operacional, levando a um menor tempo de inatividade durante o período de análise. O uso de nuvem também permite fornecer mais espaço de armazenamento de baixo custo para logs, permitindo conservar registros de atividade mais abrangentes e por mais tempo.*

3) *atualizações e parametrização padrão de segurança mais efetivas e rápidas: a padronização das imagens de máquinas virtuais e dos módulos de **software** usados pelos clientes possibilita ajustes finos (**hardening**) de parâmetros de segurança, tornando-os mais robustos e otimizados, e atualizações contínuas.*

63. Adicionalmente, a computação em nuvem também traz vantagens em sustentabilidade ambiental. A nuvem é, em geral, mais eficiente do que a infraestrutura própria de TI, pois quando a demanda por recursos computacionais de determinado cliente diminui, esses são realocados para atender às necessidades de outros clientes. Assim, o uso de recursos de infraestrutura física, como energia elétrica e ar condicionado, que seriam utilizados mesmo em situações de ociosidade da infraestrutura de TI em data centers próprios, seria otimizado em ambiente de nuvem.

2.5.1 Vantagens específicas para governo

64. Adicionalmente às vantagens gerais acima elencadas, identificam-se as seguintes vantagens mais específicas para atividades estatais:

1) *Maior agilidade da administração pública na entrega de serviços e em sua atualização tecnológica, pois os processos formais de contratação pública podem dificultar a manutenção de uma infraestrutura de TI própria atualizada e que responda rapidamente às demandas de seus usuários.*

2) *Suporte a iniciativas de Big Data e Dados Abertos, facilitando a abertura de informações governamentais que hoje encontram-se em sistemas que controlam as operações cotidianas do Estado e portanto são fechados com acesso limitado aos seus operadores. O uso de nuvem pública permitiria ampliar o acesso a esses dados a um custo menor, sem comprometer a segurança, a disponibilidade e o desempenho operacional dos sistemas originais. Uma vez os dados governamentais estando facilmente acessíveis, torna-se possível maior participação da sociedade na criação de novos serviços baseados nesses dados.*

3) *Atendimento a picos de demanda sazonal de serviços públicos pela Internet sem necessidade de alocar grande quantidade de recursos fixos. Várias atividades estatais acarretam picos sazonais de demanda de serviços próximos a datas limite como: entregas de declarações de imposto de renda, inscrições e resultados do Enem,*

resultados eleitorais e listagem de gestores públicos inelegíveis, períodos de recadastramento do INSS, listagem dos percentuais do fundo de participação dos municípios, etc.

4) *A contratação de serviços em nuvem de IaaS ou PaaS pode levar a uma redução de oportunidades de desvios e irregularidades, quando comparada às múltiplas contratações de máquinas, licenças de **software**, manutenção e suporte necessárias para a operação de CPD próprio. As ofertas de IaaS e PaaS identificadas neste levantamento são todas por contrato de adesão, utilizando métricas de precificação com custos unitários divulgados publicamente e iguais para todos os clientes, o que facilita a pesquisa de preços.*

5) *Agilidade e economia na entrega de serviços para instituições públicas com unidades descentralizadas, que podem ter serviços disponibilizados por meio de acesso à internet, mais barato que as interconexões via redes privadas atualmente utilizadas.*

2.6 Exemplos de uso da computação em nuvem

65. Ao longo do presente trabalho foram identificados diversos usos para computação em nuvem. A seguir serão descritos alguns comumente encontrados ou que tenham um grande número de usuários.

2.6.1 Terceirização de infraestrutura de TI

66. A terceirização de parte da infraestrutura de TI, ou contratação de infraestrutura como serviço (IaaS), tem seu uso bastante difundido. É um caminho natural para muitas organizações, principalmente as pequenas, utilizar infraestrutura pronta com pagamento por uso, ao invés de adquirir, implantar, gerenciar e manter sua própria infraestrutura de TI.

2.6.2 Suíte de escritório

67. Aplicações de software de escritório, como editor de texto, planilha e apresentação, já dispõem de versões em nuvem, como, por exemplo, as soluções corporativas do Google Docs e Microsoft Office 365. São soluções cujo custo pode ser similar ou mesmo inferior ao modelo tradicional, além de oferecerem benefícios adicionais, como: menor utilização de recursos de TI próprios (espaço de armazenamento, por exemplo), maior disponibilidade (por meio de acesso remoto via Internet, utilizando computadores e dispositivos portáteis) e redução de custos operacionais (como instalação e atualização de software, por exemplo).

2.6.3 Armazenamento

*68. Aplicações de armazenamento (**storage**) na nuvem permitem que os arquivos dos clientes estejam disponíveis em qualquer lugar (por meio de acesso remoto via Internet) e por meio de dispositivos diversos (computador, celular e **tablet**), facilitando também o compartilhamento de informações e o trabalho em equipe. Citam-se, como exemplos, as soluções corporativas do Google Drive, Microsoft OneDrive e DropBox.*

2.6.4 Correio eletrônico

69. O correio eletrônico na nuvem é um exemplo de SaaS em que funcionalidades típicas de uma solução de correio são replicadas em uma arquitetura de nuvem. O correio eletrônico tradicional requer um aplicativo instalado localmente em uma máquina e que se comunica com um servidor dedicado em um centro de processamento de dados da empresa, órgão ou provedor de internet. Com a nuvem, o simples uso de um navegador de internet permite a conexão a um servidor de e-mail. Assim, não se requer mais servidores dedicados em infraestrutura própria e até mesmo o armazenamento é mantido de forma distribuída na nuvem.

70. Exemplos de tais aplicativos encontram-se nos webmails gratuitos, como o Yahoo Mail ou Gmail, que também possuem versões corporativas em que o servidor de e-mails é controlado pela empresa, ainda que funcione na nuvem. De forma similar, o Exchange, servidor de correio eletrônico da

Microsoft que faz parte da solução do Office 365, também é um exemplo de correio eletrônico que pode ser tanto provido por nuvem, em servidores da Microsoft, como localmente em servidores próprios da organização.

*71. Como exemplo de aplicativo governamental de correio em nuvem, cita-se a suíte de comunicação Expresso do Serpro, utilizada por mais de 60 mil pessoas no final de 2012. Desde 2007, o Expresso está em operação no Serpro e reúne funcionalidades de e-mail, agenda, catálogo de endereços, **workflow** e mensagens instantâneas em um único ambiente. A ferramenta é construída em **software** livre (Tine 2.0), o que mantém independência frente a fornecedores comerciais, mas requer constante esforço de desenvolvimento para atualização e novas funcionalidades.*

*2.6.5 **Backup** de arquivos*

*72. Classicamente, o processo de **backup** é demorado e lento, pois necessita copiar arquivos para outra mídia, como outro disco ou fita, e transportá-la para instalações independentes onde possa ser garantida sua integridade em caso de desastre nas instalações principais. O **backup** para a nuvem é uma solução mais simples, ressalvando-se que depende de banda de **internet** suficiente para tal, na qual **backups** podem ser programados e executados automaticamente. Os dados são armazenados já em um local remoto, seguro, disponível, com capacidade de expansão de espaço automática, intrínseca à escalabilidade característica da computação em nuvem.*

2.6.6 Big Data

*73. O termo Big Data refere-se a análises de dados (**analytics**) que só são possíveis em larga escala, com objetivo de extrair novas ideias e melhorar a compreensão das informações.*

*74. Big Data requer uma infraestrutura que permita realizar armazenamento e recuperação de dados de diversos formatos em grande escala, com a finalidade de transformar um grande volume de dados em informações úteis para a organização. Com necessidades crescentes e variáveis de capacidade computacional, um projeto de **analytics** pode ter picos de demanda altos. A variabilidade de necessidade de processamento para **analytics** é particularmente bem atendida pela computação em nuvem, além de que grande parte dos dados utilizados por aplicações de Big Data estão armazenados na nuvem.*

3. Modelos de comercialização de serviços de computação em nuvem

75. Esse capítulo apresenta o panorama atual do mercado brasileiro e identifica modelos de comercialização de serviços de computação em nuvem.

76. Assim, para cada um dos três modelos de implementação (IaaS, PaaS e SaaS), são descritas as formas de precificação e outros parâmetros comuns. Ademais, foram abordados os acordos de níveis de serviço dentro dos contratos padrões preconizados pelos fornecedores.

3.1 Mercado brasileiro

*77. De acordo com artigo da IDGnow intitulado "**Cloud Corporation** e a TI baseada em cloud", um novo modelo de utilização de aplicativos em massa, com a difusão de dispositivos móveis, aliado à crise econômica e o conceito de computação em nuvem, permitiu o surgimento de um modelo de negócios para aquisição e consumo de recursos de TI. A computação em nuvem propõe a troca dos investimentos de capital inicial (Capex) pelo gasto por consumo (Opex), e a receita passa a ser distribuída pelos anos em que o cliente usa o software.*

*78. Assim, o risco da aquisição e da manutenção se desloca do usuário para o fornecedor, que necessita manter constantemente o usuário satisfeito. Como o montante a ser pago aumenta de acordo com a utilização, o fornecedor passa a ter um empenho muito maior em fazer com que o usuário aproveite todo o potencial de funcionalidades do **software**.*

*79. Ainda de acordo com o referido artigo, a consequência para o mercado é uma transformação na cadeia de valor da indústria. Com **hardware** concentrado nos provedores, as vendas destas máquinas passam a ser em grande volume, direto aos provedores, dispensando os intermediários que vendiam*

pequenos volumes a empresas de médio a pequeno porte. As empresas usuárias deixam de comprar servidores físicos e passam a comprar servidores virtuais. Por outro lado, surgem oportunidades novas, para agregadores de valor, cada vez mais concentrados em serviços e consultorias.

80. A utilização de computação em nuvem tem transformado a própria indústria de TI e os setores de TI das instituições, redesenhando orçamentos e papéis do setor de TI e seus modelos de negócio. A nuvem permite uma interação direta entre os usuários e as ofertas de serviços de tecnologia, criando independência destes com relação ao setor de TI. Com isto, a função tradicional da TI perde sua importância e as áreas de TI são obrigadas a repensar suas funções, deslocando seu foco e capacitação para atuar cada vez mais como consultores de tecnologia, mais próximos das áreas de negócio.

*81. Um estudo da empresa de consultoria Frost & Sullivan, intitulado "**Analysis of the Brazilian Cloud Computing Market**", identificou um mercado de nuvem no Brasil equivalente a US$ 328,8 milhões em 2013, com crescimento projetado para alcançar o patamar de US$ 1,1 bilhão em 2017. Isso porque, salienta a consultoria, o mercado nacional está amadurecendo, com as empresas começando a perceber os benefícios com relação a custo e flexibilidade na adoção das soluções. A queda do ritmo de crescimento econômico também é um fator que acelera a contratação de serviços na nuvem.*

82. Para o mercado brasileiro de nuvem, aventou-se, durante reunião realizada pela equipe de auditoria com o Gartner em 27/11/2014, que o maior crescimento atualmente está em Infraestrutura como Serviço, e que corresponderia a mais de 40% ao ano. Analisando-se a nossa realidade de mercado para IaaS, pode-se estabelecer quatro grupos de fornecedores: os multinacionais; os regionais ou que trabalham em alguns nichos específicos; empresas de Telecom que fazem serviços de terceirização para nuvem, as quais devem aumentar sua participação e tem se estruturado para tal (apresentam vantagem por já possuir estrutura pronta em várias áreas, como faturamento, atendimento ao cliente, infraestrutura e conectividade, entre outros); e empresas locais.

*83. Deslocando-se para PaaS, levantou-se, na mesma reunião com o Gartner, que o mercado no Brasil é de tamanho estimado em 26 milhões de reais, ainda pequeno, mas com grandes expectativas de crescimento. Nele, os fornecedores dividem-se em plataforma para desenvolvedores de aplicações (como Google e **Salesforce**), infraestrutura para execução de aplicações (**application infrastructure**), solução de inteligência de negócio (**business intelligence**) e banco de dados.*

*84. Finalizando com SaaS, hoje seu mercado representa maior volume que IaaS, principalmente devido às aplicações de CRM, ERP e suíte de escritório (**office** suíte). Para o segmento de pequenas e médias empresas, observa-se que pequenas empresas estão posicionando-se como fornecedores de aplicações, como sistemas de contabilidade.*

85. Outra característica a ser considerada é que o mercado mundial, incluindo o brasileiro, segue as tendências e modelos adotados no mercado americano. Para IaaS, os maiores e mais conhecidos provedores de nuvem dos EUA estão voltados ao público em geral, com configurações iniciais totalmente automatizadas. Além destes, existem provedores emergentes que focam somente no mercado empresarial, assim como empresas menores que revendem infraestrutura provida pelos grandes provedores, podendo incluir alguns serviços adicionais empacotados.

*86. Também há uma pressão por parte do mercado consumidor de negócios para que os fornecedores de Telecom, fornecedores de **hosting** e integradores de sistema entreguem uma gama ainda maior de serviços de TI através da nuvem. Além disto, os clientes também esperam que os provedores de nuvem ofereçam serviços profissionais e de consultoria e suporte para auxiliá-los em uma transição à nuvem. Em resposta a isso, algumas empresas de Telecom, principalmente no mercado americano e de maneira incipiente no brasileiro, têm feito o papel de intermediário ou integrador de nuvem (em inglês, **cloud broker**), com o objetivo de orientar seus clientes a escolherem os serviços de nuvem mais adequados, um movimento que também permite às operadoras aumentarem sua própria oferta de serviços através de novas parcerias.*

87. Um integrador de nuvem é um intermediário entre o fornecedor e o cliente final, agindo durante as negociações e facilitando o processo, com papéis consultivos, conhecimento de mercado e relacionamentos estabelecidos com os provedores, o que vai além de uma simples revenda. Alguns clientes estabelecem relações comerciais diretas com provedores de nuvem e utilizam seus próprios

recursos de TI para endereçar certos aspectos técnicos, como suporte, provisionamento de novos serviços e gerenciamento de projetos. Mas a realidade para muitas empresas é a falta de recursos humanos ou de prazo para executar estas tarefas, e é justamente neste nicho de mercado onde entram os integradores de nuvem.

3.2 Modelos de comercialização

88. Dada a ampla variedade de soluções comercializadas como serviço, a nuvem apresenta um número crescente de provedores e de intermediários em seus diversos níveis. Assim, comparações entre provedores ou mesmo a tentativa de se nivelar parâmetros para avaliação de modelos de comercialização não são tarefas triviais.

