SENADO FEDERAL

Instituto Legislativo Brasileiro – ILB

Rubens Vasconcellos Terra Neto

Desafios da contratação de serviços em nuvem no setor público:

critérios para a contratação no Senado Federal

Brasília

2019

Rubens Vasconcellos Terra Neto

Desafios da contratação de serviços em nuvem no setor público:

critérios para a contratação no Senado Federal

Monografia apresentada ao Instituto Legislativo Brasileiro - ILB como pré-requisito para a obtenção de certificado de conclusão de Curso de Pós-Graduação *Lato Sensu* em Tecnologia da Informação Aplicada ao Poder Legislativo.

Orientador: Prof. Me. Pabblo Cardelino Ghobad

Coorientador: Prof. Esp. Pedro Enéas Guimarães Coelho Mascarenhas

Brasília

2019

Terra Neto, Rubens Vasconcellos.
Desafios da contratação de serviços em nuvem no setor público : critérios para a contratação no Senado Federal / Rubens Vasconcellos Terra Neto. – 2019.
182p. : il.

Orientador: Pabblo Cardelino Ghobad.
Coorientador: Pedro Éneas Guimarães Coelho Mascarenhas.

Trabalho de conclusão de curso (especialização) – Curso de Pós-Graduação *Lato Sensu* em Tecnologia da Informação Aplicada ao Poder Legislativo – Instituto Legislativo Brasileiro, 2019.

1. Computação em nuvem, contratação. 2. Setor público, contratação. 3. Brasil. Congresso Nacional. Senado Federal. I. Título.

CDD 004.6782

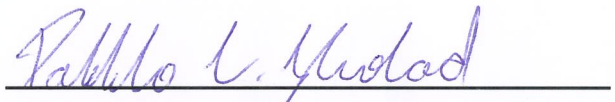
Rubens Vasconcellos Terra Neto

Desafios da contratação de serviços em nuvem no setor público: critérios para a contratação no Senado Federal

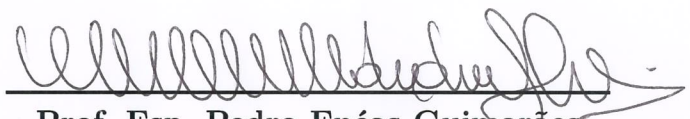
Monografia apresentada ao Instituto Legislativo Brasileiro - ILB como pré-requisito para a obtenção de certificado de conclusão de Curso de Pós-Graduação *Lato Sensu* em Tecnologia da Informação Aplicada ao Poder Legislativo.

Aprovada em Brasília, 30 de agosto de 2019 por:

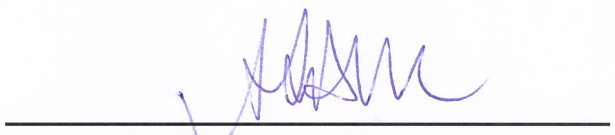
Banca Examinadora



Prof. Me. Pabblo Cardelino Ghobad



Prof. Esp. Pedro Enéas Guimarães Coelho Mascarenhas



Prof. Me. André Luiz Bandeira Molina

Dedico este trabalho à minha família, que sempre me incentivou.

Agradecimentos

Agradeço ao meu orientador Prof. Me. Pabblo Cardelino Ghobad e ao meu coorientador Prof. Esp. Pedro Enéas Guimarães Coelho Mascarenhas, pela sabedoria com que me guiaram nesta trajetória.

Aos meus colegas de sala, que dividiram comigo a busca constante de conhecimento e aprimoramento profissional, em especial ao colega Rogério Wagner Lage Guimarães Mendes, que colaborou em diversos trabalhos de inúmeras disciplinas durante o curso.

Aos professores do curso cuja dedicação foi fator preponderante para a qualidade do curso. Em especial, agradeço a professora Telma América Venturelli, que com seu entusiasmo e profissionalismo ajudou a estruturar este trabalho e ao professor Lauro César Araújo que tantas vezes me auxiliou no decorrer do curso.

A Secretaria do Curso, pela cooperação e ao Coordenador-Geral do curso Yuri Morais Bezerra que tanto se dedicou por nós do corpo discente.

Aos servidor do Senado Federal Eduardo Ferraz dos Santos por ter partilhado seu conhecimento e experiência no desenvolvimento deste trabalho.

Pela iniciativa e empenho na viabilização deste curso de especialização agradeço ao Diretor do Prodasen Alessandro Pereira de Albuquerque e ao seu adjunto à época do início do projeto Fabrício Fernandes Santana.

Gostaria de deixar registrado também, o meu reconhecimento à minha família, pois acredito que sem o apoio deles seria muito difícil vencer esse desafio.

Enfim, a todos os que por algum motivo contribuíram para a realização desta pesquisa.

"Os resultados vêm do aproveitamento de oportunidades e não da solução de problemas. A resolução de problemas apenas restaura a normalidade. Oportunidades significam explorar novos caminhos."

(Peter Drucker)

Resumo

TERRA NETO, Rubens Vasconcellos. Desafios da contratação de serviços em nuvem no setor público: um modelo de contratação para o Senado Federal. 2019. 182 folhas. Trabalho de Conclusão de Curso (Pós-Graduação) – Tecnologia da Informação Aplicada ao Poder Legislativo – Instituto Legislativo Brasileiro – Senado Federal, Brasília/DF, 2019.

A adoção da computação em nuvem na Administração Pública Federal se encontra em estágios iniciais, apesar da tecnologia já estar no mercado há mais de dez anos. Os desafios da contratação de serviços em nuvem no setor público são inúmeros e dificultam sua adoção. A legislação que é extensa e complexa e o desconhecimento da tecnologia amedrontam os gestores públicos e retardam sua utilização. Esta pesquisa levantou a legislação e normas existentes como ponto de partida para identificar os delimitadores legais para adoção dos serviços. Por meio do estudo de pesquisas acadêmicas realizadas se construiu um modelo de análise das contratações do Tribunal de Contas da União (TCU) e do Ministério do Planejamento. Para complementar a análise das contratações foram realizadas entrevistas não estruturadas com servidores do TCU e da Agência Brasileira Gestora de Fundos Garantidores e Garantias S.A. (ABGF), órgão partícipe do edital do Ministério do Planejamento e com servidores da Primesys, empresa contratada para prestar o serviço em ambos os editais. Essas entrevistas objetivaram destacar os pontos positivos e negativos destas contratações. Por meio desta análise e com a junção das especificidades normativas do Senado Federal, foram propostos critérios de contratação de serviços em nuvem para o Senado Federal. Como resultado desta pesquisa foram propostos vinte e cinco critérios para a fase de planejamento da contratação, vinte e dois critérios para a fase de seleção do fornecedor e quarenta e dois critérios para a execução contratual e gestão de serviços.

Palavras-chave: Computação em nuvem. Setor Público. Contratação de Serviços. Senado Federal.

Abstract

TERRA NETO, Rubens Vasconcellos. Challenges of contracting cloud computing services in the public sector: a model of contracting for the Brazilian Federal Senate. 2019. 182 pages. Trabalho de Conclusão de Curso (Pós-Graduação) – Tecnologia da Informação Aplicada ao Poder Legislativo – Instituto Legislativo Brasileiro – Senado Federal, Brasília/DF, 2019.

The adoption of cloud computing in the Federal Public Administration is in the early stages, although the technology has been on the market for over ten years. The challenges of hiring cloud services in the public sector are numerous and hamper its adoption. Legislation that is extensive and complex and ignorance of the technology frighten public managers and delay their use. This research has collected the existing legislation and standards as a starting point to identify the legal delimiters for adoption of services. Through the study of academic research conducted, A model for the analysis of the hiring of the Federal Court of Audit (TCU) and the Ministry of Planning was built. In order to complement the hiring analysis, unstructured interviews were conducted with TCU and the Brazilian Agency for the Management of Guarantors and Guarantees SA (ABGF), an entity participating in the bidding notice of the Ministry of Planning and with employees of Primesys, a company contracted to provide the service in both public agencies. These interviews aimed to highlight the positive and negative aspects of these hirings. By means of this analysis and with the normative specificities of the Brazilian Federal Senate, criteria for the contracting of cloud services were proposed for the Brazilian Federal Senate. As a result of this research, twenty-five criteria were proposed for the contracting planning phase, twenty-two criteria for the vendor selection phase and forty-two criteria for the contract execution and service management phase.