89. Para ilustrar a complexidade de comparação e precificação, dada a diversidade e quantidade de fornecedores e variáveis precificáveis, já existem empresas especializadas em pesquisa e comparativo de preços no mercado americano. Um exemplo é o PlanForCloud, site no qual pode-se estimar custos entre diversos provedores de IaaS após o desenho da necessidade do cliente, e que fornece estimativas de gastos anuais e totais baseados nas ofertas mais baratas dentre os provedores cadastrados:

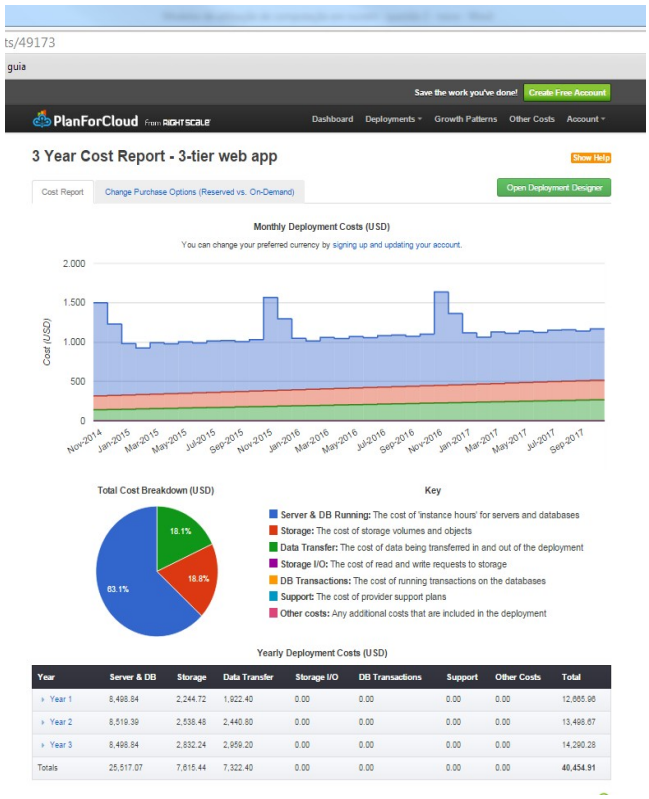

Figura 2 - PlanForcloud

90. As formas de comercialização, cobrança e prestação de serviços estão fundamentalmente relacionadas ao modelo de implantação de computação em nuvem, SaaS, PaaS, ou IaaS, possuindo critérios bastante distintos entre eles. Em geral, adota-se o pagamento por uso, apesar de constatar-se mecanismos de cobrança por usuário em ***softwares*** *vendidos como serviço. Muitos provedores vendem combinações complexas de utilização de vários recursos computacionais, e o cliente, com isso, necessita fazer um esforço com vistas a encaixar sua necessidade em alguma destas combinações, de maneira a obter o melhor custo-benefício. Estas combinações e formas de precificação são diferentes por diversas razões, dentre elas a natureza dinâmica da indústria, sem tempo hábil para amadurecimento e criação de padrões, e a alta competitividade do mercado.*

3.2.1 Comercialização de IaaS

*91. Em termos comparativos, sem dúvidas, o segmento onde identificam-se mais facilmente características em comum entre os provedores é o de Infraestrutura como Serviço. Thoran Rodrigues, em seu artigo intitulado "**Comparing cloud infrastructure as a service providers**", identificou 14 critérios comparativos comuns ao universo de 11 provedores. Grande parte destes critérios influem na composição de preço, e todos são variáveis a serem consideradas em comum na forma de comercialização dos fornecedores:*

1) ***Precificação**. São oferecidos planos de acordo com o uso (medidos geralmente por hora), planos mensais, ou descontos por "fidelização" (onde o cliente ganha um desconto em taxas de uso se assina previamente o serviço por um ano). O modelo de pagamento por uso permite um controle mais granular e está mais próximo do conceito de computação em nuvem. Já os planos mensais ou anuais aumentam o risco de pagamento por recursos não utilizados;*

2) ***Preço mensal médio**. A fim de encontrar-se um valor comum, o custo foi nivelado em dólares para um servidor na nuvem com 1 CPU e 2 GB de RAM (ou a melhor opção que mais se aproxime). Utilizou-se uma média entre data centers de provedores que possuem preços diferentes de acordo com a localização dos dados, e também uma média entre servidores Windows/Linux. Quando disponível, foi utilizada a precificação por hora, baseada em meses de 730 horas. Não estão incluídos os custos de transferência de dados;*

3) ***Service Level Agreement (SLA)**. SLA oferecido de disponibilidade, em pontos percentuais;*

4) ***Número de datacenters**. Quantidade de data centers oferecidos como escolha;*

5) ***Capacidade de ampliação (Scale Up)**. Se é possível ampliar instâncias de servidores em nuvem individualmente, adicionando mais memória, CPUs, ou armazenamento;*

6) ***Capacidade de crescimento (Scale Out)**. Se é possível implantar rapidamente novas instancias de servidores;*

7) ***Suporte**. Foi definida uma escala subjetiva de três níveis:*
   a) *Pequeno – empresas que oferecem somente suporte incluído como fóruns online; qualquer outro tipo de suporte é pago adicionalmente;*
   b) *Médio – empresas que oferecem um único tipo de suporte 24x7 incluído (ou telefônico, ou chat online), além dos fóruns;*
   c) *Extensivo – empresas com ofertas de suporte múltiplo incluídas no preço básico;*

8) ***Monitoramento**. Também definido em outra escala subjetiva em três níveis:*
   a) *Pequeno – empresas que não possuem soluções de monitoramento e alerta integradas, requerendo a implantação de ferramentas de terceiros ou que serviços extras sejam adquiridos;*
   b) *Médio – empresas com ferramentas muito simples de monitoramento integradas (poucos indicadores ou sem alertas);*
   c) *Extensivo – empresas com ferramentas de monitoramento completas integradas, oferecidas sem custo adicional;*

9) ***Interfaces (APIs)**. Se a companhia oferece interfaces para interação com os servidores;*

10) ***Testes gratuitos**. Se o provedor oferece período de testes gratuitos do serviço;*

11) ***Sistemas operacionais suportados**. Número de sistemas operacionais suportados, independentemente de versão, disponíveis como imagem pré-configurada;*

12) ***Número de tipos de instâncias**. Número disponível de diferentes configurações de servidores. Alguns provedores oferecem servidores totalmente customizáveis em termos de CPU, o que foi classificado como "configurável";*

13) ***Custo de saída de dados***. *O custo, em dólares, para cada GB de dados que saem do servidor. Empresas que oferecem conexões em Mbps sem ônus possuem custos listados como zero;*

14) ***Custo da entrada de dados***. *Mesmo que acima, mas para cada GB de dados que entram no servidor.*

92. Estes critérios, apesar de representarem somente uma fração do universo de variáveis que permeiam um contrato de serviços de computação em nuvem, estabelecem parâmetros mínimos que podem ser utilizados para efeitos comparativos, ou no mínimo, observados dentro de uma contratação. No caso do estudo citado, estabeleceu-se um comparativo entre os provedores. O primeiro ponto levantado foi a grande variação de preços entre os fornecedores, entre US$ 40,00 a US$ 135,00 por mês, valores estes de 2012 não atualizados, mas que servem para demonstrar a heterogeneidade do mercado. Além disto, alguns provedores oferecem SLA de 100%, não sendo possível saber se a médio e longo prazo este valor poderá ser mantido. Alguns também não fornecem a possibilidade de ampliação para um servidor já criado, ponto que merece atenção. Mais da metade cobra ou necessita de solução de terceiros para fazer monitoramento. Por fim, mais de 80% das empresas cobram pela transferência de dados (saída), ou seja, a utilização de rede influi nos valores cobrados.

3.2.2 Comercialização de PaaS

*93. A diferença entre os custos de serviços na nuvem entre IaaS e PaaS é que o IaaS possui critérios mais objetivos para composição de preços. Assim, uma fórmula básica para o custo de infraestrutura como serviço poderia considerar "horas de computação + horas de armazenamento+ custos de software". Já a estimativa de custos para Plataforma como Serviço é mais difícil, e neste caso, uma proposta de fórmula de custo poderia considerar, simplificadamente, algo como "horas de armazenamento + número de chamadas API * preço por chamada API + duração de consultas". O problema é que o fornecimento de Plataforma como Serviço possui muitas variáveis de custo. Além da dimensão de tempo de uso, é preciso considerar as chamadas de API, storage, etc.*

*94. As maneiras mais óbvias para fazer comparações entre provedores de PaaS, tais como linguagens de programação suportadas e bancos de dados incluídos não são tão importantes se o usuário utiliza padrões de mercado. Já avaliar os provedores de PaaS com base no suporte que estes podem dar ao ciclo de vida de desenvolvimento da aplicação, em procedimentos de desenvolvimento e grau de controle sobre a infraestrutura que sustenta a plataforma, pode ser mais útil. Por exemplo, se a equipe de desenvolvimento utiliza procedimentos e ferramentas especificas para realizar versionamento, testes e implantação em produção (**deploy**), pode-se comparar os serviços fornecidos dentre aqueles que integram com estas ferramentas. Fatores como opções de gerenciamento de ciclo de vida da aplicação (**Application Lifecycle Management**), APIs (**Application Programming Interface**) oferecidas, gerenciamento de logs e feedback, além dos acima propostos, devem ser considerados.*

3.2.3 Comercialização de SaaS

*95. O **Software** como Serviço utiliza um modelo de entrega de um-para-muitos, no qual um único provedor fornece serviços de **software** para múltiplos usuários. Neste modelo, a cobrança pelos serviços é feita baseada nos tipos e quantidades de serviços utilizados, algo semelhante ao consumo de serviços de água ou energia elétrica.*

96. Uma limitação chave ao modelo do SaaS é que este está focado em prover aplicações que possuam o potencial de alcançar um amplo mercado. Para serem rentáveis, as aplicações disponibilizadas como serviço precisam atrair uma grande base de clientes, e portanto são confeccionadas de uma forma padrão e igual para um grande número de usuários, atendendo às suas necessidades comuns. Desta forma, aplicativos de missão crítica ou que necessitam customização de acordo com as regras de negócio provavelmente não são candidatos para migração ao SaaS.

97. Os modelos de precificação de SaaS normalmente baseiam-se na quantidade de usuários, ou em volume de recursos consumidos, ou ainda em uma combinação dos dois. Normalmente a estrutura de preços é linear, e neste caso não há economia de escala.

*98. O pagamento por usuário é a estratégia de precificação mais comum. Neste modelo, um custo separado é associado para cada usuário de uma aplicação na nuvem, o que é similar ao pagamento por cada cópia de **software** instalada em uma estação de trabalho. A vantagem sobre a precificação de **software** tradicional é que no caso do **software** como serviço, o aplicativo está disponível para acesso remoto a partir de qualquer dispositivo, e não implica em cobranças separadas para **tablets**, notebooks, celulares e outros. O faturamento ocorre baseado em um período (normalmente, mensal) para o número de usuários registrados.*

99. Uma variação desse modelo é o pagamento por múltiplos usuários, em que um custo separado é calculado para uma quantidade específica de usuários. Por exemplo, uma aplicação SaaS pode ser faturada por faixas de usuários, sendo de 2 a 99 como uma primeira faixa de plano, e entre 100 a 250 usuários como uma segunda faixa.

100. Outro modelo de precificação utilizado é o pagamento por uso, o qual tipicamente cobra pelo número de usuários e quantidade de recursos (por exemplo: volume de armazenamento, uso de CPU etc) consumidos em um dado período de tempo.

101. Ressalta-se que o cliente deve verificar as ferramentas e formas de monitoração oferecidas pelo provedor. Além disto, deverão ser criados processos para monitoramento da utilização baseado nos usuários individualmente, e os clientes deverão possuir controle amplo sobre a administração dos seus usuários, também evitando provedores que não permitam modelos de segurança onde o cliente determine as permissões e papéis de seus usuários.

3.3 Acordos de nível de serviço

*102. O contrato estabelecido com o provedor deve incluir cláusula para "Acordos de Nível de Serviço" (**Service Level Agreements** - SLAs), com parâmetros específicos e níveis mínimos para cada elemento do serviço fornecido. Tais acordos necessitam ser razoáveis e exequíveis, e ao mesmo tempo estabelecer punições ou compensações quando do seu não-cumprimento. Parâmetros abordados normalmente dentro de tais acordos são disponibilidade, tempo de resposta, desempenho, tempo para correção de erros ou incidentes, e segurança.*

103. Dentro da miríade de contratos-padrão dos provedores de nuvem, é importante definir os conceitos a serem abordados para SLA, pois cada provedor utiliza sua própria terminologia e não há uniformidade entre eles. Como exemplo, a Microsoft define "máximo de minutos disponíveis", "tempo de inatividade", "porcentagem de tempo de atividade mensal", este último correspondendo ao percentual de disponibilidade em um mês, além de todo o vocabulário restante com termos que remetem ao tipo de serviço ofertado. Já o Google Apps utiliza conceitos de "inatividade", "serviços cobertos pelo Google", "porcentagem de atividade mensal". Dentro destes conceitos, os cálculos podem variar – cita-se aqui a Mandic, provedora de IaaS no mercado brasileiro, que considera como base períodos de 15 minutos de indisponibilidade e totais de períodos de 15 minutos em um mês, para o cálculo de seu SLA.

104. Outro ponto a ser observado diz respeito às exceções à computação do SLA, como manutenções programadas, casos fortuitos ou força maior, estes últimos muitas vezes com definições não claras.

105. As sanções previstas para o não cumprimento dos níveis de serviço geralmente preveem créditos em dias de serviço, proporcionais à indisponibilidade, ou em descontos no valor a ser pago no faturamento. Nem todos os provedores deduzem isto de maneira automática. O Google Apps, por exemplo, prevê que o cliente deverá solicitar, dentro de 30 dias, o crédito ao qual tem direito. Além disto, muitos incluem percentuais e limites superiores para as multas ou descontos que necessitam ser bem analisados e discutidos, objetivando razoabilidade para as duas partes.

106. Para garantir e monitorar o atendimento aos níveis de serviço acordados, um contrato deve prever o direito do cliente a auditar registros, ou logs, de desempenho e possuir acesso a estatísticas de qualidade de serviço. Dentro do padrão, alguns provedores fornecem monitoramento básico sem cobrança adicional, que pode não ser satisfatório para o cliente monitorar o SLA contratado. Métricas personalizadas também são cobradas à parte, e também existe cobrança a depender do nível de armazenamento de logs. A Amazon, por exemplo, para o serviço EC2 (IaaS), oferece dois níveis de

monitoramento: básico, com sete métricas pré-selecionadas a uma frequência de cinco minutos e três métricas de verificação de status a uma frequência de um minuto, sem custo adicional, e o detalhado, com custo adicional, que inclui todas as métricas disponíveis no monitoramento básico a uma frequência de um minuto, com agregação de dados.

107. Está claro que os provedores de computação em nuvem, dentro de qualquer modelo, trabalham com seus próprios parâmetros de precificação e métricas de disponibilidade. A filosofia da computação em nuvem permite a redução de custos através da automatização e escala de uso, e derivando-se disto não há muita margem para flexibilização nos termos contratuais ofertados. Vê-se o mercado consumidor adaptando-se ao que é ofertado pelos provedores, em troca de ganho de agilidade e redução de custos. Neste cenário, ainda é incerto o que poderá ser fornecido a mais para atender determinadas necessidades de um contratante. Provavelmente o ***cloud broker*** *poderá vender serviços mais especializados e adequados a requisitos estabelecidos pelo cliente, obviamente a um custo adicional agregado.*

4. Quadro normativo aplicável a contratações de computação em nuvem pela APF

108. O escopo do trabalho está limitado ao ambiente de contratações públicas da administração pública federal (APF) regidas pelo regulamento geral estabelecido pela Lei 8.666/1993 e por normas específicas que a complementam, como a Lei 10.520/2002, que institui o pregão, e o Decreto 5.450/2005, que regulamenta o pregão eletrônico. Portanto, não foram consideradas situações de organizações públicas que possuem regulamentos específicos próprios.

109. Além disso, o escopo do trabalho também está restrito a aspectos particulares da contratação de serviços de computação em nuvem, não incluindo a análise de aspectos comuns da contratação de serviços de TI em geral, como os regulamentados pela Instrução Normativa SLTI/MP 4/2014.

110. Desse modo, buscou-se identificar normativos brasileiros específicos sobre computação em nuvem ou pontos específicos em normativos gerais que pudessem ter aplicabilidade nas contratações de serviços de computação em nuvem pela APF.

4.1 Marco Civil da Internet

111. Dentro do quadro normativo brasileiro recente, destaca-se o chamado Marco Civil da ***Internet*** *(Lei 12.965/2014), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Como pontos positivos do Marco Civil da* ***Internet****, destacam-se a obrigatoriedade de neutralidade da rede (todos os fluxos de dados devem ser tratados igualmente) e as garantias de privacidade e liberdade de expressão para os usuários.*

112. Pelo fato de a rede mundial ser o principal meio de acesso a serviços disponíveis em nuvem, principalmente em nuvens públicas, o Marco Civil da ***Internet*** *era aguardado pelo mercado com apreensão, pois poderia representar restrição à oferta de serviços de computação em nuvem por fornecedores multinacionais. Caso a lei fosse aprovada conforme a proposta do governo, os dados dos usuários brasileiros deveriam ser obrigatoriamente armazenados em bases de dados de data centers localizados fisicamente no Brasil.*

*113. O caso de Edward Snowden, ex-prestador de serviço terceirizado da NSA (****National Security Agency****), que revelou um esquema de monitoramento de dados e espionagem por parte do governo dos EUA, foi um dos motivadores da discussão, sendo que o armazenamento de dados localmente era indicado como uma forma de mitigar o risco de espionagem e vazamento de informações. Em território nacional, os provedores de serviço ficam sujeitos ao foro brasileiro e os usuários são beneficiados pelo direito de privacidade assegurado inclusive pelo próprio Marco Civil da* ***Internet****, pois uma quebra de sigilo só pode ser feita mediante ordem judicial brasileira. Por outro lado, o alto custo dos datacenters no Brasil quando comparado a outros países era apontado como obstáculo pelas empresas do mercado de serviços de TI.*

114. Devido à polêmica em torno do tema, o Brasil optou por finalmente retirar essa restrição e estabelecer apenas como diretriz para atuação do poder público no desenvolvimento da ***Internet*** *no Brasil a "otimização da infraestrutura das redes e estímulo à implantação de centros de*

armazenamento, gerenciamento e disseminação de dados no País" (Lei 12.965/2014, art. 24, inciso VII).

4.2 Decreto 8.135/2013 e Portaria Interministerial 141/2014

115. Por outro lado, como resposta do Brasil às notícias de espionagem por parte dos EUA, o Decreto 8.135/2013 foi mais restritivo ao tentar colocar as comunicações de dados do governo federal sob controle e tutela de empresas públicas da União, buscando assegurar a soberania dos dados. Em seu art. 1º, caput, o Decreto determina que: "As comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de TI fornecidos por órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias".

116. No art. 2º, o Decreto dispensa "[...] a licitação para contratação de órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista e suas subsidiárias, para atendimento ao disposto no art. 1º".

117. Desse modo, com objetivo de garantir a inviolabilidade das comunicações de dados para preservar a segurança nacional, o Decreto restringe o fornecimento de serviços para a comunicação de dados da APF a empresas públicas, como Serpro, Dataprev e Telebras. Entretanto, conforme o Decreto já prevê (art. 1º, § 5º, inciso II), existe a necessidade de considerar a capacidade dessas empresas de ofertar satisfatoriamente esses serviços.

118. Outros pontos do art. 1º também merecem destaque:

> *§ 2º Os órgãos e entidades da União a que se refere o **caput** deverão adotar os serviços de correio eletrônico e suas funcionalidades complementares oferecidos por órgãos e entidades da administração pública federal.*
> *(...)*
> *§ 4º O armazenamento e a recuperação de dados a que se refere o **caput** deverá ser realizada em centro de processamento de dados fornecido por órgãos e entidades da administração pública federal.*
> *$ 5º Ato conjunto dos Ministros de Estado da Defesa, do Planejamento, Orçamento e Gestão e das Comunicações disciplinará o disposto neste artigo e estabelecerá procedimentos, abrangência e prazos de implementação, considerando:*
> *I - as peculiaridades das comunicações dos órgãos e entidades da administração pública federal; e*
> *II - a capacidade dos órgãos e entidades da administração pública federal de ofertar satisfatoriamente as redes e os serviços a que se refere o **caput**.*

119. O Expresso V3 do Serpro (parágrafo 71) é um serviço de correio eletrônico e funcionalidades complementares que pode ser adotado pelos órgãos e entidades da União. Os centros de processamento de dados tanto do Serpro como da Dataprev podem realizar o armazenamento e a recuperação de dados a que se refere o caput do art. 1º.

120. Em decorrência do comando do § 5º indicado acima, a Portaria Interministerial 141/2014 (ato conjunto dos Ministros de Estado da Defesa, do Planejamento, Orçamento e Gestão e das Comunicações) estabelece os procedimentos a serem observados pela APF para a contratação de serviços de comunicação de dados (Capítulo III). Além disso, estabelece requisitos de implementação dos serviços (Capítulo IV) e de auditoria de programas e equipamentos (Capítulo V), bem como define as competências do Ministério do Planejamento, Orçamento e Gestão (MP), como órgão gerenciador em relação à contratação dos serviços previstos na Portaria (Capítulos II e VI).

121. No capítulo III, seção I, artigos 5º e 6º, a Portaria trata dos procedimentos gerais para contratação dos serviços. O caput do art. 5º determina que "a contratação de serviços de redes de telecomunicações e de tecnologia da informação prestados por órgãos ou entidades fornecedores deverá ser efetuada por dispensa de licitação". O § 1º estabelece que a contratação "será efetuada em conformidade com as normas e os procedimentos estabelecidos pelo órgão gerenciador, observada as disposições relativas à segurança da informação e comunicações fixadas pelo Gabinete de Segurança Institucional da Presidência da República" (grifou-se).

122. Entretanto, conforme informação da Nota Técnica 255 /DSR/SLTI-MP (peça 44, p. 2-4), encaminhada pelo Ofício 3456 /DSR/SLTI-MP (peça 44, p. 1), as normas e os procedimentos ainda estão sendo elaborados e serão formalizados por meio de uma instrução normativa da SLTI/MP.

123. Um procedimento importante estabelecido pela Portaria Interministerial 141/2014 é a consulta, que o órgão ou entidade contratante deve fazer até o término da fase de planejamento da contratação, sobre a disponibilidade para atendimento das especificações técnicas e níveis de serviço necessários (art. 5º, § 3º), pois a contratação de órgãos e entidades fornecedores a que se refere o caput do art. 5º deixa de ser obrigatória nos casos em que não houver oferta da prestação de serviço demandada (art. 6º, inciso I).

124. Nesses casos, a Portaria abre possibilidade de contratação com fornecedores privados (capítulo III, seção II, artigo 7º). Segundo o § 1º do art. 7º, o serviço será considerado não ofertado quando o órgão ou entidade fornecedor: "não atender à localidade da prestação do serviço" (inciso I), não atender aos requisitos técnicos demandados pelo contratante (inciso II), "não responder a consulta formal sobre o atendimento dos serviços no prazo de trinta dias" (inciso III), e "não puder enquadrar a demanda do órgão ou entidade contratante nas prioridades de contratação de que trata o art. 4º, inciso I, alínea 'a'" (inciso IV).

125. Nesse ponto, destaca-se da minuta de instrução normativa encaminhada pela SLTI/MP (peça 44, p. 5-10) que a prioridade de contratação obedecerá o plano de disponibilidade de prestação de serviços apresentado pelo órgão ou entidade fornecedor (conforme art. 4º, inciso I, alínea "a", da Portaria Interministerial 141/2014) e que a prioridade de atendimento dos serviços será definida com base nos seguintes critérios:

> *I – observância de imperativos estratégicos e de segurança nacional;*
> *II – nível de urgência no atendimento, entendido como os riscos causados pela não disponibilização do serviço;*
> *III – capacidade de atendimento pelo órgão ou entidade fornecedor.*

126. Continuando no texto da Portaria, o capítulo IV trata dos requisitos de implementação dos serviços; a seção I, artigos 8º e 9º, dos requisitos comuns; a seção II, artigos 10, 11 e 12, dos requisitos específicos.

127. O art. 8º estabelece que os serviços prestados tanto por fornecedores privados como por órgãos e entidades da APF devem adotar padrões específicos definidos na arquitetura e-PING – Padrões de Interoperabilidade de Governo Eletrônico.

128. Os incisos do art. 9º relacionam obrigações do órgão ou entidade contratado que devem estar contidas no termo de referência ou projeto básico e no contrato, como:

> *(...)*
> *II - apresentação da política de segurança de dados e o detalhamento das ações de segurança da informação e comunicações a serem implementadas nos serviços contratados;*
> *III - fornecimento (...) de informações de monitoramento e acesso a instrumentos e procedimentos de prevenção e reação a incidentes de segurança;*
> *(...)*
> *V - manutenção de confidencialidade das informações e documentos (...);*
> *VI - comunicação à Administração da ocorrência de incidentes de segurança e a existência de vulnerabilidades relativas ao objeto da contratação (...);*
> *VII - fornecimento de informações gerenciais sobre o desempenho dos serviços objeto do contrato, de maneira agregada e individualizada;*
> *VIII - possibilidade de realização de auditoria em programas e equipamentos por órgão ou entidade contratante ou por instituição credenciada pelo Governo Federal.*

129. Com relação aos requisitos específicos, o art. 10 estabelece como requisitos mínimos para os serviços de redes de telecomunicações: "I - utilização de ferramenta de monitoramento do tráfego" e "II - utilização de ferramentas de prevenção à intrusão no acesso do serviço de Internet".

130. Os incisos do art. 11 definem os serviços de TI que a Portaria abrange: "I - correio eletrônico"; "II - compartilhamento e sincronização de arquivos"; "III - mensageria instantânea"; "IV - conferência (teleconferência, telepresença e webconferência)"; e "V - comunicação de voz sobre protocolo de internet (VoIP)".

131. Devido às suas características técnicas, esses serviços, especialmente o de correio eletrônico e o de compartilhamento e sincronização de arquivos, podem ser viabilizados pela tecnologia de computação em nuvem; enquanto os serviços de redes de telecomunicações citados no caput do art. 1º são viabilizadores dos serviços de computação em nuvem. Desse modo, o gestor público deve considerar o disposto no Decreto 8.135/2013 e na Portaria Interministerial 141/2014 no planejamento

da contratação de serviços de computação em nuvem, embora não sejam objetos explícitos desses dois normativos.

132. Entretanto, ressalva-se que a equipe de fiscalização não entrou na análise de mérito quanto à aplicabilidade do Decreto 8.135/2013 e da Portaria 141/2014 aos diversos tipos de serviços de computação em nuvem. Analisar se um serviço em particular enquadra-se ou não nas definições desses dois normativos ou se pode comprometer ou não a segurança nacional só é possível em casos concretos e depende do contexto e do risco de cada contratação. Portanto, essa decisão caso a caso é tarefa da administração com apoio de sua consultoria jurídica.

133. Com relação à segurança da informação, os incisos do art. 12 da Portaria definem critérios mínimos que os serviços de TI devem adotar: uso de criptografia para informações sigilosas (inciso I); uso de ferramenta de controle de acesso e de gerenciamento de identidades (inciso II); uso de ferramenta de prevenção do envio de mensagens em massa e de ferramenta de detecção de códigos maliciosos especificamente para os serviços de correio eletrônico e mensageria instantânea (§ 1º); e de ferramenta de detecção de códigos maliciosos para os serviços de compartilhamento e sincronização de arquivos (§ 2º).

134. No capítulo V, artigos 13 e 14, a Portaria trata da auditoria de programas e equipamentos. De acordo com o Art. 14, o termo de referência ou projeto básico e o respectivo contrato devem prever a possibilidade de auditoria em programas e equipamentos de acordo com as diretrizes e especificações da arquitetura e-PING – Padrões de Interoperabilidade de Governo Eletrônico.

4.3 <u>Normas complementares do DSIC/GSI/PR</u>

135. O § 1º do art. 5º da Portaria 141/2014 estabelece que a contratação de serviços de redes de telecomunicações e de tecnologia da informação para as comunicações de dados da APF deve observar as disposições relativas à segurança da informação e comunicações fixadas pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

136. Essas disposições estão positivadas por meio das normas complementares à Instrução Normativa GSI/PR 1/2008, que são emitidas pelo Departamento de Segurança da Informação e Comunicações (DSIC) do GSI/PR. Especificamente para o objeto deste levantamento, existe a Norma Complementar 14/IN01/DSIC/GSIPR, que estabelece "diretrizes relacionadas à segurança da informação e comunicações para o uso de computação em nuvem nos órgãos e entidades da administração pública federal". Subsidiariamente, existe a Norma Complementar 19/IN01/DSIC/GSIPR, que estabelece "padrões mínimos de segurança da informação e comunicações para os sistemas estruturantes da administração pública federal".

137. De acordo com a Norma Complementar 14/IN01/DSIC/GSIPR, "antes de adotar a tecnologia de computação em nuvem", os órgãos ou entidades da APF devem observar no mínimo (item 5.1):

> *5.1.1. As diretrizes estabelecidas em sua POSIC [(Política de Segurança da Informação e Comunicações)];*
> *5.1.2. As diretrizes do processo de Gestão de Riscos de SIC [Segurança da Informação e Comunicações)] a respeito da adoção dos modelos de serviço e implementação de computação em nuvem;*
> *5.1.3. As diretrizes do processo de Gestão de Continuidade de Negócios nos aspectos relacionados à SIC;*

138. "Ao contratar ou implementar um serviço de computação em nuvem", os órgãos ou entidades devem garantir que (item 5.2):

> *5.2.1. O ambiente de computação em nuvem, sua infraestrutura e canal de comunicação estejam aderentes às diretrizes e normas de SIC, estabelecidas pelo GSIPR, e às legislações vigentes;*
> *5.2.2. A legislação brasileira prevaleça sobre qualquer outra, de modo a ter todas as garantias legais enquanto tomadora do serviço e proprietária das informações hospedadas na nuvem;*
> *5.2.3. O contrato de prestação de serviço, quando for o caso, deve conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço;*

139. Os órgãos ou entidades devem "avaliar quais informações serão hospedadas na nuvem", considerando (item 5.3):

> *5.3.1. O processo de Classificação da Informação de acordo com a legislação vigente;*
> *5.3.2. O valor do ativo de informação;*

5.3.3. Os Controles de Acesso, físicos e lógicos, relativos à SIC;
5.3.4. O modelo de serviço e de implementação de computação em nuvem a serem adotados;
5.3.5. A localização geográfica onde as informações estarão fisicamente armazenadas.

140. Assim sendo, independentemente da avaliação de quais informações serão hospedadas na nuvem, a Norma Complementar 14/IN01/DSIC/GSIPR, ao estabelecer que a legislação brasileira prevaleça sobre qualquer outra, pode limitar na prática o processamento e o armazenamento dos dados apenas em data centers localizados no Brasil, sem permitir a possibilidade de contingência ou replicação no exterior. Por outro lado, pode oferecer maior segurança jurídica e proteção da soberania sobre os dados.

141. No caso dos sistemas estruturantes dos órgãos e entidades da APF, buscou-se uma proteção ainda maior por meio da Norma Complementar 19/IN01/DSIC/GSIPR, a qual estabelece que as soluções de infraestrutura de nuvem para esses sistemas devem estar restritas às infraestruturas de órgãos ou entidades da APF (item 4.2.3), como Serpro e Dataprev.

142. O item 3.9 da Norma Complementar 19/IN01/DSIC/GSIPR apresenta a seguinte definição para sistema estruturante: "sistema com suporte de tecnologia da informação fundamental e imprescindível para planejamento, coordenação, execução, descentralização, delegação de competência, controle ou auditoria das ações do Estado, além de outras atividades auxiliares, desde que comum a dois ou mais órgãos da Administração e que necessitem de coordenação central".

4.4 Normas técnicas brasileiras relacionadas à computação em nuvem

143. Como o escopo do trabalho está restrito a aspectos particulares da contratação de serviços de computação em nuvem, não incluindo a análise de aspectos comuns da contratação de serviços de TI em geral, buscou-se identificar normas técnicas brasileiras que tratassem do tema de forma específica ou pontos específicos (controles e boas práticas) em normas técnicas brasileiras de TI em geral. Desse modo, não foi analisada, por exemplo, a aplicação dos controles gerais de segurança da informação da Norma Técnica NBR ISO/IEC 27002:2013 no contexto do ambiente dos serviços de computação em nuvem.

144. A única referência direta a computação em nuvem nessa norma está no item 15.1 – Segurança da informação na cadeia de suprimento –, cujo objetivo é "Garantir a proteção dos ativos da organização que são acessados pelos fornecedores". É uma referência pontual no subitem 15.1.3 – Cadeia de suprimento na tecnologia da informação e comunicação –, no qual há a recomendação para que "acordos com fornecedores incluam requisitos para contemplar os riscos de segurança associados à cadeia de suprimento de produtos e serviços de tecnologia da informação e comunicação", sendo que a cadeia de suprimento "aqui abordada inclui os serviços de computação em nuvem".

145. Entretanto, não foi identificada pela equipe de fiscalização nenhuma outra norma técnica brasileira que pudesse ser referência para a contratação de serviços de computação em nuvem pela APF.