Keywords: Cloud computing. Public sector. Contracting services. Brazilian Federal Senate.

Lista de ilustrações

Lista de quadros

Lista de abreviaturas e siglas

ABNT	Associção Brasileira de Normas Técnicas
ADG	Ato da Diretoria-Geral
ANS	Acordo de Nível de Serviço
APF	Administração Pública Federal
API	Interface de Programação de Aplicações da sigla em inglês para *Application Programming Interface*
APS	Ato do Primeiro-Secretário
Art.	Artigo
ATC	Ato da Comissão Diretora
AWS	*Amazon Web Services*
CAPEX	*Capital Expenditure*
CGIbr	Comitê Gestor da *Internet* no Brasil
CISAP	Comissão Interministerial de Sustentabilidade na Administração Pública
COMPRASNET	Portal de Compras Governamentais
CPF	Cadastro de Pessoas Físicas
CPU	Unidade Central de Processamento da sigla em inglês para Central Process Unit
DICA	Disponibilidade, integridade, confidencialidade, autenticidade
DSIC	Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República
GSI	Gabinete de Segurança Institucional da Presidência da República
HLB	Hora Legal Brasileira
IaaS	Infraestrutura como serviço do inglês *Infrastructure as a Service*
IDC	*International Data Corporation*

IEC	Comissão Eletrotécnica Internacional da sigla em inglês para *International Electrotechnical Commission*
IN	Instrução Normativa
ISO	Organização Internacional para Padronização da sigla em inglês para *International Organization for Standardization*
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
MP	Ministério do Planejamento, e suas variações "Ministério do Planejamento, Desenvolvimento e Gestão" e "Ministério do Planejamento, Orçamento e Gestão"
NBR	Norma Brasileira, aprovada pela Associação Brasileira de Normas Técnicas
NC	Norma Complementar
NGACTI	Núcleo de Gestão e Apoio às Contratações de Tecnologia da Informação
NIST	*National Institute of Standards and Tecnology*
NMS	Nível Mínimo de Serviço
ON	Observatório Nacional
OPEX	*Operational Expenditure*
PaaS	Plataforma como serviço do inglês *Platform as a Service*
PI	Informações Pessoais do inglês *Personal Information*
PII	Informações Pessoalmente Identificáveis do inglês *Personally Identifiable Information*
PR	Presidência da República
QoS	Qualidade de Serviço do inglês *Quality of Service*
RAM	Memória de Acesso Randômico da sigla em inglês para Random Access Memory
RASF	Regulamento Administrativo do Senado Federal
Ref.	Referência

RSF	Resolução do Senado Federal
SaaS	Software como serviço do inglês *Software as a Service*
SADCON	Secretaria de Administração de Contratações
SF	Senado Federal
SIC	Segurança da Informação e Comunicações
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
SLA	Acordo de nível de serviço do inglês *Service Level Agreement*
SLTI	Secretaria de Logística e Tecnologia da Informação
SPATR	Secretaria de Patrimônio
SRP	Sistema de Registro de Preços
STI	Secretaria de Tecnologia da Informação
TCMS	Termo de Compromisso de Manutenção de Sigilo
TCO	Custo Total de Propriedade, da sigla em inglês para Total Cost of Ownership
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
USN	Unidade de Serviço em Nuvem
UST	Unidade de Serviço Técnico
VPN	Rede privada virtual do inglês *Virtual Private Network*
XaaS	Alguma coisa como serviço da sigla em inglês onde o X é uma variável para indicar alguma coisa *as a service*

Sumário

1 Introdução

O *National Institute of Standards and Technology* – NIST define a computação em nuvem como:

> "Um modelo que possibilita acesso, de modo conveniente e sob demanda, a um conjunto de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente adquiridos e liberados com mínimo esforço gerencial ou interação com o provedor de serviços." (MELL; GRANCE, 2011, tradução nossa).

A computação em nuvem é vista nas organizações como uma oportunidade estratégica, pois não só pode reduzir os custos, mas facilita a adoção de novas tecnologias mediante o uso sobre demanda e a flexibilidade da contratação que esta tecnologia proporciona. A adoção da computação em nuvem altera as despesas da empresa de *CAPEX* (sigla em inglês para *capital expenditure*) para *OPEX* (sigla em inglês para *operational expenditure*), ou seja, as despesas deixam de ser em bens de capital e passam a ser custos operacionais.

Nos serviços em nuvem o cliente paga exclusivamente pelo que consome, evitando o que normalmente ocorre no serviço público que é adquirir o total que se utiliza em determinado período contratual, o que ocasiona nos primeiros meses um alto nível de ociosidade, gerando altos custos nas avenças. A definição de um modelo para a contratação de nuvens tem se tornado um desafio a ser resolvido pela Administração Pública Federal (APF), tanto pela quantidade de soluções distintas oferecidas pelo mercado, quanto pelo fato de que cada fornecedor tem uma forma própria de comercialização, o que foi observado pelo Acórdão 2.569/2018 do Tribunal de Contas da União (TCU) (BRASIL. TCU, 2018, parágrafo 388, alínea c). Para a aquisição de qualquer solução, a APF deve se utilizar da Lei 8.666/93 (BRASIL, 1993), que estabelece as normas gerais sobre as licitações e contratos administrativos. A licitação é um procedimento formal, estabelecido nessa lei, que regula o processo de competição entre as empresas que pretendem oferecer os seus serviços à APF.

Além das dificuldades encontradas pelos diferentes modelos de comercialização dos serviços de computação em nuvem, o modelo de contratação do governo estabelecido pela Lei 8.666/93 tem inibido os órgãos da APF em caminharem para a contratação desse tipo de serviço. Apesar do interesse por parte do governo na contratação desses serviços ter crescido, principalmente em virtude dos cortes do investimento e da diminuição da contratação e da formação de pessoal, a complexidade da lei de contratações limita a adoção desse modelo de prestação de serviços. O TCU destaca no Acórdão 2.569/2018 que "Não há experiências consistentes de adoção de software baseados totalmente em serviços

ou no modelo de computação em nuvem pela Administração Pública" (BRASIL. TCU, 2018, parágrafo 388, alínea a).

O TCU em 2017 e o extinto Ministério do Planejamento, Desenvolvimento e Gestão (MP) no ano de 2018 se aventuraram na contratação de serviços em nuvem no setor público e são, atualmente, os principais casos a serem analisados para que a administração pública encontre o caminho mais adequado para a adoção dessas novas tecnologias.

Dentre os desafios que devem ser equacionados na contratação de serviços em nuvem estão: o aprisionamento tecnológico, ou *vendor lock-in*, no qual o contratante fica refém do contratado, por não existirem soluções tecnológicas compatíveis nos demais fornecedores ou pelos custos adicionais para a troca de provedor serem substanciais e a localização dos dados, para garantia de prevalência da legislação brasileira sobre qualquer outra.

1.1 Problema de Pesquisa

No âmbito do Senado Federal (SF) ainda não existe uma definição de critérios a serem adotados quanto à contratação de serviços em nuvem. Apesar de já terem sido realizadas as aquisições do TCU e do MP, o SF tem suas especificidades nas contratações, já que não é um órgão do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), e é regido por seus próprios normativos gerando a necessidade de elaboração de um modelo próprio a ser implementado.

Neste estudo foram levantadas as normas vigentes que regem a contratação dos serviços em nuvem, os seus benefícios e riscos, como foram implementadas essas contratações no âmbito do TCU e do MP, e quais as dificuldades encontradas por esses órgãos.

Com base nestes subsídios e considerando as especificidades do Senado Federal, buscou-se responder à seguinte questão "Quais são os critérios essenciais a serem adotados para a contratação de serviços em nuvem nesta casa legislativa?".

1.2 Objetivos

1.2.1 Objetivo geral

Propor critérios de contratação de serviços em nuvem para o Senado Federal.