5. Política e estratégia de governo relacionada a computação em nuvem

146. Uma política de governo que regulamente e também incentive o uso da computação em nuvem pode contribuir para o alcance de benefícios não só para a administração pública, mas também para organizações da iniciativa privada, sejam elas usuárias ou provedoras de recursos de tecnologia da informação.

147. Considerando o mercado brasileiro, há que se esperar que, a partir de uma intervenção positiva por parte do governo para promover e regulamentar o seu uso, a utilização da computação em nuvem seja cada vez mais expressiva pela administração pública, promovendo consequentemente o crescimento do mercado de provedores e a confiança de pequenas e médias empresas no modelo, que passariam então a utilizar-se também desses serviços, alcançando benefícios de economia, agilidade e inovação.

148. De acordo com TAKAHASHI (2000), o setor governamental é o principal indutor de ações estratégicas rumo à Sociedade da Informação, seja porque cabe ao governo definir o quadro regulatório dentro do qual projetos e iniciativas concretas poderão ser formuladas, seja porque como regra o governo é o maior consumidor de bens e serviços em tecnologias de informação e comunicação em um país. Isso representa uma grande responsabilidade dos atores institucionais encarregados pela definição das tecnologias a serem utilizadas no setor público, pois ao decidir fazer uso da computação

em nuvem, o governo pode acelerar o uso do modelo em toda a economia, gerando benefícios para toda a sociedade.

149. Entretanto, o que se verificou neste trabalho é que as iniciativas de governo ainda são incipientes.

5.1 Programa TI Maior do MCTI

150. O TI Maior, programa estratégico de software e serviços de tecnologia da informação do Ministério da Ciência, Tecnologia e Inovação (MCTI), prevê investimentos de R$ 40 milhões em pesquisa, desenvolvimento e inovação (P,D&I) em tecnologia de computação em nuvem, no período 2012-2015, com os seguintes objetivos:

a) Estabelecimento de um conjunto de incentivos para a atração de grandes centros de dados regionais para o Brasil (data centers);
b) Criação do Comitê Interministerial de Computação em Nuvem, no âmbito de governo e com participação da sociedade civil organizada, com as atribuições de definir padrões interoperáveis entre fornecedores em território nacional, áreas para investimentos em P,D&I, infraestrutura acadêmica para computação em nuvem, harmonização tecnológica internacional, dentre outros temas;
c) Apoio à criação de uma Lei de Proteção de Dados Pessoais;
d) Criação de um Centro Nacional de Computação em Nuvem, articulado em rede, com a presença de universidades, empresas e governos;
e) Criação de três demonstrações piloto em nuvem de uso governamental;
f) Amplo programa de capacitação de profissionais em subáreas, tais como virtualização, armazenamento (SAN), aplicações analíticas, segurança e novas arquiteturas.

151. Entretanto, com base em informações da Secretaria de Política de Informática (Sepin) do MCTI, fornecidas por meio do Ofício 583/2014 Gab/Sepin, de 2/12/214 (peça 40), verificou-se que pouco foi realizado para cada um dos objetivos acima elencados:

a) Para o estabelecimento de um conjunto de incentivos para atração de data centers, foi realizado apenas "um estudo detalhado sobre os fatores comparativos e distintivos que o Brasil possui frente a outros países", cujos resultados demonstraram que o país é pouco competitivo;
b) Quanto ao Comitê Interministerial de Computação em Nuvem, foi elaborada apenas uma minuta de portaria para criação de um comitê técnico sobre o tema nuvem e governo;
c) O projeto de lei de proteção de dados pessoais estava ainda em elaboração;
d) A criação de um centro nacional de computação em nuvem e a realização de demonstrações piloto em nuvem governamental não se concretizaram, "em grande parte, pela falta de consenso no âmbito do governo sobre como conduzir estas duas ações e também pela falta de recursos disponíveis";
e) Com relação a um amplo programa de capacitação de profissionais, poderá ser criada uma nova trilha dentro do Programa Brasil + TI, contemplando conceitos e tecnologias ligadas a nuvem.

152. Como iniciativa de uso de nuvem, destaca-se a oportunidade identificada pela Sepin de "conjugar a ação de computação avançada de alto desempenho (high-performance computing), rede de pesquisa de alta performance e uso de equipamentos de data centers com o objetivo de prover infraestrutura de pesquisa computacional em nuvem para fim de apoio às pesquisas em várias áreas do conhecimento que demandem altas cargas de processamento como é o caso de simulações" (peça 40, p. 2).

153. Por último, a Sepin informou as três linhas em que o seu trabalho no âmbito da computação em nuvem vem se desenvolvendo (peça 40, p. 3):

a) "fundamentar tecnicamente órgãos públicos sobre conceitos e tecnologias relativas a computação em nuvem, em especial por meio de um grupo de pesquisadores dedicados ao tema no CTI (Centro de Tecnologias da Informação Renato Archer) em Campinas";

b) "estimular e apoiar ações de orientação e regulamentação/normatização quanto ao uso de computação em nuvem no âmbito do governo federal";

c) "tendência para a consolidação de uma nuvem para suporte a pesquisa científica com base em três pilares: rede dedicada e de alta velocidade, data center compartilhado e computação de alto desempenho".

154. Ainda no âmbito do TI Maior, estão previstas várias ações de incentivo, fomento e financiamento à pesquisa e desenvolvimento em TI no Brasil. Dentre essas, destaca-se a subvenção econômica da Finep, empresa pública vinculada ao MCTI. Em seleção pública de 2013 (peça 62), os projetos para computação em nuvem receberam os maiores valores. A empresa multinacional IBM, por exemplo, que solicitou R$ 5.699.601,44 em sua proposta, foi selecionada para o desenvolvimento de uma plataforma como serviço em nuvem (PaaS) para aplicações com demanda dinâmica por recursos computacionais especializados e de alto desempenho (peça 63).

5.2 Datagov

155. De acordo com a SLTI/MP, a Estratégia Geral de Segurança Cibernética do Sistema de Administração dos Recursos de Tecnologia da Informação (EGSC.Sisp) será um instrumento de gestão que definirá macro diretrizes com objetivo de aumentar os níveis da segurança cibernética nos órgãos e entidades integrantes do Sisp (peça 48, p. 6).

156. Dentre as iniciativas previstas (peça 48, p. 8), destaca-se o Datagov, que, por conceito, será um "conjunto integrado de componentes de alta tecnologia que possibilitará o fornecimento de serviços de infraestrutura de valor agregado, geralmente processamento e armazenamento de dados, em larga escala e que otimize a utilização dos recursos de TI", que "deverá suportar a recuperação dessa infraestrutura em caso de desastres, fazendo com que os órgãos e entidades do Sisp continuem a funcionar sem interrupção, de forma a entregar níveis de serviço adequados" (peça 48, p. 12).

157. O objetivo do Datagov é "modelar e implantar ambiente de Data Center compartilhado entre os órgãos e entidades da APF, visando à continuidade dos processos de negócio considerados essenciais para a ação do Estado" (peça 49, p. 5).

158. Desse modo, conforme a estrutura de governança proposta, o Datagov pretende compartilhar infraestrutura de TIC (especialmente serviços de data center e telecomunicações) do Serpro, Dataprev e Telebras entre órgãos e entidades do Sisp e prover serviços em nuvem para a APF e para a sociedade, sendo que há previsão de parceria também com a iniciativa privada (peça 48, p. 13-14).

159. Dentre as justificativas para o Datagov apontadas pela a SLTI/MP, cita-se a necessidade de (peça 49, p. 10):

1) maior segurança aos dados e informações sensíveis do Estado;

2) melhoria dos processos de segurança da informação;

3) melhoria de desempenho e disponibilidade dos sistemas estruturantes da APF;

4) maior resiliência para sistemas críticos;

5) prestação de serviços em nuvem (infraestrutura como serviço e software como serviço.

160. Dentre os benefícios esperados, cita-se (peça 49, p. 12):

1) redução de custos;

2) padronização;

3) integração e interoperabilidade;

4) gestão centralizada (arquitetura central de gestão do Sisp).

161. Um objetivo específico destacado pela SLTI/MP é "promover a gestão de SIC em conformidade com o arcabouço legal vigente", de modo que "os órgãos e entidades atenderiam requisitos legais e boas práticas no que se refere às suas informações sob a custódia do DataGov". Especialmente em relação à conformidade com o Decreto 8.135/2013, deverá ser realizada auditoria de hardware e software nos ativos de informação do Datagov (peça 49, p. 13).

162. Após a realização de oficinas com o Serpro e Dataprev e a definição de um plano de projeto, os próximos passos planejados pela SLTI/MP são a criação de grupos de trabalho (em níveis estratégico e tático) e a definição de um modelo (peça 49, p. 15-20).

5.3 EGTIC 2014-2015

163. Dentro do objetivo "Implantar soluções de TIC que fortaleçam a padronização e o reuso" (peça 50, p. 45), a Estratégia Geral de Tecnologia da Informação e Comunicações (EGTIC) 2014-2015 do Sisp prevê o projeto "Disponibilizar modelo de oferta de serviços em nuvem aos órgãos do Sisp", cujo responsável é a SLTI/MP e o prazo é 2015. A descrição do projeto é "Orientar os órgãos do SISP, por intermédio de uma Instrução Normativa, que defina um modelo de oferta de serviços em nuvem a ser implantado nos órgãos. (...) O modelo a ser proposto deverá estar alinhado com Decreto nº 8.135, de 4 de novembro de 2013, Portaria Interministerial nº 141, de 5 de maio de 2014, suas regulamentações posteriores e Norma Complementar nº 14/IN01/DSIC/GSIPR, de 30 de janeiro de 2012" (peça 50, p. 47).

164. Entretanto, conforme informação da Nota Técnica 255/DSR/SLTI-MP (peça 44, p. 2-4), encaminhada pelo Ofício 3456/DSR/SLTI-MP (peça 44, p. 1), "as ações acima estão previstas para realização durante o ano de 2015, tendo sido iniciada a discussão do tema em reunião de coordenação do SISP e criado Grupo de Trabalho, contando com a participação de alguns dos órgãos que compõem o SISP e tendo como objetivo definir aspectos relacionados à hospedagem de equipamentos e serviços em seus diversos formatos" (grifou-se).

6. Normas e padrões internacionais aplicáveis à contratação e à auditoria de serviços de computação em nuvem

165. Como o escopo do trabalho está dirigido a aspectos particulares da contratação de serviços de computação em nuvem, buscou-se identificar normas técnicas e padrões internacionais específicos sobre o tema ou a aplicabilidade de pontos específicos em normas e padrões gerais de TI. O objetivo foi identificar referências de boas práticas e controles relacionados à contratação e à auditoria de serviços de computação em nuvem que pudessem ser utilizados na identificação de riscos e na elaboração da matriz de auditoria.

166. Há diversos esforços de padronização nas formas de auditoria de prestação de serviços em nuvem. Como uma das características de serviços em nuvem encontra-se em ganhos de escala crescentes, tem-se um limitado número de fornecedores com um grande número de clientes, o que torna pouco provável que cada cliente audite por si próprio os controles de cada fornecedor.

167. Assim, a solução mais comum de auditoria é o próprio fornecedor contratar serviços de auditoria externa de reconhecidas empresas especializadas (comumente por uma das "4 grandes": KPMG, Deloitte Touche Tohmatsu, PriceWaterhouseCoopers e Ernst & Young), que aplicam procedimentos de auditoria padronizados e cujos relatórios são comunicados aos clientes para que estes avaliem se os riscos específicos do fornecedor são aceitáveis.

168. Duas instituições se destacam na padronização de procedimentos de auditoria para nuvem e também servem de referência para avaliação de fornecedores: CSA (Cloud Security Alliance) e AICPA (American Institute of Certified Public Accountants). Quanto à definição de controles e boas práticas em ambiente de nuvem, destacam-se também a ENISA (European Union Agency for Network and Information Security) e o NIST (National Institute of Stantards and Technology).

169. Apesar de ser um framework de governança de TI em geral, o Cobit 5 da Isaca (Information Systems Audit and Control Association) também é uma referência para implantação de serviços de computação em nuvem pelas organizações.

6.1 CSA

170. A Aliança para Segurança em Nuvem (Cloud Security Alliance - CSA) é uma organização sem fins lucrativos com a missão de promover a utilização das melhores práticas para prover garantias de segurança na prestação de serviços de computação em nuvem, e educar o público sobre seus usos como forma de proteger todas as demais modalidades de computação. A CSA é liderada por uma ampla coalizão de profissionais da indústria, empresas, associações e outras partes interessadas.

171. A CSA elaborou uma matriz de controles de nuvem (Cloud Controls Matrix - CCM, peça 64) como uma meta-estrutura de controles de segurança específicos para nuvem, mapeando os padrões de referência, melhores práticas e regulação governamental.

172. Também foi elaborado o guia "Security Guidance for Critical Areas of Focus in Cloud Computing" (peça 65), com orientações e recomendações para reduzir riscos na adoção de computação em nuvem. O documento está estruturado em 14 domínios que cobrem arquitetura, governança e operações em ambiente de computação em nuvem.

173. A principal referência hoje é o programa Registro de Segurança, Confiança e Garantia da CSA (Security, Trust & Assurance Registry - STAR). O STAR fornece avaliações de diversos provedores de serviços de nuvem em função da matriz de controles de nuvem da CSA (matriz CCM), com o objetivo de desenvolver confiança nos provedores de serviços de nuvem e padronizar garantias sobre seus serviços. Assim, o STAR provê um registro acessível ao público, projetado para reconhecer as exigências de garantia e variados níveis de maturidade dos fornecedores e consumidores. O modelo é usado por clientes, fornecedores, indústrias e governos de todo o mundo.

*174. Há também um projeto em curso da CSA para padronizar uma interface de programação de aplicações (**application programing interface** - API) para funcionalidades de automação de auditoria, asseveração, avaliação e garantia (**assurance**) chamada CloudAudit.*

6.2 AICPA

*175. O Instituto Americano de Contadores Públicos Certificados (**American Institute of Certified Public Accountants** - AICPA) é uma organização profissional de contadores públicos dos Estados Unidos. O AICPA desenvolve padrões para auditoria de prestadores de serviço para empresas americanas e elaborou controles específicos de segurança aplicáveis aos prestadores de serviços de computação em nuvem.*

*176. O relatório de Controles de Prestador de Serviço (**Service Organization Controls** - SOC) avalia controles internos do prestador de serviço em aspectos relevantes para a segurança, disponibilidade, integridade de processamento, confidencialidade e privacidade. O relatório de tipo 2 (SOC 2) relata a descrição do sistema de informação do prestador de serviço, a adequação do sistema aos seus propósitos e a efetividade operacional de seus controles internos.*

177. Esses relatórios SOC 2 tornaram-se o padrão de referência para comparar desempenho e riscos associados de propostas de diferentes prestadores de serviço para computação em nuvem.

6.3 ENISA

*178. A Agência da União Europeia para a Segurança das Redes e da Informação (**European Union Agency for Network and Information Security** - ENISA) estabeleceu um quadro referencial de garantias (**Cloud Computing Information Assurance Framework**) destinado a avaliar o risco de adoção de serviços em nuvem, comparar ofertas de diferentes provedores de nuvem, obter garantias dos provedores de nuvem selecionados e reduzir o esforço necessário para que os provedores de nuvem forneçam garantias padronizadas e criem confiança junto aos seus clientes.*

179. O quadro-referência da ENISA (peça 66) prevê um conjunto de questões que uma organização pode abordar junto a provedores de nuvem para assegurar-se de que eles estão protegendo adequadamente a informação que lhes foi confiada.

180. Estas perguntas têm a intenção de fornecer uma base mínima comum. Assim alguma organização pode ter requisitos específicos adicionais não cobertos pelo questionário.

181. Similarmente, o questionário não fornece um formato padrão de resposta para o provedor de nuvem, contemplando respostas em formato de texto livre. No entanto, o conjunto das respostas deverá alimentar uma referência detalhada mais abrangente, que ainda será desenvolvida, permitindo padronizar um conjunto consistente, comparável de respostas. Tais respostas fornecerão métricas quantificáveis e poderão ser utilizadas para avaliar a maturidade do provedor.