1.2.2 Objetivos específicos

- Identificar legislação e normas vigentes para a contratação de serviços em nuvem na Administração Pública Federal;

- Analisar trabalhos acadêmicos anteriores;
- Identificar as especificidades das contratações do Senado Federal;
- Elaborar critérios de análise dos editais do TCU e MP por meio das legislações e normas vigentes identificadas;
- Analisar as contratações do TCU e do Ministério do Planejamento.

1.3 Justificativa

Como discutido anteriormente, a computação em nuvem é uma oportunidade de redução de custos nas organizações e sua utilização tem se acentuado no mundo inteiro como podemos perceber por meio da pesquisa de Smith e Shirer (2019):

> Estima-se que os gastos mundiais em serviços e infraestrutura de nuvem pública atinjam US$ 210 bilhões em 2019, um aumento de 23,8% em relação a 2018, de acordo com a mais recente atualização do Guia Semestral de Gastos em Serviços de Nuvem Pública da *International Data Corporation* (IDC). Embora o crescimento anual dos gastos deva desacelerar levemente durante o período de previsão 2017-2022, o mercado deverá alcançar uma taxa de crescimento anual composta de cinco anos (CAGR) de 22,5%, com os gastos em serviços de nuvem pública chegando a US $ 370 bilhões em 2022.

Os principais motivadores da adoção da computação em nuvem têm sido a facilidade de instalação e atualização, redução de custos, diminuição do risco de utilização de aplicações defasadas, possibilidade de integração, ganho de agilidade, não imobilizar capital pela troca do CAPEX por OPEX, melhoria do gerenciamento, aumento de disponibilidade e melhoria da segurança.

A adoção de um modelo de computação em nuvem tem se tornado uma solução para a APF, já que com a instituição da Emenda constitucional nº. 95 do teto dos gastos (BRASIL, 2016b), houve o congelamento dos gastos públicos, tornando premente que os órgãos sejam mais eficientes na utilização do seu orçamento, para que se possa aumentar a produtividade sem aumentar os custos. O TCU (BRASIL. TCU, 2015), por meio de seu Acórdão 1.739/2015 e o MP (BRASIL. MP, 2016b) em seu documento "Boas práticas, orientações e vedações para contratação de serviços de computação em nuvem" têm sido os grandes norteadores da APF sobre como contratar o serviço de nuvem. Porém, esses documentos foram elaborados antes de contratações de vulto de tais serviços.

1.4 Principais contribuições

A principal contribuição deste trabalho será propor um modelo de critérios de contratação em nuvem para o Senado Federal por meio da avaliação de como foram

realizadas as contratações do TCU e do MP, o grau de acerto de suas orientações, modelos, e quais foram seus pontos positivos e negativos.

1.5 Apresentação do manuscrito

Este estudo está estruturado da seguinte forma:

- **Capítulo 2**: apresenta a Metodologia empregada para o desenvolvimento deste estudo;
- **Capítulo 3**: apresenta os conceitos de computação em nuvem, suas características essenciais, modelos de serviço, modelos de implementação e os principais papéis de uma arquitetura de referência;
- **Capítulo 4**: apresenta o arcabouço normativo referente à contratação de serviços em nuvem na APF, destacando os pontos essenciais das leis, decretos, instruções normativas, normas complementares, portarias, acórdãos do TCU e normas técnicas;
- **Capítulo 5**: discute em relação aos trabalhos acadêmicos levantados, alguns pontos que devem ser considerados na proposição de critérios para o Senado Federal;
- **Capítulo 6**: apresenta as especificidades do Senado Federal, por meio da análise dos pontos essenciais das resoluções, atos da Comissão Diretora, atos do Primeiro Secretário e Atos da Diretoria Geral que normatizam o processo de contratação e outros assuntos afetos à computação em nuvem;
- **Capítulo 7**: analisa as contratações de serviços de computação em nuvem realizadas pelo TCU e pelo MP;
- **Capítulo 8**: apresenta a proposição dos critérios para contratação de serviços em nuvem pelo Senado Federal, divididos em critérios para a fase de planejamento da contratação, para a fase de seleção do fornecedor e para a fase de execução e gestão dos serviços;
- **Capítulo 9**: apresenta as conclusões, as limitações encontradas durante a realização do estudo e os trabalhos futuros que podem se originar ou ser realizados com base neste.
- **Apêndice A**: apresenta as leis, decretos, instruções normativas e documentos vigentes aplicáveis à contratação de serviços em nuvem identificados quando do levantamento de referências para a realização deste trabalho.
- **Apêndice B**: apresenta os trabalhos acadêmicos relacionados à contratação de nuvem no setor público brasileiro pesquisados.

- **Apêndice C**: apresenta as resoluções, normas e atos próprios do Senado Federal relacionados às contratações e a sua área de Tecnologia da Informação.

2 Metodologia

Nesta pesquisa buscou-se definir critérios para a contratação de serviços em nuvem para o Senado Federal, por meio da avaliação dos riscos, benefícios e desafios encontrados na execução de contratos semelhantes da administração pública federal, em especial o Tribunal de Contas da União (TCU) e o Ministério do Planejamento, Desenvolvimento e Gestão (MP), que estão na vanguarda na adoção dessa nova tecnologia. Para Gil (2017, p.26) as pesquisas aplicadas têm o objetivo de adquirir conhecimentos com vistas à aplicação em uma situação específica e as exploratórias visam proporcionar mais familiaridade com o problema, habilitando o pesquisador a construir hipóteses. O planejamento das pesquisas exploratórias é flexível e se desenvolve normalmente por meio de levantamento bibliográfico, entrevistas com pessoas que tiveram experiência prática com o assunto e análise de exemplos.

Para os estudos dos casos foram adotadas as pesquisas bibliográficas e entrevistas não estruturadas com os responsáveis pelos contratos. Para Yin (2001, p.19) os estudos de caso são em geral utilizados quando o pesquisador não tem controle sobre os acontecimentos e quando os fenômenos estudados são contemporâneos e fazem parte de algum contexto da vida real. Yin (2001, p.21) reforça ainda que o estudo de caso contribui sobremaneira para a compreensão de fenômenos organizacionais, que é o objeto deste estudo.

As entrevistas aconteceram no dia 15 de maio de 2019 com o gerente de contas da área de governo e o gerente de soluções digitais da Embratel Primesys, que é a empresa contratada como *broker* nos contratos do TCU e do MP. No dia 10 de junho de 2019 com a Diretora do Ambiente Computacional da Secretaria de Infraestrutura de TI e gestora do contrato de serviços em nuvem do TCU. E no dia 02 de julho de 2019 com o Gerente de Tecnologia da Informação da Agência Brasileira Gestora de Fundos Garantidores e Garantias S.A.(ABGF), que era no momento o partícipe do edital do MP que se encontrava mais adiantado na adoção de serviços em nuvem.

Os dados coletados foram classificados e avaliados quanto a diversos princípios adotando-se para tanto a literatura existente para a área como a legislação brasileira, os documentos oficiais expedidos pelas duas entidades e pelos pesquisadores da área. Essa classificação procurou levantar os riscos e benefícios inerentes à utilização dos serviços em nuvem e como cada um deles foi tratado no âmbito dos casos estudados.

A partir dessa análise foram realizadas sugestões de solução para compor os critérios essenciais para o Senado Federal.

3 Conceitos de Computação em Nuvem

Antes de apresentar os critérios essenciais para a contratação de serviços em nuvem no Senado Federal, é preciso introduzir alguns conceitos básicos. Neste capítulo serão apresentados os conceitos relacionados à computação em nuvem, que formam a fundamentação teórica relativa à essa tecnologia.

3.1 Computação em Nuvem

A definição de nuvem do *National Institute of Standards and Technology* – NIST, que foi citada no Capítulo 1, página 29, é hoje a definição mais utilizada na literatura sobre o assunto. Outros autores procuraram definir também a computação em nuvem, e esse tema foi estudado por Vaquero et al. (2008, p.51, tradução livre), que definiu nuvem como:

> As nuvens são um grande conjunto de recursos virtualizados facilmente utilizáveis e acessíveis (como *hardware*, plataformas de desenvolvimento e/ou serviços). Esses recursos podem ser dinamicamente adaptados a uma carga variável (escala), permitindo também uma ótima utilização dos recursos. Esse conjunto de recursos é tipicamente explorado por um modelo pagamento por uso, no qual as garantias são oferecidas pelo provedor de infraestrutura por meio de acordos de nível de serviço personalizados.