182. Pretende-se que essas métricas sejam coerentes e unificadas entre provedores de tal forma que os serviços oferecidos sejam facilmente comparáveis pelos usuários finais.

183. Assim, a solução para auditar fornecedores de serviços em nuvem, preconizada pela ENISA, é bastante semelhante ao registro de controles (STAR) da CSA e poderia ser amplamente utilizado no Brasil, elaborando-se semelhante registro das características dos principais fornecedores que atuam no mercado nacional.

*184. Destaca-se também o documento "**Cloud Computing Security Risk Assessment**" (peça 67), com benefícios, riscos e recomendações para segurança da informação em computação em nuvem.*

6.4 NIST

*185. O Instituto Nacional de Padrões e Tecnologia (**National Institute of Stantards and Technology** – NIST) é uma agência federal dos EUA, cuja missão é promover inovação e competitividade industrial. O NIST edita séries de publicações especiais em suas diversas áreas de atuação, incluindo tecnologia de sistemas computacionais (SP-500-XX) e segurança de computadores (SP-800-XX).*

*186. A publicação SP 800-145, "**The NIST Definition of Cloud**" (peça 68), apresenta a definição do NIST para computação em nuvem, a qual é adotada como referência para este trabalho (parágrafo 22).*

*187. A publicação SP 500-292, "**NIST Cloud Computing Reference Architecture**" (peça 69), apresenta uma arquitetura de referência do NIST para computação em nuvem, incluindo uma visão dos atores envolvidos e seus papeis e dos componentes necessários para a gestão e a prestação de serviços em nuvem, como implantação (**deployment**), orquestração, gerenciamento, segurança e privacidade.*

*188. Na publicação SP 800-144, "**Guidelines on Security and Privacy in Public Cloud Computing**" (peça 70), o NIST fornece uma visão geral da nuvem pública e apresenta considerações a respeito de segurança e privacidade no contexto da terceirização de dados, aplicações e infraestrutura para o ambiente de nuvem pública. São abordados aspectos de governança, conformidade, confiança, arquitetura, gerenciamento de identidade e acesso, isolamento de **software**, proteção de dados, disponibilidade e resposta a incidentes.*

6.5 ISACA

*189. "**Controls and Assurance in the Cloud: Using COBIT 5**" é uma publicação editada pela Isaca (**Information Systems Audit and Control Association**) com o propósito de mostrar como o Cobit 5 pode auxiliar as organizações na avaliação do valor da computação em nuvem para o negócio em função dos riscos associados com essa nova maneira de entregar serviços de TI, bem como na implantação de controles e mecanismos de governança apropriados.*

190. A publicação apresenta inicialmente os fundamentos da computação em nuvem, os desafios da computação em nuvem para o negócio em relação aos sete habilitadores do Cobit 5 e uma avaliação de risco da migração para nuvem em função dos modelos de serviços de nuvem.

191. De acordo com a publicação, quando uma organização decide usar computação em nuvem para prover serviços de TI, os processos de negócios são impactados, o que torna a governança ainda mais crítica. Gerenciar riscos crescentes e assegurar a continuidade de processos críticos de negócio que são estendidos além do data center local são algumas das razões pelas quais as organizações devem implementar uma boa governança em ambiente de nuvem.

192. Para obter consenso na organização e estabelecer as necessidades das partes interessadas em um programa de uso de computação em nuvem, a publicação sugere uma sequência de processos do Cobit 5. Considerando necessidades em geral (como conformidade com leis, regulamentos e políticas internas), objetivos organizacionais que são particularmente importantes em um ambiente de nuvem são identificados e correlacionados com objetivos de TI e também com processos do Cobit 5 que devem ser implementados para assegurar o alcance desses objetivos.

*193. A publicação apresenta também um guia prático para decidir se ativos devem ser movidos para a nuvem e qual modelo de serviço é o melhor para a organização. Os quatro passos recomendados são: i) preparar o ambiente interno; ii) selecionar o modelo de serviço de nuvem; iii) selecionar o modelo de implantação de nuvem; e iv) selecionar o provedor de nuvem. Destaca-se que: no primeiro passo é apresentado um método de cálculo de retorno de investimento (ROI – **return of investment**) para computação em nuvem, em que são apresentados também os benefícios (tangíveis e intangíveis), custos e desafios a serem considerados; no segundo é apresentada uma árvore de decisão para auxiliar na escolha do modelo de serviço; e no terceiro passo uma árvore de decisão para escolha do modelo de implantação.*

*194. Considerações de segurança para computação em nuvem são apresentadas com base na publicação "**Cobit 5 for Information Security**" (também da Isaca), incluindo relação de ameaças e correspondentes ações de mitigação.*

*195. Por causa de preocupações específicas como compartilhamento de recursos, arrendamento múltiplo e geolocalização, a computação nuvem requer uma nova abordagem para obtenção de confiança/garantia (**assurance**). Assim, a publicação analisa a aplicabilidade de alguns modelos e*

certificações ao ambiente de nuvem, bem como apresenta benefícios e desafios do uso de cada um deles.

196. A publicação aborda ainda alguns aspectos da parceria entre o provedor de serviços em nuvem e o cliente, que devem compartilhar responsabilidades pela gerência de ativos que residem na nuvem.

197. Ao final, os apêndices da publicação fornecem informações mais detalhadas sobre os tópicos abordados em cada capítulo. Destacam-se o apêndice A, que adapta o modelo de processos do Cobit 5 ao ambiente de nuvem e identifica as práticas de processos que são relevantes para usuários e provedores de serviços de nuvem (figura 35); o apêndice D, que exemplifica cenários de riscos de nuvem positivos e negativos (figura 41); e o apêndice E, que fornece uma visão geral sobre aspectos contratuais.

7. Panorama da contratação de computação em nuvem na APF

198. Este capítulo apresenta o cenário de adoção de computação em nuvem na Administração Pública Federal (APF), com exemplos de contratação encontrados através de pesquisas no Diário Oficial da União e junto a pessoas, organizações, órgãos e fornecedores relacionados ao tema. Além disso, apresenta também as iniciativas dos dois principais provedores públicos de serviços de TI, Serpro e Dataprev, para prover serviços de computação em nuvem para a APF.

199. Ressalte-se que a pesquisa concentrou-se no fornecimento de computação em nuvem no modelo "como serviço", ou seja, em contratos abrangendo nuvem pública (vide parágrafos 51 a 54). Se observarmos as iniciativas de nuvem privada, muitos órgãos encontram-se em algum estágio evolutivo para a adoção de infraestrutura de nuvem privada, pois no mínimo apresentam parque computacional virtualizado. A adoção de computação em nuvem pública apresentou iniciativas isoladas e que afetam somente parte dos serviços de TI prestados pela entidade.

200. De maneira geral, os gestores públicos não têm incluído em seu planejamento ações envolvendo computação em nuvem. Dentre as possíveis razões para isto, podem ser citadas a incerteza do impacto de certos dispositivos legais recentes, como o Decreto 8.135/2013, e a inexistência de uma forma consolidada de como tratar riscos relativos à segurança na nuvem. Um contraponto é que os dados críticos ou sigilosos teriam pouca representatividade face ao total do que pode ser migrado para a nuvem, e que se faz necessária análise mais profunda sobre a classificação da informação antes de se excluir a possibilidade de contratar serviços na nuvem.

7.1 Iniciativas de contratação de serviços de computação em nuvem na APF

201. Por meio de pesquisa documental em editais e contratos, bem como de reuniões realizadas com gestores, constatou-se que a adoção de computação em nuvem pública (como serviço) encontra-se muito incipiente. Observou-se, também, que instituições menores ou com restrições orçamentárias são mais propensas a migrar para uma nuvem pública. Os principais motivos são:

1) *facilidade de migração, por possuírem menor e menos complexa infraestrutura, com poucos ou nenhum sistema legado;*
2) *falta de pessoal técnico especializado suficiente para lidar com as demandas de TI;*
3) *restrições orçamentárias que dificultam ou limitam a atualização do parque computacional.*

202. Dada esta realidade, a nuvem apresenta um potencial de ganho em diversos requisitos, especialmente em disponibilidade e segurança, devido à existência de estruturas de contingência no provedor, e de que este tem mais condições de alcançar padrões internacionais de segurança que uma instituição pequena e com limitações orçamentárias significativas.

203. Destacam-se as iniciativas realizadas pelas seguintes instituições: Financiadora de Estudos e Projetos (Finep), Ministério das Comunicações, Infraero, além do Serviço Federal de Processamento de Dados (Serpro) e Empresa de Tecnologia e Informações da Previdência Social (Dataprev), esses últimos também atuando como provedores para o governo.

204. A partir do segundo semestre de 2014, percebe-se um movimento de contratação de serviços em nuvem comercializados pelo Serpro, especialmente o Expresso (solução de correio eletrônico comercializada como SaaS) e o serviço de IaaS. Este movimento explica-se em função do Decreto 8.135/2013. Para o Expresso, já são contratantes Ministério das Comunicações, Ministério do Planejamento e Superintendência de Administração do Ministério da Fazenda no Distrito Federal. Esta última também contratou IaaS do Serpro.

7.1.1 Finep – Infraestrutura como Serviço

*205. A Finep optou por um modelo de IaaS para a utilização do seu sistema de ERP, e lançou edital com objeto "Contratação de empresa para prestação de serviços continuados de Data Center, infraestrutura de **hardware** e **software**, através de **Cloud Computing**, na modalidade de distribuição NUVEM PRIVADA, incluindo os serviços de hospedagem, armazenamento, processamento e comunicação de dados, ponto-a-ponto, com os sistemas e aplicativos da Financiadora de Estudos e Projetos FINEP" (peça 51).*

*206. Foi escolhida esta opção porque, conforme argumentado por gestores da Finep em reunião com integrantes da equipe de fiscalização, os sistemas de ERP exigem muito da infraestrutura de TI, e a tecnologia de computação em nuvem permite não mobilizar ativos ou vários recursos de **hardware** para isso. Ademais, a lógica de partir para uma solução de serviços de nuvem possui o foco principal de diminuir os custos em curto e médio prazo após implantada a solução de ERP.*

207. Também considerou-se que a Finep prevê um crescimento gigantesco de orçamento e operações (de bilhões para dezenas de bilhões) e a elasticidade da nuvem se configura como parte da resposta da TI a esta demanda.

*208. Percebe-se que solução escolhida tem características de nuvem privada virtual, pois o acesso aos recursos é realizado através de **link** de comunicações dedicado. No entanto, apesar do faturamento ser por uso, existem degraus de uso. Há flexibilidade e revisão dos parâmetros de uso para mais ou menos mensalmente, ou seja, o pagamento não é por uso efetivo, necessitando haver ajustes prévios mensais. Para tanto, foram estabelecidos em edital limites máximo e mínimo mensal para os recursos computacionais, conforme figura abaixo:*

Tabela 3 - Finep – Limites mensais para os recursos computacionais na nuvem

SUBITEM AA			
Ambientes	**Elementos**	**Limite Mensal Mínimo**	**Limite Mensal Máximo**
Ambientes de: Produção, Homologação, Desenvolvimento e Monitoração	Memória	386 GB	972 GB
	Disco	6710 GB	13330 GB
	Núcleo de Processador	298 Núcleos de Processadores	744 Núcleos de Processadores
SUBITEM AB			
Ambientes	**Elementos**	**Limite Mensal Mínimo**	**Limite Mensal Máximo**
Comunicação de Dados entre a FINEP e o Data Center	Link Dedicado (Banda)	50 Mbps	100 Mbps

209. O provisionamento de orçamento foi feito considerando-se a capacidade máxima prevista inicialmente. Também não há sistema de auto provisionamento, ou seja, é necessário abrir chamado junto ao provedor.

*210. A partir desta primeira experiência, os gestores pretendem sempre avaliar nuvem como primeira opção para novas contratações. Para os sistemas legados, optou-se primeiro por licitar serviço de **collocation**, ou seja, priorizando a infraestrutura de um data center seguro. Após esta etapa, pretendem paulatinamente migrar as soluções para nuvem.*

211. Outro contrato firmado com características de nuvem, no modelo de SaaS, foi o serviço correio eletrônico (peça 52). Neste caso, o pagamento é feito por caixa postal. A criação, exclusão ou alteração de parâmetros é realizada por chamado. Neste caso, foi estabelecido requisito de ser provido fisicamente no Brasil, e o valor pago mensalmente por usuário é de R$ 11,67.

212. Segundo os gestores informaram em reunião do dia 25/11/2014, houve melhorias em comparação com a solução anterior como, por exemplo, aumento de mobilidade (acesso via celular), maior estabilidade e maior capacidade de armazenamento (de 10 MB para 25GB por caixa postal de usuário). O único ponto negativo relatado é que a Finep não possui mais autonomia para realizar determinadas intervenções, necessitando passar por todo um processo de abertura de chamados com contagem de prazos para seu atendimento.

7.1.2 Infraero – licenças de Microsoft Office em nuvem

*213. A Infraero recentemente contratou licenças de **software** Microsoft em nuvem, por meio do pregão eletrônico 61/DFLC/SEDE/2014, cujo objeto é a "contratação de empresa para fornecimento de licenciamento de software da Microsoft na modalidade EAS (**Enterprise Agreement Subscription**), incluindo os benefícios do **software** Assurance", pelo valor de R$ 10.999.910,47 (peça 53).*

214. Conforme informado por gestores da Infraero em reunião com integrantes da equipe de fiscalização, a empresa possui como um de seus objetivos estratégicos a adoção de computação em nuvem. Os argumentos utilizados para a adoção de computação em nuvem estão relacionados com o cenário restritivo atual da empresa (privatização de aeroportos): i) redução de pessoal, pois 35 analistas de TI deixaram a empresa recentemente e novas contratações estão suspensas; ii) encolhimento orçamentário, que torna o fator "custo" um argumento decisivo para a adoção de solução de nuvem. Com relação à questão orçamentária, foi destacado que 18 a 25% do valor de investimento em TI transforma-se em despesas de custeio ao final do contrato.

*215. Segundo os gestores, o licenciamento do Office 365 traz novos benefícios e tem custo similar ao licenciamento tradicional. Por fornecer armazenamento na nuvem, o uso do Office 365 ajuda a desonerar o uso de recursos de TI próprios da empresa (como **storage** e servidores), podendo direcioná-los da área administrativa para atividades da área finalística.*

216. No estudo técnico preliminar para a contratação do licenciamento de software da Microsoft (análise de viabilidade da contratação; peça 54, p. 10-11), a Infraero menciona os benefícios da computação em nuvem aplicados à sua realidade, dentre os quais destacam-se:

1) *Redução do custo operacional e dos custos de aquisição de infraestrutura haja visto que, nessa modalidade, a infraestrutura de armazenamento, servidores, sistema operacional e serviços ficam sob responsabilidade da contratada (operação, monitoramento, manutenção, atualização tecnológica, entre outros);*
2) *Aumento de disponibilidade dos serviços uma vez que a modalidade em questão possui uma infraestrutura de TI mais robusta distribuída em data centers espalhados por todo o mundo;*
3) *Essa modalidade permite utilização local ou na nuvem (cenário híbrido), dando à Infraero a possibilidade de realizar gestão do risco de sobrecarga dos links de comunicação;*
4) *Redução da utilização dos links WAN para localidades que possuem saída de **internet** por meio dos recursos de utilização do correio eletrônico (Outlook) e armazenamento (OneDrive) na nuvem;*
5) *Redução dos custos com diárias e passagens por meio da utilização plena dos recursos de videoconferência (Microsoft Lync);*
6) *Possibilidade de aumento da eficiência mediante a utilização de ferramentas colaborativas (Office 365, Sharepoint, Yammer etc.);*
7) *Redução no custo de licenciamento da suíte de escritório (Microsoft Office), uma vez que cada usuário pode utilizar uma licença do produto em até 5 dispositivos. Por exemplo, se um mesmo usuário possui um **desktop**, um notebook e um **tablet**, no modelo de licenciamento convencional precisará de 3 licenças do Microsoft Office. Na modalidade de licenciamento na nuvem, precisará de apenas 1 (uma) licença.*

217. Entretanto, não foi objetivo deste levantamento efetuar avaliação crítica sobre os benefícios indicados pela Infraero nessa contratação.

218. Os gestores informaram ainda que o contrato foi assinado recentemente e que a empresa ainda não está armazenando documentos na nuvem do Office 365. O uso do OneDrive está sendo avaliado, mas considera-se que será utilizado apenas para documentos corporativos administrativos, mantendo-se os dados finalísticos nos CPDs próprios da Infraero.

7.1.3 Ministério das Comunicações – Expresso

219. O Ministério das Comunicações foi o primeiro a adotar o Expresso, serviço de correio eletrônico comercializado como SaaS pelo Serpro, após a publicação do Decreto 8.135/2013. Em abril de 2014, foram contratadas 1.900 caixas de correio eletrônico com capacidade de 500 MB cada, ao custo de R$ 3,43 por mês/caixa postal, em abril de 2014 (Contrato 7/2014-MC; peça 55).

220. O pagamento do Expresso é mensal e varia conforme o uso, considerando as caixas postais ativadas, com utilização fixa mínima de 500 MB por caixa ativada e cobrança do que exceder essa utilização, e também a quantidade de certificados digitais emitidos. De acordo com estabelecido em contrato, são emitidos relatórios de demonstrativo para cada um dos itens, com a finalidade de controle por parte do gestor.

221. Com a migração do Exchange 2003 para o Expresso, houve um ganho de disponibilidade e de segurança devido à maior infraestrutura e quantidade de recursos humanos especializados do Serpro, quando comparada com a existente no Ministério.

222. Apesar de ser uma solução de SaaS, não há auto-provisionamento. Toda criação, alteração, exclusão e manutenção é feita através de abertura de chamados.

223. O Ministério não migrou as caixas postais da plataforma antiga para o Expresso. Uma das questões a ser considerada nas contratações de serviços de nuvem é de quem seria a responsabilidade pela migração entre sistema antigo e novo provedor, nas transições contratuais.

7.1.4 Ministério da Comunicações – Cidades Digitais

224. O programa Cidades Digitais foi criado em 2011, e consiste em um conjunto de iniciativas em diferentes áreas e relacionadas entre si, a saber: construção de uma rede de fibras ópticas para conectar órgãos públicos dos municípios; disponibilização de aplicativos e serviços para modernizar a gestão e o acesso a serviços; e capacitação de servidores públicos (peça 56).

225. Para disponibilizar aplicativos de gestão pública municipal, o Ministério das Comunicações firmou contrato com o Serpro (Contrato 17/2014-MC; peça 57), cujo objeto é a prestação de "serviços na área de tecnologia da informação para a hospedagem em nuvem de soluções de gestão municipal (Governo Eletrônico) para atendimento ao Projeto Cidades Digitais do Ministério das Comunicações para o acesso de 80 (oitenta) prefeituras escolhidas pelo programa", incluindo: "a) Hospedagem e Produção de Nuvem"; "b) Desenvolvimento de Portal"; e "c) Consultoria Técnica". O valor anual máximo estimado é de R$ 14.344.331,71 para o período de 12 meses.

226. Tratam-se de seis aplicativos que estão no portal desenvolvido e hospedado pelo Serpro. Por meio destes aplicativos, os moradores das cidades contempladas podem acessar serviços, o município pode fazer a gestão de recursos e pessoal, e publicar informações em cumprimento à Lei de Acesso à Informação.

227. Para os serviços de hospedagem e produção em nuvem, o pagamento é mensal, calculado em função da quantidade total de municípios com acesso no mês e a quantidade de sistemas utilizados por esses municípios. O preço da cota básica fixado na proposta, por sistema e por cada grupo de 10.000 habitantes, é de R$ 421,02.

7.2 Iniciativas da Dataprev

228. Por meio do Ofício PR/485/2014, de 14/11/2014 (peça 29), a Dataprev elenca, na definição de computação em nuvem que adota, potenciais benefícios da contratação pela APF desse tipo de serviço: diminuição da "necessidade de expertise técnica local, investimento em infraestrutura física entre outros custos relacionados" (peça 29, p. 2).

229. A empresa destaca como obstáculos para promover maior utilização do modelo de computação em nuvem "a compreensão dos clientes sobre os conceitos, limites e responsabilidades" desse modelo (peça 29, p. 2).

230. O Plano de ação 2014 da Dataprev (peça 47) possui três elementos relacionados à computação em nuvem, na seguinte situação:

1) *"3.12. Arquitetura de referência em nuvem implantada em Ambiente de produção para Infraestrutura como Serviço (IaaS)" (peça 47, p. 6). "Este resultado está com 89% de conclusão, sendo executado atualmente ações relacionadas à implantação do monitoramento, padronização de bilhetagem, atualização do catálogo" (peça 29, p. 3);*
2) *"3.16. Novo modelo de aplicação de referência e **framework** suportando arquitetura em nuvem" (peça 47, p. 6). "Este resultado está com 87% de conclusão, sendo executado atualmente ações relacionadas à adaptação da aplicação de referência para replicação de sessão" (peça 29, p. 3);*
3) *"4.59. Serviço de nuvem comercializado para pelo menos 1 cliente" (peça 47, p. 10). "Após avaliação da viabilidade do resultado, o mesmo passou a ter nova redação -*

Serviço de nuvem definido para comercialização. Dessa forma, o resultado prevê a conclusão da definição dos processos que ainda não foram completamente detalhados, com vistas a possibilitar o oferecimento e comercialização do serviço de nuvem para o próximo ano, com todos requisitos que garantam a sua qualidade" (peça 29, p. 3).

231. Desse modo, os serviços de computação em nuvem ainda não são oferecidos pela Dataprev (peça 29, p. 3). Já no papel de cliente, a empresa possui contratos recentes com empresas privadas de diferentes tipos de serviços de computação em nuvem, conforme quadro fornecido pela própria empresa (peça 29, p. 3-4):

Processo	Contrato	Objeto	Prazo	Fornecedor	Valor
44101.000033.2013.10	01.016457.2013	Contratação de Serviço de Rede Social - Serviço em Ambiente "Nuvem"	25/06/2013 a 24/10/2015	TOTVS S.A	1.295.000,00
44101.000106.2014.54	01.018960.2014	Contratação de Solução de Gestão de Pessoas em Ambiente "Nuvem"	24/10/2014 a 23/10/2019	MAIS2X TECNOLOGIA EM DOBRO LTDA	17.799.983,51
44101.000267.2013-67	01.018416.2014	Solução de Gerenciamento de Processos Jurídicos em Ambiente "Nuvem"	26/06/2014 a 25/10/2016	E-XYON TECNOLOGIA E INFORMACAO LTDA	415.060,00
44101.000084/2014-22	01.019093.2014	Contratação de Solução de Auditoria em Ambiente "Nuvem"	28 MESES A PARTIR DA ASSINATURA DO CONTRATO (*)	WJ TECNOLOGIA LTDA	363.900,00

Figura 3 - Contratos de serviços de computação em nuvem da Dataprev

7.3 Iniciativas do Serpro

232. Conforme informado por meio do Ofício COGTI/CIPOA/CIPD - 039774/2014, de 16/12/2014 (peça 43), o Serpro passou a comercializar em 2014 serviços de computação em nuvem na modalidade de IaaS, a partir de seu centro de processamento de dados localizado no Rio de Janeiro, contando naquele momento com cinco servidores físicos (peça 43, p. 14-15).

233. De acordo o Serpro, "a nova modalidade de serviço pode indicar uma saída para um antigo problema no governo, onde é comum as instituições públicas terem aplicações armazenadas localmente, em equipamentos e ambientes que não tenham condições ideais para a atividade" (peça 43, p. 3).

234. A empresa apontou algumas vantagens na adoção da nuvem, sendo que uma vantagem determinante "é a redução de custos, já que se paga apenas pelo recurso de TI que é necessário" (peça 43, p. 3).

235. Um portal web de autosserviço permitirá ao cliente alocar para si mesmo recursos computacionais, na forma de instâncias de máquinas virtuais pré-definidas em função da capacidade necessária para atender sua demanda, sem intervenção do suporte técnico do Serpro (peça 43, p. 3-4).

236. Os serviços de IaaS são oferecidos como um Centro de Dados Virtual, que abstrai os componentes de processamento, armazenamento e rede de um CPD tradicional, permitindo o auto provisionamento automático desses recursos em função da demanda (peça 43, p. 5-7). OpenStack é o nome da solução de código aberto utilizada para orquestração e gerenciamento das máquinas virtuais desse Centro de Dados Virtual (peça 43, p. 3-4).

*237. Dentre os serviços de segurança a serem disponibilizados adicionalmente à solução de IaaS, a empresa destaca a segurança de perímetro, proteção contra ataques de negação de serviço distribuídos, sistema de prevenção e detecção de intrusão (IPS/IDS), **firewall** e consultoria de análise de vulnerabilidades e testes de segurança (peça 43, p. 4-5).*

*238. O Serpro oferece também serviços de computação em nuvem na modalidade SaaS. O primeiro cliente dessa modalidade é o Ministério das Comunicações com o programa Cidades Digitais (seção 7.1.4), que está disponibilizando por meio da nuvem do Serpro **softwares** das áreas de gestão, educação e saúde para cerca de oitenta municípios (peça 43, p. 5). Cita-se também o serviço de correio eletrônico Expresso, que tem como expressivo cliente também o Ministério das Comunicações (seção 7.1.3).*

239. O Serpro emprega, para o provisionamento de seus serviços de nuvem, as mesmas políticas gerais da empresa para análise de risco, gestão de continuidade, tratamento de incidentes e recuperação de desastres (peça 43, p. 16). Assim, a infraestrutura oferecida aos clientes como serviço teria as mesmas garantias e expectativas de desempenho da infraestrutura própria do Serpro.

240. Destaca-se a norma Segurança da Computação em Nuvem (peça 58), publicada em 8/12/2014, que foi elaborada com base na Norma Complementar 14/IN01/DSIC/GSIPR e nas melhores práticas

recomendadas pela CSA (peça 43, p. 21-22), estabelecendo "os controles de segurança a serem implementados no provisionamento de recursos em nuvens públicas e privadas fornecidos pelo Serpro". A norma traz determinações quanto às responsabilidades do cliente e do Serpro com relação a: governança, gestão de riscos e conformidade; continuidade de negócios; controles e requisitos de segurança; administração e gerenciamento da nuvem; e tratamento de incidentes.

241. Operações de backup realizadas pelo próprio Serpro servem exclusivamente para garantir a recuperação de sua infraestrutura de provisionamento de máquinas virtuais para os clientes, os quais não podem utilizá-las para recuperação de dados perdidos em casos de falhas de uso. Desse modo, os clientes devem realizar backups próprios para os seus dados (peça 43, p. 24-25).

7.4 Análise da oferta de serviços de nuvem pelas empresas públicas

242. A Dataprev ainda não oferece serviços de computação em nuvem (peça 29, p. 3), e também ainda não definiu política de preços, níveis de serviço e nem elaborou modelo de contrato padrão. No entanto, a empresa afirmou que já está construindo capacidade própria para oferecer tais serviços, pelo menos na modalidade IaaS, com previsão de comercializá-los em 2015.

243. Passa-se, então, a analisar a oferta de serviços por parte do Serpro.

244. Quanto às informações a respeito de sua estratégia relacionada à nuvem (peça 43, p. 2), o Serpro não abordou aspectos como: expectativas de crescimento das demandas de seus clientes, alocação interna dos recursos necessários para prover a demanda, previsão de investimentos em capacidade computacional, pesquisa e desenvolvimento, ou ainda posicionamento de mercado da oferta da empresa frente à concorrência da iniciativa privada.

245. A fronteira que delimita as responsabilidades do fornecedor de serviços e as do cliente não se encontra plenamente definida. Por exemplo, na área de segurança, o Serpro comercializa diversos serviços para garantir confidencialidade, disponibilidade e integridade de sua infraestrutura, mas, ao mesmo tempo, reconhece que o cliente de IaaS deve estar ciente, "pelas definições estabelecidas em contrato, que a segurança de ativos por ele provisionados como serviço na nuvem são de sua responsabilidade" (peça 43, p. 6).

246. Não há definição prévia de níveis de serviço, os quais são estabelecidos somente nos contratos com os clientes (peça 43, p. 6). O modelo de contrato padrão para serviços de nuvem ainda não se encontrava concluído (peça 43, p. 8).

247. Não há definição quanto aos valores praticados para os serviços de migração de dados ou entrada e saída do ambiente de nuvem. O Serpro respondeu que "a incorporação de novos serviços será avaliada caso a caso, decorrente de suas características de produção e níveis de serviços e os custos correspondentes serão avaliados conforme a formatação da demanda" (peça 43, p. 8). Os custos e condições de saída de um serviço de nuvem devem estar claros e são essenciais para a decisão de adoção do serviço e seleção do fornecedor.

248. Há indefinição quanto aos custos dos serviços. O Serpro afirma que "a incorporação de novos serviços será avaliada caso a caso", considerando capacidade computacional, processamento, memória, espaço de disco, velocidade de comunicação e características do SLA demandado (peça 43, p. 7-8). Porém, não é fornecida uma tabela de preços individuais de cada componente para permitir a formulação de solução mais adequada às necessidades do órgão em função dos preços cobrados.

249. Não há previsão de auditoria externa periódica contratada pelo Serpro para fornecer garantias aos seus clientes de serviços de nuvem, mas também não haveria impedimento a que tal auditoria seja contratada pelo cliente (peça 43, p. 12-13).

250. O Serpro não provê soluções de criptografia para seus clientes, mas a empresa informou que está prospectando soluções no mercado (peça 43, P. 15-16).

251. Maior tolerância a falhas e capacidade de recuperação são dois motivos que levam organizações a contratar serviços de computação em nuvem. No entanto, a concentração dos servidores físicos que proveem os serviços de nuvem em único data center do Rio de Janeiro (peça 43, p. 14), sem redundância em outra localidade, incorre em riscos sistêmicos como catástrofes climáticas, interrupção no fornecimento de energia ou ruptura em cabos de fibra ótica, dificultando a recuperação de desastres e retorno de funcionamento dos serviços.

252. Prevê-se o pagamento por capacidade alocada ao cliente, e não por capacidade efetivamente utilizada (peça 43, p. 7-8). Assim, com a variabilidade da carga computacional a cada instante, o cliente do Serpro precisa prever a capacidade necessária para atender aos picos de demanda, solicitar

e pagar pela capacidade correspondente. Serviços em nuvem costumam prever alocação dinâmica, automática e em tempo real dos recursos necessários, avaliados continuamente em função da demanda por esses serviços, sendo o pagamento final apenas pelo uso efetivo dos recursos, e não por sua mera disponibilidade.

253. A iniciativa de computação em nuvem do Serpro é relativamente recente, ainda envolve recursos e funcionalidades limitados, típicas de projetos de implantação de novas tecnologias em suas fases iniciais. Assim, a capacidade atual da solução de nuvem do Serpro pode ser considerada adequada aos poucos contratos específicos de nuvem, atualmente vigentes.

254. Ressalva-se que a análise detalhada da arquitetura ou topologia da infraestrutura de TI que suporta os serviços de computação em nuvem oferecidos pelo Serpro, com a finalidade de compará-las a seus equivalentes em serviços da iniciativa privada, requereria auditoria específica e, portanto, encontra-se fora do escopo do presente levantamento.

255. Diante da situação atual da oferta de serviços de computação em nuvem por estas empresas, a interpretação mais restritiva do Decreto 8.135/2013 – de que a APF deveria contratar exclusivamente as empresas públicas de TI para serviços de computação em nuvem – pode levar, pelo menos a médio ou curto prazo, ao não aproveitamento de oportunidades geradas por essa nova tecnologia, como entrega mais rápida de soluções de governo eletrônico para a população, redução de custos e realocação de recursos humanos hoje bloqueados na sustentação de sistemas e de infraestrutura de TI para inovação e desenvolvimento de novos serviços.