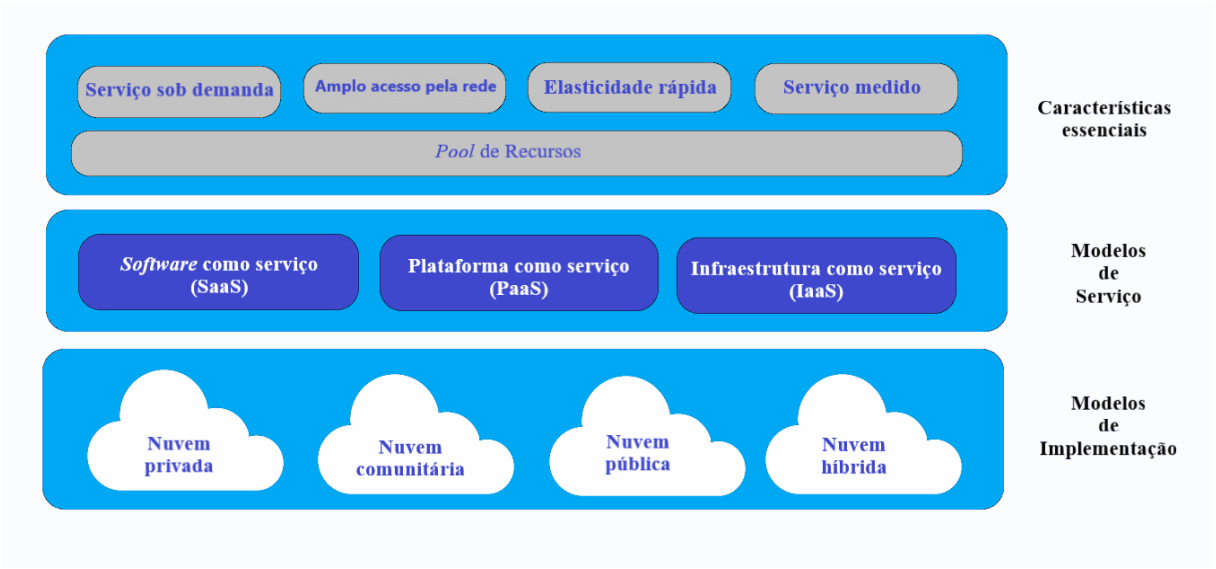
Além da própria definição de nuvem, Mell e Grance (2011, pp.2–3) definem ainda as características essenciais, os modelos de serviço e os modelos de implantação da Computação em Nuvem ilustrados na Figura 1 e que serão definidos a seguir.

3.1.1 Características essenciais

a) **Serviço sob demanda**. Por meio desta característica, o usuário do serviço pode escolher quais recursos computacionais ele deseja utilizar. Ele pode definir o poder de processamento, a quantidade de memória, o tamanho do armazenamento, e várias outros recursos conforme necessário, sem exigir interação com cada provedor de serviços. Os recursos poderão ser alocados pelo usuário na medida necessária, pois o provedor funciona como um *pool* de recursos virtualmente infinitos à disposição da organização.

b) **Amplo acesso pela rede**. Os recursos estão disponíveis na rede e são acessíveis por meio de mecanismos padronizados que permitem o uso por plataformas

Figura 1 – Definições de Computação em nuvem



Fonte: NIST (MELL; GRANCE, 2011, tradução nossa)

heterogêneas. O acesso é possível para qualquer tipo de dispositivo cliente como, por exemplo, telefones celulares, *tablets*, *laptops* e estações de trabalho.

c) ***Pool* de recursos**. Os recursos computacionais do provedor são agrupados para atender a vários usuários usando um modelo *multi-tenant*[1], com diferentes recursos físicos e virtuais dinamicamente atribuídos e reatribuídos de acordo com a demanda dos usuários, sem que um interfira no outro. Existe uma sensação de independência da localização em que o cliente geralmente não tem controle ou conhecimento sobre a exata localização dos recursos fornecidos, mas pode ser capaz de especificar a localização em um nível de abstração (por exemplo, país, estado ou *Data center*).

d) **Elasticidade rápida**. Os recursos podem ser provisionados e liberados elasticamente, em alguns casos automaticamente, sendo aumentados ou diminuídos proporcionalmente à demanda. Para o usuário, os recursos disponíveis para provisionamento geralmente parecem ilimitados e podem ser utilizados em qualquer quantidade e a qualquer momento que necessitar.

e) **Serviço medido**. Os sistemas em nuvem controlam e otimizam automaticamente o uso de recursos aproveitando uma capacidade de medição por algum recurso apropriado ao tipo de serviço (por exemplo, armazenamento, processa-

[1] Um dos princípios fundamentais da computação em nuvem pública é o modelo *multi-tenant*, de uma única instância lógica compartilhada por centenas ou milhares de usuários. Em outras palavras, a típica arquitetura que permite a otimização do uso de recursos de infraestrutura e *software* por meio de compartilhamento, mantendo os inquilinos/usuários logicamente separados. É comum os usuários compartilharem os mesmos recursos de computação: processamento, armazenamento, espaço, memória, largura de banda de rede, etc.

mento, largura de banda e contas de usuário ativas). O uso de recursos pode ser monitorado, controlado e medido, proporcionando transparência tanto para o provedor como para o usuário do serviço utilizado. Os recursos computacionais então podem, por meio do uso de computação em nuvem, passar a ser utilizados e tarifados como se fossem água, luz, telefone, etc.

3.1.2 Modelos de serviço

O TCU (BRASIL. TCU, 2015, pp. 6–7) traduz da seguinte forma as definições dos modelos de serviços feitas por Mell e Grance (2011, pp. 2–3):

> ***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.
>
> **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.
>
> **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).

Esses três modelos são os modelos fundamentais da computação em nuvem, mas em artigos, principalmente de marketing das empresas, podemos verificar outros modelos como comentado por (CARISSIMI, 2015, p. 8)

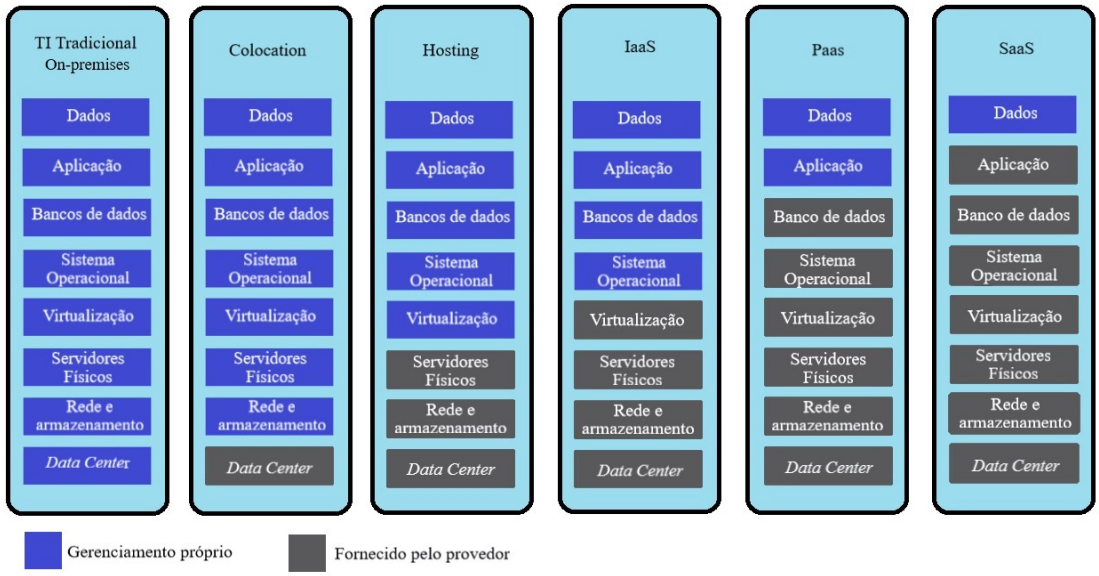
> É interessante comentar que o marketing define muitos outros serviços, mas que, na verdade, nada mais são que especializações do modelo SaaS. Por exemplo, é possível citar serviços como *Information as a Service, Integration as a Service, Security as a Service, Testing as a Service* e até mesmo *Fax as a Service* para o envio de *faxes*. Tal criatividade do marketing cunhou o modelo *XaaS (x as a service)*, onde x significa "alguma coisa".