256. Desse modo, afigura-se como oportunidade de trabalho futuro a avaliação da oferta de serviços por parte de empresas públicas de TI como Serpro e Dataprev, tanto no aspecto de segurança da informação frente aos requisitos da Portaria Interministerial 141/2014 como em relação à capacidade da empresa de prover satisfatoriamente os serviços de computação em nuvem, tendo como parâmetro o ofertado pelo mercado privado nos aspectos de custo e qualidade.

8. Principais riscos e controles para contratação de serviços de computação em nuvem

257. Conforme já descrito, verifica-se que é possível obter vantagem competitiva ou econômica por meio da adoção de computação em nuvem. Não obstante, não é possível alcançá-las sem antes considerar riscos associados, seu alinhamento com os objetivos de negócio e com todos as partes envolvidas no processo.

258. Muito se polemiza acerca dos riscos de adoção de computação em nuvem pela administração pública, principalmente no tocante à segurança da informação. Porém, já é realidade a adoção extraoficial de serviços na nuvem pelos seus funcionários, muitas vezes sem o conhecimento da área de TI e sem controles adequados, devido à facilidade de acesso à internet e ampla difusão de uma grande variedade de serviços na nuvem. Esse problema é comum a todas as organizações, em maior ou menor grau, e já é conhecido por TI invisível (Shadow IT): são tecnologias ou serviços adquiridos pelos próprios usuários finais para fins corporativos, sem conhecimento da área de TI, e que normalmente são serviços na nuvem.

*259. Mesmo considerando que vários desses serviços possuem uso legítimo para o negócio, muitos não são homologados para uso corporativo, e portanto podem inserir riscos à organização, como o vazamento de dados sensíveis. Invasores estão utilizando cada vez mais serviços de computação em nuvem voltados ao consumidor doméstico, como vetor para promover vazamento de informações corporativas. Por exemplo, o relatório intitulado **Cloud Adoption & Risk Report** da empresa Skyhighnetworks cita dois casos de vazamento de informações através de serviços de nuvem não gerenciados: no primeiro, um **malware** vazava dados via uma conta privada do Twitter, o qual possui um limite máximo de apenas 140 caracteres por mensagem; no segundo, informações sensíveis eram codificadas dentro de arquivos de vídeo e posteriormente transmitidas a sites de compartilhamento de vídeo, a partir dos quais poderiam ser facilmente recuperadas.*

260. Para mitigar esses riscos, as organizações precisam prover novas opções de acesso móvel e seguro a seus recursos, que supram as necessidades de ferramentas hoje fornecidas pela computação em nuvem voltadas ao usuário doméstico. Tais alternativas podem, muito bem, ser serviços corporativos de nuvem pública, homologados depois de passar por processo de avaliação de riscos. Ou seja, a agilidade trazida pela computação em nuvem pode ser uma aliada para prover tempestivamente novas soluções como alternativa ao uso de ferramentas particulares não homologadas.

261. Também é importante frisar que a computação em nuvem, apesar de introduzir certos riscos, como os derivados da terceirização e do compartilhamento de recursos, mitiga uma série de outros tão comuns à tecnologia da informação, como a falta de capacidade de expansão e a demora na implantação de ambientes ou sistemas. Um dos riscos mitigados pela nuvem, devido à sua natureza elástica (parágrafo 30), é o de superdimensionamento ou subdimensionamento de recursos de TI. Essa característica permite otimização de recursos e representa grande vantagem em termos de resiliência como, por exemplo, durante ataques de negação de negação de serviço em larga escala, quando recursos de TI precisam ser expandidos rapidamente de maneira defensiva.

262. 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.

263. Qualquer organização está suscetível, em maior ou menor grau, a riscos específicos decorrentes da utilização da computação em nuvem. Um dos problemas para a mitigação de riscos pode ser o espaço limitado para negociação dentro dos contratos de adesão oferecidos para os serviços de computação em nuvem, que são na sua maioria genéricos. Isso deve-se ao próprio modelo de negócios de computação em nuvem, onde entrega-se serviços com custo competitivo e altamente dinâmicos baseando-se na economia de escala da prestação de serviços dentro de um padrão, como se fossem um produto, sem customizações. Quanto maior o grau de customização, maior a dificuldade em se negociar com o provedor e se conseguir valores mais competitivos no mercado, já que isto distorce a ideia de serviço em nuvem. A flexibilidade de negociação sem aumento de custo vai depender, essencialmente, da concorrência de mercado e do valor do contrato.

264. Neste sentido, é fundamental a realização de pesquisa prévia de mercado a fim de identificar se existe diversidade de provedores adequada ao perfil de risco associado à organização. Obviamente, um trabalho de levantamento e análise de riscos deve ser executado para subsidiar a decisão de migrar para a nuvem e moldar previamente o processo de contratação. Cada organização deve avaliar a criticidade de cada risco levantado de acordo com sua realidade, bem como se seus controles associados são, um a um, aplicáveis, ou se podem ser individualmente desconsiderados em função da análise de seu custo/benefício.

265. Ademais, antes de considerar o uso de computação em nuvem, deve-se avaliar possíveis riscos decorrentes de sua adoção. Para isto, a análise de riscos do uso de serviços de computação em nuvem deve entender a importância, sensibilidade, e valor da informação que será processada e armazenada naquele serviço. Pode-se, também, iniciar a utilização de computação em nuvem com dados e aplicações não críticas e públicas, com baixo risco de segurança da informação.

8.1 Estruturação dos riscos identificados e da matriz de auditoria de serviços de computação em nuvem

*266. Com a finalidade de facilitar a utilização tanto pelo gestor como pelo auditor, foi estruturada uma tabela (Anexo I) contendo possíveis controles associados aos riscos identificados, bem como referências de critérios (normas e boas práticas). Foram levantados riscos específicos da adoção e da contratação de computação em nuvem, não sendo finalidade deste trabalho abordar riscos gerais como os aplicáveis a qualquer contratação de TI, ou que abordam serviços de TI em geral, como os regulamentados pela Instrução Normativa SLTI/MP 4/2014. O levantamento baseou-se, portanto, em normas e padrões internacionais, como descrito nos documentos **Cloud Controls Matrix** (CCM), elaborado pela CSA; **Cloud Computing Security Risk Assessment**, elaborado pela ENISA; e Cobit 5 do ISACA; e normativos brasileiros específicos à Administração Pública Federal (normas complementares do DSIC/GSI/PR, Decreto 8.135/2013 e Portaria Interministerial 141/2014).*

267. Além do mais, no decorrer deste trabalho, observou-se que computação em nuvem pode referir-se a diferentes modelos arquiteturais, incluindo SaaS, PaaS e IaaS. Ainda que os riscos, controles e

vantagens associados a cada modelo possam ser diferentes, buscou-se aqui elencar os principais riscos, comuns a qualquer um dos modelos, dentro do foco dos serviços de computação em nuvem pública.

268. Os controles elencados na tabela do Anexo I podem ser seguidos um a um, ou de acordo com o agrupamento feito por categorias de risco. Tais categorias, por sua vez, também são agrupadas em quatro temas: "segurança da informação", "governança e gestão de riscos", "contratação e gestão contratual", e "infraestrutura de TI". Abaixo estão relacionados os 43 riscos identificados durante o trabalho de levantamento, agrupados por temas e categorias de risco:

Tabela 4 - Riscos de contratação de serviços de computação em nuvem

Tema: Segurança da informação
Categoria de risco: Indisponibilidade do serviço
1 - Não implementação de controles e salvaguardas suficientes para garantir a continuidade da infraestrutura do provedor, afetando assim a disponibilidade do serviço para o usuário final
2 - Indisponibilidade de elementos da infraestrutura do cliente que são críticos para o acesso a serviços na nuvem
Categoria de risco: Confidencialidade e integridade de dados
3 - Controle de acesso inexistente ou insuficiente para assegurar a confidencialidade dos dados armazenados na nuvem
4 - A segurança dos dados transmitidos para o provedor de nuvem pela internet pode ser comprometida durante a transferência
5 - Acesso indevido do provedor aos dados
6 - O provedor pode ser forçado legalmente a fornecer dados por estar submetido a jurisdição estrangeira, colocando em risco a privacidade e a disponibilidade das informações
7 - Um cliente pode ter acesso indevido a dados de outro cliente
8 - Acesso indevido à medida que os serviços de computação em nuvem são amplamente acessíveis, independentemente de localização
Categoria de risco: Gestão de mudanças
9 - A gestão de mudanças do provedor de computação em nuvem pode não ser adequada às necessidades do cliente. Por exemplo, mudanças na infraestrutura de software do provedor (patch corretivo, atualização de versão etc) podem não passar por processos de gestão de mudanças individuais dos clientes, causando impactos negativos (risco agravado em caso de SaaS)
Categoria de risco: Trilhas de auditoria
10 - A política do provedor para liberar os logs de acesso, de sistema e de segurança não atende aos requisitos do cliente; há perda ou fornecimento incompleto de informações do provedor para o cliente relativas a incidentes de segurança e ao fornecimento de trilhas de auditoria
11 - Logs possuem período de retenção no provedor menor que o esperado e estabelecido nas políticas internas do cliente
12 - Ausência de isolamento de logs entre vários clientes; vazamento de dados de log
Categoria de risco: Segurança de interfaces de programação (APIs)
13 - As APIs para acesso à infraestrutura do provedor e aos dados do cliente possuem falhas ou vulnerabilidades
Categoria de risco: Acesso indevido por invasor interno
14 - As políticas e orientações do provedor de nuvem quanto ao acesso de seus funcionários aos ativos físicos e virtuais podem não ser adequadas ou de conhecimento do cliente
15 - As políticas e orientações do provedor quanto a contratação de pessoal, monitoramento de atividades de seus funcionários e verificação do cumprimento das normas organizacionais podem não ser adequadas ou de conhecimento do cliente
Categoria de risco: Atualizações e correções de segurança
16 - Exploração de vulnerabilidades do provedor podem impactar operações do cliente

Tema: Governança e gestão de riscos
Categoria de risco: Planejamento

17 - Dimensionamento inadequado das vantagens e riscos relativos à incorporação de serviços de computação em nuvem em função das características e requisitos individuais da organização
18 - Planejamento orçamentário de TI não adequado às características de contratação de serviços de computação em nuvem
Categoria de risco: Política de recursos humanos
19 - Resistência da equipe de TI à adoção de computação em nuvem por receio de perder suas funções
Categoria de risco: Governança
20 - Perda de governança e controle da TI por parte da organização quando da utilização de serviços na nuvem
21 - Menor reatividade do fornecedor a comandos do cliente se comparado a provimento interno do serviço
22 - Falta de apoio interno devido à cultura organizacional e percepção do cliente de que há maiores riscos associados a serviços em nuvem
Categoria de risco: Legislação e normativos pertinentes
23 - Não observância de legislação e normativos específicos que regulam a contratação de serviços de computação em nuvem ou de pontos específicos em regulamentos de contratação de serviços de TI em geral
24 - Desconformidade com o Decreto 8.135/2013 e com a Portaria Interministerial 141/2014
25 - Não observância das normas de segurança do DSIC/GSI/PR

Tema: Contratação e gestão contratual
Categoria de risco: Gestão contratual
26 - Níveis de serviço estabelecidos em contrato podem não ser cumpridos
27 - Vulnerabilidades e problemas de segurança detectados no provedor demoram para ser corrigidos ou não são corrigidos
28 - Falhas no monitoramento e gestão contratuais
29 - Estouro de orçamento para o contrato devido à falta de controle sobre o uso dos recursos de computação em nuvem e estimativas imprecisas de custo
Categoria de risco: Dependência frente ao provedor
*30 - Dependência do cliente com relação ao provedor (vendor **lock-in**)*
31 - Dificuldades do cliente em migrar dados de um provedor para outro ou internalizá-los novamente, por problemas de interoperabilidade ou de portabilidade
32 - Falta de previsão dos custos de saída do provedor
33 - Indisponibilidade do fornecedor (ruptura contratual, falência, sequestro de dados)
Categoria de risco: Falhas contratuais
34 - Conflitos sobre a propriedade dos dados armazenados na nuvem
35 - Falta de delimitação legal regendo as relações contratuais, dado que os serviços de nuvem podem ser prestados globalmente
36 - Não exclusão de dados armazenados na nuvem ao término de um contrato

Tema: Infraestrutura de TI
Categoria de risco: Falhas relativas à infraestrutura de TI
37 - Falhas de isolamento entre ambientes ou instâncias virtuais de clientes diferentes
38 - O compartilhamento de recursos pelos provedores de nuvem entre vários clientes pode inserir vulnerabilidades adicionais
39 - As ferramentas e processos para gestão de incidentes do provedor podem ser incompatíveis com os utilizados pelo cliente
40 - O processo de gestão de incidentes do provedor apresenta falhas em documentação, resolução, escalonamento ou encerramento de incidentes
41 - Problemas de infraestrutura de rede do cliente podem afetar o desempenho dos serviços de computação em nuvem
42 - Problemas de dimensionamento de carga da infraestrutura do provedor podem afetar o desempenho dos serviços de computação em nuvem

43 - Incompatibilidade entre o modelo arquitetural do cliente e do provedor

269. No tocante a riscos inerentes à APF, foram abordados aspectos específicos e relevantes dos normativos brasileiros com forte ênfase em segurança da informação, como as normas do DSIC/GSI/PR, do Decreto 8.135/2013 e da Portaria Interministerial 141/2014.

270. Ademais, riscos identificados compreendem a restrição orçamentária à utilização de computação em nuvem, quando se trata do uso de verba de custeio para tal. Portanto, a fase de planejamento orçamentário do negócio deve englobar e garantir, para TI, verba adequada aos serviços de computação em nuvem. Ainda no tocante a orçamento, devem ser previstos controles para assegurar tetos de recursos máximos contratuais utilizáveis para o pagamento por uso, evitando assim estouro de orçamento e perda de controle sobre o contrato de computação em nuvem.

271. A partir da tabela de riscos e controles contida no Anexo I, derivou-se matriz de procedimentos de auditoria de computação em nuvem (Anexo II), detalhando procedimentos a serem executados pelo auditor, bem como possíveis achados associados. A matriz foi idealizada como referência para futuras auditorias de contratações de serviços em nuvem, com a ressalva de que ainda necessita ser avaliada em uma auditoria piloto, a fim de se evidenciar, na prática, se os procedimentos são adequados e completos. Observa-se que ela pode constituir o núcleo de uma matriz de auditoria que pode ser complementada com outros aspectos, como conformidades específicas de um sistema ou aspectos mais gerais (como contratação e terceirização de TI).

272. Espera-se que essa matriz, com seu nível de detalhamento de procedimentos, possa ser aplicada, em conjunto com os conceitos e informações apresentados neste relatório, por auditores com conhecimento de TI ainda que não especializados em computação em nuvem.

273. Por último, ressalva-se que a tabela de riscos e controles e a matriz de procedimentos de auditoria apresentadas estão em sua primeira versão, resultado de um trabalho que cobre riscos e possíveis controles identificados no período de outubro de 2014 a fevereiro de 2015 e, portanto, que reflete a realidade deste momento, necessitando de atualização passível da dinâmica e evolução da computação em nuvem.

9. Conclusão

274. O levantamento teve o objetivo de identificar riscos em contratações de serviços de TI sob o modelo de computação em nuvem pela APF. Para tanto, buscou-se aprofundar o conhecimento sobre o tema por meio de consultas a referências nacionais e internacionais, analisar as peculiaridades da legislação brasileira para contratações públicas e adaptar critérios de auditoria internacionais a requisitos específicos da APF.

275. Foram identificados diversos benefícios do uso de computação em nuvem (seção 2.5), como: redução de custos de infraestrutura e serviços TI devido a ganhos de escala; otimização da produtividade da equipe de TI, melhorando o suporte de operações de missão crítica; maior disponibilidade dos serviços de TI e consequente melhor produtividade do usuário final; resistência a ataques contra a disponibilidade dos serviços; redução do tempo para implementação de novos serviços e ciclo mais rápido de inovação.