Os modelos de serviços em nuvem são evoluções de modelos de terceirização de serviços de Tecnologia da Informação (TI), nos quais aos poucos a responsabilidade sobre os serviços vem sendo gradualmente transferida para provedores de serviços.

O ponto de partida dessa evolução é um modelo em que todos os serviços são prestados pela área de TI do próprio cliente, *on-premises*[2]. O passo seguinte é a utilização do modelo de *Colocation*[3], no qual a empresa alugava espaço em um *Data Center* para a colocação de seus equipamentos, seguido pela Hospedagem, ou *Hosting*[4], em que a responsabilidade do provedor passava a ser fornecer servidores físicos para os usuários, para se chegar enfim aos modelos de serviços fundamentais de nuvem.

Em cada um dos modelos a responsabilidade é dividida entre o provedor do serviço e o usuário. Porém, não é apenas a responsabilidade que é transferida, mas também o Custo Total de Propriedade (TCO, do inglês *Total Cost of Ownership*), que inclui as despesas de manutenção, atualização e operação dos equipamentos, além dos custos inerentes aos profissionais de TI que trabalham diretamente com essas atividades. Na Figura 2 se vê como se dá a divisão de responsabilidade em cada um dos modelos.

Figura 2 – Divisão de responsabilidades entre cliente e fornecedor de nuvem



Fonte: (FEDOSEENKO, 2018, tradução nossa)

[2] O sistema *on-premises* é o uso de servidores, equipamentos e recursos de TI dentro da empresa sob sua responsabilidade. Ou seja, é utilizada infraestrutura local interna própria ou de terceiros em vez de serviço externo para processar suas aplicações de *hardware* e *software*. A própria empresa é responsável pelas configurações, implementações e atualizações.

[3] O *Colocation* é um serviço de aluguel apenas da infraestrutura de data center para a instalação do servidor do cliente. Ele se diferencia do servidor dedicado pela ausência de contratação do equipamento de processamento, já que esse pertence ao cliente. O serviço de *data center* entra como suporte, fornecendo serviço, espaço no *rack*, energia elétrica, conectividade com a internet, climatização, etc

[4] *Hosting* é hospedagem tradicional. Hospeda aplicações, soluções de tecnologia da informação ou ativos, além de gerenciar tarefas de manutenção para garantir o pleno e bom funcionamento do ambiente. Ele se apresenta em duas categorias: hospedagem dedicada e hospedagem compartilhada

3.1.3 Modelos de implantação

Mell e Grance (2011, p. 3) definem os seguintes modelos de implantação:

> **Nuvem privada**. A infraestrutura de nuvem é provisionada para uso exclusivo por uma única organização que inclui vários consumidores (por exemplo, unidades de negócios). Ele pode ser de propriedade, gerenciado e operado pela organização, por terceiros ou por alguma combinação deles, e pode existir dentro ou fora das instalações.
>
> **Nuvem comunitária**. A infraestrutura em nuvem é provisionada para uso exclusivo por uma comunidade específica de consumidores de organizações que compartilham preocupações (por exemplo, missão, requisitos de segurança, políticas e considerações de conformidade). Ele pode ser de propriedade, gerenciado e operado por uma ou mais organizações da comunidade, um terceiro ou uma combinação deles, e pode existir dentro ou fora das instalações.
>
> **Nuvem pública**. A infraestrutura de computação em nuvem é disponibilizada para utilização aberta pelo público em geral. Pode ser de propriedade, geridos e operados por uma organização empresarial, acadêmica ou governamental, ou alguma combinação entre elas. Ela existe nas instalações do provedor de nuvem.
>
> **Nuvem híbrida**. A infraestrutura de nuvem é uma composição de duas ou mais infraestruturas de nuvem distintas (privada, comunitária ou pública) que permanecem como entidades exclusivas, mas unidas por tecnologia padronizada ou proprietária que permite a portabilidade de dados e aplicativos (por exemplo, *cloud bursting*[5] para balanceamento de carga entre nuvens).

3.1.4 Arquitetura de Referência da Computação em Nuvem

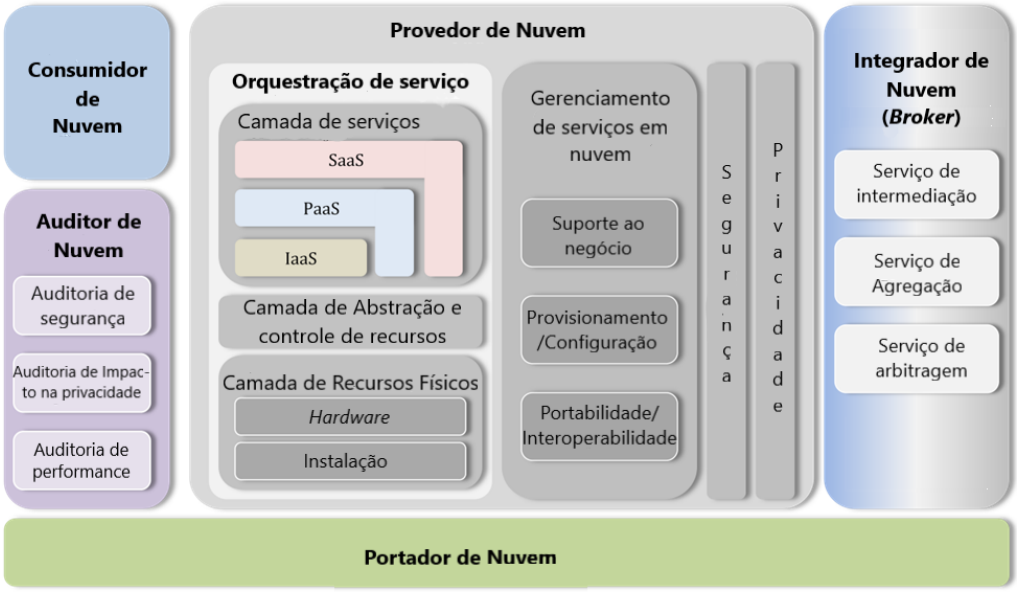
O NIST, conforme Liu et al. (2011, p.3), define uma visão da arquitetura de referência da computação em nuvem, que é apresentada no modelo da Figura 3, na página 42. Neste modelo são definidos cinco papéis: o consumidor de nuvem, o provedor de nuvem, o integrador de nuvem (*Broker*), o auditor de nuvem e o portador de nuvem. Nas seções seguintes iremos detalhar os papéis de cada uma destas entidades, conforme definidos por Liu et al. (2011, pp.5–8).

3.1.4.1 Consumidor de nuvem

O consumidor de nuvem é uma pessoa ou organização que mantém algum relacionamento de negócios com um provedor de nuvem e utiliza os seus serviços. É o cliente ou usuário do serviço de nuvem.

[5] Em computação em nuvem, *cloud bursting* é uma configuração definida entre uma nuvem privada e uma nuvem pública para lidar com picos na demanda de TI. Se uma organização que usa uma nuvem privada alcançar 100% de sua capacidade de recursos, o tráfego excedente será direcionado a uma nuvem pública para que não haja interrupção de serviços

Figura 3 – Arquitetura de Referência da Computação em Nuvem

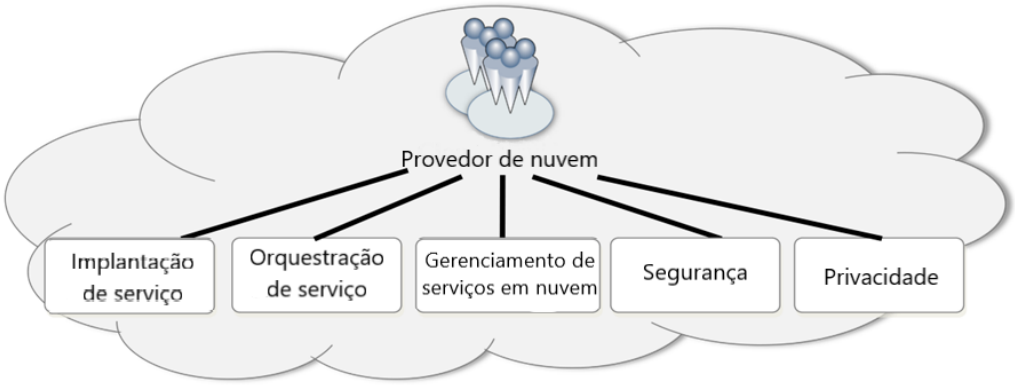


Fonte: Adaptado de Liu et al. (2011, p. 3, tradução nossa)

3.1.4.2 Provedor de nuvem

O provedor de nuvem, como o próprio nome já diz, é uma pessoa ou organização que provê um serviço em nuvem. Um provedor de nuvem tem maior ou menor grau de responsabilidade de acordo com o serviço que oferece, conforme foi mostrado na Figura 2 da subseção 3.1.2 na página 40, e suas atividades são conduzidas em cinco grandes áreas: implantação de serviços, orquestração de serviços, gerenciamento de serviços em nuvem, segurança e privacidade, conforme definidos por Liu et al. (2011, pp.10–17). Como mostrada na Figura 4.

Figura 4 – Provedor de nuvem - Principais áreas de atividades



Fonte: (LIU et al., 2011, p.7, tradução nossa)

3.1.4.2.1 Implantação de serviços

A implantação de serviços é a disponibilização do serviço de nuvem por meio de um dos modelos de implantação conforme definidos na subseção 3.1.3, na página 41, em que as diferenças estão baseadas em quão exclusivos os recursos computacionais são para os consumidores de nuvem.

3.1.4.2.2 Orquestração de serviços

A orquestração de serviços segundo Liu et al. (2011, pp.12–13), refere-se à composição de componentes do sistema para oferecer suporte às atividades dos provedores de nuvem na organização, coordenação e gerenciamento de recursos de computação, a fim de fornecer serviços de TI para os consumidores de nuvem.

Na Figura 3, na página 42, pode ser visto dentro da orquestração de serviço um modelo de três camadas. Na parte superior está a camada de serviços, onde os provedores de nuvem definem interfaces de acesso para cada um dos três modelos de serviços para utilização pelos consumidores de nuvem. Já a camada intermediária é uma camada de abstração e controle dos recursos, ela contém os componentes do sistema que os provedores utilizam para fornecer e gerenciar o acesso aos recursos de computação física por meio da abstração de software. A abstração de recursos precisa garantir o uso eficiente, seguro e confiável dos recursos físicos. O aspecto de controle dessa camada refere-se aos componentes de software responsáveis pela alocação de recursos, controle de acesso e monitoramento de uso. Essa é a malha de software que une os numerosos recursos físicos subjacentes e suas abstrações de software para permitir o pool de recursos, a alocação dinâmica e o serviço medido.

A camada mais baixa é a camada de recursos físicos, que inclui todos os recursos de computação física. Essa camada inclui recursos de hardware, como computadores (CPU e memória), redes (roteadores, *firewalls*, *switches*, *links* de rede e interfaces), componentes de armazenamento (discos rígidos) e outros elementos da infraestrutura de computação física. Também inclui recursos de instalações, como aquecimento, ventilação e ar condicionado, energia, comunicações e outros aspectos da planta física.

A orquestração pode se dar tanto dentro de um único provedor de nuvem, como também pode tratar-se de organização e coordenação dos recursos de diversos provedores de forma automatizada em uma única plataforma de trabalho.

3.1.4.2.3 Gerenciamento de serviços em nuvem

O gerenciamento de serviços em nuvem inclui todas as funções relacionadas aos serviços que são necessárias para o gerenciamento e operação dos serviços requeridos pelos

consumidores de nuvem. Os serviços de gerenciamento, incluem o suporte ao negócio, o provisionamento e configuração, e a portabilidade e interoperabilidade.

O suporte de negócios envolve o conjunto de serviços usados para executar operações de negócios voltadas para o cliente. Estas operações incluem o gerenciamento dos clientes, gerenciamento dos contratos, catálogo de serviços, contabilidade e faturamento dos clientes, relatórios e auditoria, e preço e avaliação dos serviços.

O provisionamento e configuração são duas funções principais da arquitetura de serviços em nuvem, que segundo Liu et al. (2011, p.15, tradução nossa) são compostos de:

> **Provisionamento rápido**: implantação automática de sistemas em nuvem com base no serviço/recursos/recursos solicitados.
>
> **Mudança de recursos**: ajuste de configuração/alocação de recursos para reparos, atualizações e junção de novos nós na nuvem.
>
> **Monitoramento e Relatórios**: Descobrindo e monitorando recursos virtuais, monitorando operações e eventos na nuvem e gerando relatórios de desempenho.
>
> **Medição**: Fornecer um recurso de medição em algum nível de abstração apropriado ao tipo de serviço (por exemplo, armazenamento, processamento, largura de banda e contas de usuário ativas).
>
> **Gerenciamento de Acordo de Nível de Serviço (ANS)**: englobando a definição de contrato de ANS (esquema básico com parâmetros de Qualidade do Serviço (QoS)), monitoramento de ANS e aplicativo de ANS de acordo com políticas definidas.

Provedores de nuvem devem fornecer mecanismos para suportar portabilidade de dados, interoperabilidade de serviços e portabilidade do sistema. A portabilidade de dados é a capacidade dos consumidores da nuvem de copiar objetos de dados para dentro ou fora de uma nuvem ou de usar um disco para transferência de dados em massa. A interoperabilidade de serviços é a capacidade dos consumidores da nuvem de usar seus dados e serviços em vários provedores de nuvem com uma interface de gerenciamento unificada. A portabilidade do sistema permite a migração de uma instância de máquina virtual totalmente parada ou de uma imagem de máquina de um provedor para outro provedor ou a migração de aplicativos e serviços e seu conteúdo de um provedor de serviços para outro.

3.1.4.2.4 Segurança

É fundamental reconhecer que a segurança é um aspecto transversal da arquitetura que abrange todas as camadas do modelo de referência, desde a segurança física até a segurança do aplicativo. Portanto, a segurança nas preocupações de arquitetura de computação em nuvem não está apenas sob a alçada dos Provedores de Nuvem, mas também dos Consumidores em Nuvem e outros atores relevantes, como auditores, integradores e

portadores. Os sistemas baseados em nuvem ainda precisam atender aos requisitos de segurança, como autenticação, autorização, disponibilidade, confidencialidade, gerenciamento de identidade, integridade, auditoria, monitoramento de segurança, resposta a incidentes e gerenciamento de políticas de segurança.

3.1.4.2.5 Privacidade

Os provedores de nuvem devem proteger a coleta, processamento, comunicação, uso e armazenamento seguros, adequados e consistentes de informações pessoais (PI, do inglês *Personal Information*) e informações pessoalmente identificáveis (PII, do inglês *Personally Identifiable Information)* na nuvem.

A Lei Geral de Proteção de Dados (LGPD) visa garantir a privacidade das informações pessoalmente identificáveis coletadas. PII é a informação que pode ser usada para distinguir ou rastrear a identidade de um indivíduo, como seu nome, número no Cadastro de Pessoas Físicas (CPF), registros biométricos, etc. sozinho, ou quando combinado com outras informações pessoais ou de identificação vinculadas ou vinculáveis a um indivíduo específico, como data e local de nascimento, nome de solteira da mãe, etc. Embora a computação em nuvem forneça uma solução flexível para recursos, software e informações compartilhados, ela também representa desafios adicionais de preservação da privacidade para os consumidores que usam as nuvens.

3.1.4.3 Auditor de nuvem

O auditor de nuvem é uma entidade que realiza avaliações independentes dos serviços em nuvem, das operações dos sistemas de informações, do desempenho e da segurança da implementação da nuvem.

Auditorias são realizadas para verificar a conformidade com os padrões por meio da revisão de evidências objetivas. Um auditor de nuvem pode avaliar os serviços fornecidos por um provedor de nuvem em termos de controles de segurança, impacto de privacidade, desempenho etc.