276. No âmbito da Administração Pública Federal (APF), foram levantados, ainda, benefícios adicionais da adoção de computação em nuvem (seção 2.5.1), como: maior agilidade na entrega e na atualização tecnológica de serviços públicos; atendimento de demanda sazonal de serviços públicos pela Internet sem necessidade de alocar grande quantidade de recursos de TI fixos, que ficam subutilizados em momentos de pouco uso; ampliação do acesso e do uso de informações governamentais; e suporte mais ágil a iniciativas de Big Data e Dados Abertos.

277. Entretanto, as iniciativas de uso de serviços de computação em nuvem ainda constituem exceção no âmbito da APF. De maneira geral, os gestores ainda estão cautelosos, em especial por causa de preocupação com riscos relativos à segurança da informação, bem como de incerteza quanto a uma eventual interpretação mais restritiva do Decreto 8.135/2013, segundo a qual a APF deve contratar exclusivamente as empresas públicas de TI para serviços de computação em nuvem. Das empresas públicas que podem prestar esses serviços, a Dataprev (seção 7.2) ainda não iniciou a sua comercialização e a oferta do Serpro (seção 7.3) ainda é limitada, não apresentando todas as características elencadas neste relatório (seção 2.2).

278. Desse modo, um provável represamento de projetos dessa natureza, por limitações de capacidade das empresas públicas de TI, pode levar ao não aproveitamento de oportunidades geradas por essa nova tecnologia.

279. A computação em nuvem, apesar de introduzir certos riscos, como os derivados da terceirização e do compartilhamento de recursos, mitiga uma série de outros tão comuns à tecnologia da informação, como a falta de capacidade de expansão e a demora na implantação de ambientes ou sistemas. Há vários riscos relativos à segurança da informação que necessitam ser observados pelo gestor, mas há de se considerar também que as defesas baseadas em nuvem muitas vezes são mais robustas, escaláveis, eficientes e baratas se comparadas às soluções internas, em razão da especialização e do ganho de escala.

280. Um trabalho de levantamento e análise de riscos deve ser executado para subsidiar a decisão de migrar para a nuvem e moldar previamente o processo de contratação. A análise de riscos do uso de serviços de computação em nuvem deve entender a importância, sensibilidade e valor para a organização da informação que será processada e armazenada. De todo modo, pode-se iniciar com aplicações públicas e não críticas, com baixo risco de segurança da informação.

281. Por fim, como produtos deste trabalho, foram elaboradas tabela de riscos e possíveis controles associados à contratação de serviços de computação em nuvem pela APF (Anexo I) e matriz de referência contendo questões, procedimentos e possíveis achados de auditoria (Anexo II). Assim, pode-se considerar a matriz como ferramenta valiosa no auxílio aos auditores do TCU em fiscalizações de contratações de serviços dessa natureza. As informações obtidas e os riscos identificados neste levantamento podem subsidiar futuros trabalhos do TCU no campo da tecnologia da computação em nuvem, formato inovador no fornecimento de soluções e na prestação de serviços de TI.

10. Propostas de Encaminhamento

282. Diante do exposto, submetem-se os autos à consideração superior com as seguintes propostas:

a) encaminhar cópia da deliberação que vier a ser adotada, bem como do relatório, do voto, do relatório da unidade técnica e dos respectivos anexos que a fundamentarem:

i. à Controladoria-Geral da União (CGU);

ii. ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR);

iii. à Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (SLTI/MP);

iv. à Secretaria Executiva do Ministério da Ciência, Tecnologia e Inovação (SE/MCTI);

v. à Secretaria Executiva do Ministério das Comunicações (SE/MC);

vi. ao Serviço de Processamento de Dados do Governo Federal (Serpro);

vii. à Empresa de Tecnologia e Informações da Previdência Social (Dataprev);

viii. à Financiadora de Estudos e Projetos (Finep);

ix. à Empresa Brasileira de Infraestrutura Aeroportuária (Infraero);

x. ao Conselho Nacional de Justiça;

xi. ao Conselho Nacional do Ministério Público;

xii. à Diretoria-Geral da Câmara dos Deputados;

xiii. à Diretoria-Geral do Senado Federal;

xiv. à Secretaria Geral da Presidência do Tribunal de Contas da União (Segepres/TCU);

b) levantar o sigilo deste relatório, por conter informações relevantes às organizações públicas quanto ao tema Computação em Nuvem;

c) arquivar o presente processo, com fulcro no art. 169, inciso V, do Regimento Interno do TCU."

É o relatório.

VOTO

Cuida-se de relatório de fiscalização, modalidade levantamento, cujo objetivo foi "*identificar os riscos mais relevantes em contratações de serviços de Tecnologia da Informação (TI) sob o modelo de computação em nuvem, considerando os critérios da legislação brasileira, e elaborar modelo de matriz de procedimentos e de achados para futuras fiscalizações"*.

2. Buscando cumprir sua meta, a equipe da Secretaria de Fiscalização em Tecnologia da Informação (Sefit) elaborou matriz de planejamento por meio da qual evidenciou que os trabalhos deveriam fornecer respostas às seguintes questões de auditoria, *in verbis*:

a) O que é computação em nuvem, suas características e aplicações?
b) Quais são os modelos de comercialização de computação em nuvem?
c) Qual o quadro normativo aplicável a contratações de serviços de computação em nuvem pela Administração Pública Federal (APF)?
d) Qual o panorama atual da contratação de serviços de computação em nuvem pela APF?
e) Quais as principais vantagens, riscos e controles quando da contratação de serviços de computação em nuvem?

3. Conforme se depreende do minudente documento elaborado pela equipe de fiscalização, transcrito, na essência, no relatório que antecede este voto, as tarefas desenvolvidas incluíram pesquisas na *internet,* entrevistas, envios de questionários a diversos provedores de serviços (públicos e privados), requisições de informações e reuniões com gestores. Compreenderam, ainda, análises do Diário Oficial da União com vistas a serem identificados contratos celebrados pela administração pública federal.

4. Esse conjunto de ações permitiu que as questões de auditoria fossem adequadamente respondidas e também possibilitou que a unidade instrutiva apresentasse ao Tribunal, de modo bastante sistematizado, abrangente, diversas informações acerca do modelo computacional em questão, sendo expostos conceitos aplicáveis, características, vantagens, desvantagens e um panorama geral da computação em nuvem no âmbito da administração pública federal.

5. Nesse contexto, convém ressaltar que a computação em nuvem possui diversas definições, tendo a Sefit enfatizado aquele cunhado pelo *National Institute of Standards and Technology (NIST),* agência governamental não regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos, segundo o qual a "*computação em nuvem é um modelo que permite acesso ubíquo, conveniente e sob demanda, por intermédio da rede, a um conjunto compartilhado de recursos computacionais configuráveis [...] que podem ser rapidamente provisionados e disponibilizados com o mínimo de esforço de gerenciamento ou de interação com o provedor de serviços*".

6. As características desse modelo computacional, conforme também explicado pelo Nist, são o auto-provisionamento sob demanda, o acesso amplo pela rede mundial de computadores, o compartilhamento por intermédio de *pool* de recursos, a rápida elasticidade e a presença de serviços medidos por utilização.

7. Ressalta a unidade instrutiva que as vantagens da computação na nuvem "*decorrem essencialmente de benefícios de escala: ao consolidar centros de processamento de dados (CPDs) isolados em um pool de recursos computacionais compartilhados em nuvem, reúne-se um conjunto maior de recursos o que permite reduzir seus custos unitários, melhorar seu aproveitamento, balanceando as demandas por serviços de diversos clientes, o que otimiza o nível de uso dos recursos e divide os custos fixos em uma maior base de usuários*".

8. Especificamente quanto à administração pública, foram enfatizados os seguintes benefícios: (a) maior agilidade da administração na entrega de serviços e em sua atualização tecnológica; (b) suporte a iniciativas de *Big Data* e Dados Abertos, facilitando a abertura de informações governamentais que hoje se encontram em sistemas que controlam as operações cotidianas do Estado (c) atendimento a picos de demanda de serviços pela *internet* sem necessidade de alocar grande quantidade de recursos fixos; (d) a contratação de serviços em nuvem de IaaS ou PaaS pode levar a uma redução de oportunidades de desvios e irregularidades, quando comparada às múltiplas contratações de máquinas, licenças de *software*, manutenção e suporte necessárias para a operação de CPD próprio; (e) agilidade e economia na entrega de serviços para instituições públicas com unidades descentralizadas, que podem ter serviços disponibilizados por meio de acesso à *internet*.

9. No tocante às iniciativas adotadas pelo governo para fomentar a utilização da computação em nuvem em território nacional, os exames empreendidos evidenciam que estão em vigor três programas distintos os quais, contudo, ainda possuem baixo grau de execução.

10. Destes, é digno de nota o Programa TI Maior do Ministério da Ciência, Tecnologia e Inovação (MCTI), o qual é conceituado como um "*programa estratégico de software e serviços de tecnologia da informação*" e prevê investimentos da ordem de R$ 40 milhões em pesquisa, desenvolvimento e inovação em tecnologia de computação no período compreendido entre 2012 e 2015. Os outros dois programas identificados pela unidade instrutiva são o Datagov e o EGTCI 2014-2015.

11. Especificamente quanto à utilização da computação em nuvem no âmbito da administração pública federal, a averiguação promovida pela unidade instrutiva evidenciou que, por diversos motivos, tal opção não tem sido incluída no planejamento dos gestores dessa esfera governamental.

12. Nessa linha, foram constatadas incertezas inerentes ao quadro normativo aplicável a contratações de computação em nuvem e à inexistência de uma forma consolidada para se tratarem os riscos de segurança na nuvem, aspectos estes que contribuem sobremaneira para a pouca utilização de modalidade de computação em tela.

13. Com efeito, em relação ao citado quadro normativo, destacou-se o Marco Civil da *internet*, no qual são estabelecidos princípios, garantias, direitos e deveres para o uso da rede mundial de computadores no Brasil.

14. Além disso, foram evidenciados o Decreto 8.135, de 2013, e a Portaria interministerial 141/2014, competindo ao primeiro, o qual dispõe sobre as comunicações de dados da administração pública, estipular que *"as comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades da economia mista da União e suas subsidiárias*".

15. É de se ressaltar que no citado decreto há diversos comandos que, por um lado, visam fomentar empresas públicas que prestam serviços de tecnologia da informação e, por outro ângulo, com foco em resguardar informações sensíveis dos órgãos da administração pública federal, limitam o fornecimento de serviços de comunicação de dados às citadas empresas públicas, devendo estas empresas ofertar satisfatoriamente os serviços.

16. No tocante aos riscos, relacionados precipuamente, à segurança das informações e à disponibilidade dos serviços, destacou a unidade instrutiva que, muito embora seja possível obter

vantagem competitiva e/ou econômica por meio da adoção da computação em nuvem, devem ser adotadas ações com vistas a mitigá-los.

17. Nesse sentir, a Sefit, após pontuar, com acerto, que as defesas baseadas em nuvem tendem a ser mais robustas e eficientes em virtude do ganho de escala e da maior especialização das provedoras de serviços, deixou assente que "*um trabalho de levantamento e análise de riscos deve ser executado para subsidiar a decisão de migrar para a nuvem e moldar previamente o processo de contratação",* competindo a cada organização *"avaliar a criticidade de cada risco levantado de acordo com sua realidade, bem como se seus controles associados são, um a um, aplicáveis ou se podem ser individualmente desconsiderados em função da análise de seu custo/benefício".*

18. Como contribuição ao controle dos diversos riscos associados à migração e à utilização da computação em nuvem, elaborou a unidade instrutiva importante tabela, contida no anexo I de seu relatório, por meio da qual são enumerados diversos riscos específicos, devidamente categorizados, bem como são apresentados controles possíveis com base em critérios internacionalmente aceitos.

19. Derivado da referida tabela é outro importante produto do relatório de levantamento em apreço, pois foi elaborada matriz de procedimentos, idealizada como "*referência para futuras auditorias de contratações de serviços em nuvem",* a qual deverá ser avaliada e, talvez, aprimorada por intermédio de auditoria piloto versando sobre o tema, consoante reconheceu a própria unidade que a idealizou.

20. Dito isto, ressaltando a abrangência do exame empreendido pela unidade instrutiva e a possibilidade de os elementos coligidos fomentarem, de pronto, o controle dos riscos inerentes à computação em nuvem no âmbito da administração pública federal, deve prosperar a proposta de encaminhamento suscitada pela unidade instrutiva, no sentido de serem enviadas cópias dos trabalhos desenvolvidos, acompanhadas da presente deliberação, a diversos entes da administração pública federal.

Isso posto, voto por que o Tribunal adote o Acórdão que submeto à deliberação desse colegiado.

TCU, Sala das Sessões Ministro Luciano Brandão Alves de Souza, em 15 de julho de 2015.

BENJAMIN ZYMLER

Relator

1. Processo nº TC 025.994/2014-0.
2. Grupo I – Classe de Assunto: V - Relatório de Levantamento.
3. Interessados/Responsáveis: Empresa de Tecnologia e Informações da Previdência Social; Ministério das Comunicações (vinculador); Secretaria de Logística e Tecnologia da Informação - MP; Serviço Federal de Processamento de Dados
3.1. Interessado: Identidade preservada (art. 55, caput, da Lei n. 8.443/1992)
3.2. Responsável: Identidade preservada (art. 55, caput, da Lei n. 8.443/1992).
4. Órgãos/Entidades: Empresa de Tecnologia e Informações da Previdência Social; Ministério das Comunicações (vinculador); Secretaria de Logística e Tecnologia da Informação - MP; Serviço Federal de Processamento de Dados.
5. Relator: Ministro Benjamin Zymler.
6. Representante do Ministério Público: não atuou.
7. Unidade Técnica: Secretaria de Fiscalização de Tecnologia da Informação (SEFTI).
8. Advogado constituído nos autos: não há.

9. Acórdão:

VISTOS, relatados e discutidos estes autos de relatório de levantamento cujo objetivo foi identificar os riscos mais relevantes em contratações de serviços de Tecnologia da Informação (TI) sob o modelo de computação em nuvem,

ACORDAM os Ministros do Tribunal de Contas da União, reunidos em sessão do Plenário, em:

9.1.dar ciência deste Acórdão, acompanhado do relatório e do voto que o fundamentam, bem como do relatório de levantamento elaborado pela unidade instrutiva e dos seus respectivos anexos, à Controladoria-Geral da União (CGU); ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR); à Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (SLTI/MP); à Secretaria Executiva do Ministério da Ciência, Tecnologia e Inovação (SE/MCTI); à Secretaria Executiva do Ministério das Comunicações (SE/MC); ao Serviço de Processamento de Dados do Governo Federal (Serpro); à Empresa de Tecnologia e Informações da Previdência Social (Dataprev); à Financiadora de Estudos e Projetos (Finep); à Empresa Brasileira de Infraestrutura Aeroportuária (Infraero); ao Conselho Nacional de Justiça; ao Conselho Nacional do Ministério Público; à Diretoria-Geral da Câmara dos Deputados; à Diretoria-Geral do Senado Federal; e à Secretaria Geral da Presidência do Tribunal de Contas da União (Segepres/TCU);

9.2.levantar o sigilo deste processo, por conter informações relevantes para as organizações públicas; e

9.3.arquivar o presente processo, com fulcro no art. 169, inciso V, do Regimento Interno do TCU.

10. Ata n° 24/2015 – Plenário.
11. Data da Sessão: 15/7/2015 – Extraordinária de Caráter Reservado.
12. Código eletrônico para localização na página do TCU na Internet: AC-1739-24/15-P.
13. Especificação do quorum:
13.1. Ministros presentes: Aroldo Cedraz (Presidente), Benjamin Zymler (Relator), Raimundo Carreiro, José Múcio Monteiro, Bruno Dantas e Vital do Rêgo.
13.2. Ministros-Substitutos convocados: Augusto Sherman Cavalcanti, Marcos Bemquerer Costa e André Luís de Carvalho.
13.3. Ministro-Substituto presente: Weder de Oliveira.

(Assinado Eletronicamente)
AROLDO CEDRAZ
Presidente

(Assinado Eletronicamente)
BENJAMIN ZYMLER
Relator

Fui presente:

(Assinado Eletronicamente)
LUCAS ROCHA FURTADO
Procurador-Geral, em exercício