Os controles de segurança são técnicas empregadas dentro de um sistema de informações organizacionais para proteger a confidencialidade, integridade e disponibilidade do sistema e suas informações. A auditoria de segurança deve incluir também a verificação da conformidade com a regulamentação e a política de segurança.

Uma auditoria de impacto de privacidade deve garantir que estão sendo cumpridas as leis e regulamentos de privacidade aplicáveis que regem a privacidade de um indivíduo e garantir a confidencialidade, integridade e disponibilidade das informações pessoais de um indivíduo em cada estágio de desenvolvimento e operação.

3.1.4.4 Integrador de nuvem (*Broker*)

O Integrador de nuvem, ou *Broker*, é uma entidade que gerencia o uso, desempenho e entrega de serviços em nuvem e faz a intermediação do relacionamento entre provedores de nuvem e os consumidores.

Conforme a computação em nuvem evolui, a integração de serviços de nuvem pode ser muito complexa para os consumidores de nuvem gerenciarem. Neste ponto é que entra o *broker* que faz a intermediação da solicitação do serviço e presta consultoria e suporte aos consumidores. Em geral o *broker* fornece três tipos de serviço:

a) **Serviço de intermediação**. um broker aprimora um determinado serviço, aprimorando alguns recursos específicos e fornecendo serviços de valor agregado aos consumidores de nuvem. A melhoria pode ser o gerenciamento de acesso a serviços em nuvem, gerenciamento de identidades, relatórios de desempenho, segurança aprimorada, etc.

b) **Serviço de agregação**. o *broker* combina e integra vários serviços em um ou mais novos serviços. Ele fornece integração de dados e garante a movimentação segura de dados entre o consumidor de nuvem e vários provedores de nuvem.

c) **Serviço de arbitragem**. O serviço de arbitragem é semelhante ao serviço de agregação, exceto que os serviços que estão sendo agregados não são fixos. Serviço de arbitragem significa que um *broker* tem a flexibilidade de escolher serviços de vários provedores. O *broker*, por exemplo, pode usar um serviço de pontuação de crédito para medir e selecionar qual o provedor com a melhor pontuação.

3.1.4.5 Portador de nuvem

É um intermediário que fornece a conectividade entre o provedor de nuvem e o consumidor do serviço. O portador de nuvem fornece conectividade para o dispositivo do consumidor poder acessar e transferir aplicativos e serviços do provedor de nuvem. Um bom exemplo de portador de nuvem é uma empresa de telefonia.

3.2 Conclusão do capítulo

Neste capítulo foram apresentados os conceitos básicos de computação em nuvem, suas características essenciais, os modelos de serviço e de implantação e sua arquitetura de referência. No próximo capítulo serão apresentadas a legislação e as normas vigentes para a contratação desses serviços na Administração Pública Federal (APF).

4 Legislação e normas vigentes para a contratação de serviços em nuvem na APF

O primeiro objetivo específico deste estudo era "Identificar legislação e normas vigentes para a contratação de serviços em nuvem na Administração Pública Federal", para tanto, foi realizada uma pesquisa buscando as legislações, normas e documentos que se aplicam às contratações públicas e em especial à contratação de serviços em nuvem no âmbito da Administração Pública Federal.

Foram encontradas no Acórdão 1.739/2015 do TCU (BRASIL. TCU, 2015, pp. 20–22), e em diversos estudos, entre eles Lopes (2015, pp. 44–52), Santos (2019, p. 8) e Ferreira e Andrade (2016, pp. 9–11), levantamentos de legislação e normas para a contratação de serviços em nuvem na APF. Contudo, verificou-se que, após esses estudos alguns normativos foram revogados.

Assim, para se ter um referencial sobre os normativos atualmente em vigor foi feito um novo levantamento e os mesmos foram divididos em diversos quadros que se encontram no Apêndice A na página 171. No Quadro 20 estão listadas as leis, no Quadro 21 os decretos, no Quadro 22 as instruções normativas, no Quadro 23 as normas complementares e no Quadro 24 os demais documentos e normas. Neste capítulo destacou-se o que deve ser utilizado como referencial normativo para a elaboração de um modelo de contratação de serviços em nuvem na APF.

4.1 Leis

Nenhuma das leis levantadas, relacionadas no Quadro 20 do Apêndice A na página 171, trata especificamente de contratação de serviços em nuvem. Sua aplicabilidade no estudo está relacionada a contratação pública, internet e classificação de dados, que são assuntos que compõem a base para os serviços em nuvem. Na análise não vamos nos deter em aspectos comuns das contratações de TI, mas procurar destacar aspectos que devam ser observados para as contratações de serviços em nuvem.

A Lei nº 8.666/93, de 21 de junho de 1993 (BRASIL, 1993), que é a regulamentação do modelo de contratações da Administração Pública Federal, e a Lei nº 10.520, de 17 de julho de 2002 (BRASIL, 2002), que institui o pregão, que é uma modalidade de licitação aplicável a aquisição de bens e serviços comuns, são a base legal aplicada para as contratações da Administração Pública Federal e deverão ser seguidas. Cabe destacar que, nessas leis são estabelecidos os critérios de classificação das propostas para a determinação

do ganhador do processo licitatório e que cada provedor de serviços em nuvem tem serviços e forma de comercialização distintos, o que faz com que seja um desafio a ser discutido na definição do modelo o critério a ser utilizado para determinar a proposta mais vantajosa para a APF.

A Lei nº 12.527, de 18 de novembro de 2011 conhecida como Lei de Acesso à Informação (LAI) regula o acesso as informações públicas dos órgãos e entidades. Essa lei mudou o paradigma quanto às informações no setor público, que passam a ser predominantemente públicas e aberta a todos. A publicidade é o preceito geral e o sigilo a exceção. Os órgãos devem assegurar: uma gestão transparente da informação, propiciando amplo acesso e divulgação; proteção da informação, garantindo sua disponibilidade, autenticidade e integridade; proteção da informação sigilosa e da informação pessoal, e eventual restrição de acesso. Portanto, procedimentos para garantir o cumprimento da LAI deverão ser adotados na formulação dos critérios de contratação de serviços em nuvem. Cabe ressaltar o parágrafo único do artigo 26 da Seção III:

> Parágrafo único. A pessoa física ou entidade privada que, em razão de qualquer vínculo com o poder público, executar atividades de tratamento de informações sigilosas adotará as providências necessárias para que seus empregados, prepostos ou representantes observem as medidas e procedimentos de segurança das informações resultantes da aplicação desta Lei.
>
> (BRASIL, 2011, Seção III, Artigo 26, Parágrafo único)

A Lei nº 12.965, de 23 de abril de 2014 conhecida como Marco Civil da Internet estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Esta lei se destaca quanto à garantia da neutralidade da rede (garantia de tratamento isonômico de quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação), da proteção aos registros, aos dados pessoais, às comunicações privadas e à liberdade de expressão. Deixa claro a aplicabilidade da legislação brasileira quanto aos dados coletados em território nacional conforme artigo 11:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
>
> (BRASIL, 2014a, art. 11)

Cabe destacar que, a lei não obriga que os dados dos usuários brasileiros sejam armazenados em bases de dados de *data centers* localizados fisicamente no Brasil, e apenas estabelece uma diretriz para atuação do poder público quanto ao estímulo à implantação

de centros de armazenamento, gerenciamento e disseminação de dados no País (BRASIL, 2014a, art. 24, inciso VII).

A Lei nº 13.709, de 14 de agosto de 2018 conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD) regula o tratamento de dados pessoais, inclusive nos meios digitais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018c, art. 1º). Essa lei está relacionada à contratação de serviços em nuvem, pois gera a necessidade de zelarmos pela proteção dos dados pessoais, e sua aplicação se dá conforme o artigo 3º:

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
>
> I - a operação de tratamento seja realizada no território nacional;
>
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;
>
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Medida Provisória nº 869, de 2018)
>
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
>
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
>
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

4.2 Decretos

Assim como no caso das leis, alguns dos decretos citados no Quadro 21 da página 172 são a base de normativos legais que regulamentam as contratações da administração pública federal. São os casos dos decretos nº 5.450, de 31 de maio de 2005 (BRASIL, 2005), que estabelece o pregão eletrônico, nº 7.174, de 12 de maio de 2010 (BRASIL, 2010), que regulamenta a contratação de bens e serviços de informática e automação, e nº 7.892, de 23 de janeiro de 2013 (BRASIL, 2013a), que regulamenta o Sistema de Registro de Preços. Apesar de aplicáveis ao processo de contratações de serviços em computação em nuvem, não têm pontos específicos que mereçam destaque para a elaboração do modelo a ser proposto.

O Decreto nº 7.724, de 16 de maio de 2012 (BRASIL, 2012a) regulamenta a Lei nº 12.527, de 18 de novembro de 2011 (LAI) e alerta quanto as providências a serem tomadas no tratamento de informações classificadas em qualquer grau de sigilo no seu artigo 44:

> Art. 44. As autoridades do Poder Executivo federal adotarão as providências necessárias para que o pessoal a elas subordinado conheça as normas e observe as medidas e procedimentos de segurança para tratamento de informações classificadas em qualquer grau de sigilo.
>
> Parágrafo único. A pessoa natural ou entidade privada que, em razão de qualquer vínculo com o Poder Público, executar atividades de tratamento de informações classificadas, adotará as providências necessárias para que seus empregados, prepostos ou representantes observem as medidas e procedimentos de segurança das informações.
>
> (BRASIL, 2012a, art. 44)

O Decreto nº 7.845, de 14 de novembro de 2012 regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e com base nele, será imprescindível o modelo tratar da celebração de um Termo de Compromisso de Manutenção de Sigilo (TCMS) (BRASIL, 2012b, Anexo I), como descrito no art. 48.

> Art. 48. A celebração de contrato, convênio, acordo, ajuste, termo de cooperação ou protocolo de intenção cujo objeto contenha informação classificada em qualquer grau de sigilo, ou cuja execução envolva informação classificada, é condicionada à assinatura de TCMS e ao estabelecimento de cláusulas contratuais que prevejam os seguintes requisitos:
>
> I obrigação de manter sigilo relativo ao objeto e a sua execução;
>
> II possibilidade de alteração do objeto para inclusão ou alteração de cláusula de segurança não estipulada previamente;
>
> III obrigação de adotar procedimentos de segurança adequados, no âmbito das atividades sob seu controle, para a manutenção do sigilo relativo ao objeto;
>
> IV identificação, para fins de concessão de credencial de segurança e assinatura do TCMS, das pessoas que poderão ter acesso a informação classificada em qualquer grau de sigilo e material de acesso restrito;
>
> V obrigação de receber inspeções para habilitação de segurança e sua manutenção;
>
> VI responsabilidade em relação aos procedimentos de segurança, relativa à subcontratação, no todo ou em parte.
>
> (BRASIL, 2012b, artigo 48)

Percebe-se que caso decida-se por armazenar na nuvem dados classificados em qualquer grau de sigilo, será necessário que conste no contrato com o provedor de serviços em nuvem diversos dispositivos que garantam o cumprimento da legislação, inclusive verificando se o provedor atende aos requisitos definidos no artigo 11:

> Art. 11. A concessão de habilitação de entidade privada como posto de controle fica condicionada aos seguintes requisitos:
>
> I - regularidade fiscal;
>
> II - comprovação de qualificação técnica necessária à segurança de informação classificada em qualquer grau de sigilo;

> III - expectativa de assinatura de contrato sigiloso;
>
> IV - designação de gestor de segurança e credenciamento, e de seu substituto; e
>
> V - aprovação em inspeção para habilitação de segurança.
>
> (BRASIL, 2012b, artigo 11)

Novamente no Decreto nº 8.771, de 11 de maio de 2016 que regulamenta a Lei nº 12.965, de 23 de abril de 2014, fica ressaltada a preocupação com os padrões de segurança e sigilo dos registros, dados pessoais e comunicações privadas, como podemos verificar no art.23 (BRASIL, 2016a, art. 23):

> Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:
>
> I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;
>
> II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;
>
> III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014; e
>
> IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.
>
> § 1º Cabe ao CGIbr promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais para o disposto nesse artigo, de acordo com as especificidades e o porte dos provedores de conexão e de aplicação.
>
> § 2º Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014 , os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos:
>
> I - tão logo atingida a finalidade de seu uso; ou
>
> II - se encerrado o prazo determinado por obrigação legal.

A segurança das informações é uma constante na legislação, e o Decreto nº 9.637, de 26 de dezembro de 2018 (BRASIL, 2018b) institui a Política Nacional de Segurança da Informação, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação a nível nacional, baseado em inúmero princípios, dentro os quais a soberania nacional. Nesse decreto é atribuído ao Gabinete de Segurança Institucional da Presidência da República a competência de "aprovar diretrizes, estratégias, normas e recomendações nos temas relacionados à segurança da informação" (BRASIL, 2018b, art.12,inciso II) e

> "estabelecer os requisitos mínimos de segurança para o uso dos produtos que incorporem recursos de segurança da informação, de modo a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação e garantir a interoperabilidade entre os sistemas de segurança da informação, ressalvadas as competências específicas de outros órgãos." (BRASIL, 2018b, art.12,inciso IX)

4.3 Instruções Normativas

Em decorrência do Princípio da separação de poderes presente na Constituição de 1.988, em seu artigo 2º, que dispõe que são Poderes da União, independentes e harmônicos entre si, o Legislativo, o Executivo e o Judiciário, o Senado Federal não se sujeita as regulamentações expedidas pelo Poder Executivo na forma de Portarias, Instruções Normativas e Normas Complementares, contudo, neste estudo, o que não contrariar norma emitida pelo próprio Poder Legislativo, iremos considerar como uma boa prática.

Foram elencadas no Quadro 22 do Apêndice A, página 173, as Instruções Normativas que serão analisadas nessa seção 4.3.

4.3.1 Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008

A Instrução Normativa GSI/PR nº 1 é uma instrução que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, mas que não apresenta no seu bojo nenhuma recomendação que deva ser aplicada diretamente para a formação dos critérios de contração de serviços de computação em nuvem. As suas normas complementares são o que efetivamente regulam a Gestão de Segurança da Informação e Comunicações e por isso são o objeto de estudo e serão detalhadas na seção 4.4.

4.3.2 Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013

A Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013 dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.

No Art. 2º temos duas definições importantes para entendermos a aplicabilidade desta Instrução Normativa para os serviços de computação em nuvem, que são:

> XIII - Órgãos de Registro nível 1: os Ministérios e os órgãos e entidades públicos de nível equivalente, credenciados pelo Núcleo de Segurança e Credenciamento;
>
> [...]
>
> XV - Postos de Controle: unidade de órgão ou entidade pública ou privada, habilitada, responsável pelo armazenamento de informação classificada em qualquer grau de sigilo;

(BRASIL, 2013b, Art 2º, Incisos XIII e XV)

A instrução normativa atribui ao Órgão de Registro nível 1 a competência de " habilitar Posto de Controle dos órgãos e entidades públicas ou privadas que com ele mantenham vínculo de qualquer natureza, para o armazenamento de informação classificada em qualquer grau de sigilo;" (BRASIL, 2013b, Art 4º, incisoII), e ao Posto de Controle de:

> I - armazenar e controlar as informações classificadas, inclusive as credenciais de segurança, sob sua responsabilidade;
>
> II - manter a segurança lógica e física das informações classificadas, sob sua guarda;
>
> IV - encaminhar, periodicamente, ao Órgão de Registro que o credenciou relatórios de suas atividades;
>
> V - notificar o Órgão de Registro que o credenciou, imediatamente, quando da quebra de segurança das informações classificadas por ele custodiadas; (BRASIL, 2013b, art 6º)

No caso do serviço de computação em nuvem, se algum órgão armazenar informação classificada em qualquer grau de sigilo na nuvem, isso faz com que o provedor de nuvem seja um posto de controle, já que o mesmo estará responsável pelo armazenamento da informação. Sendo assim, os contratos com esses provedores devem lhes atribuir as competências elencadas no artigo 6º.

Os artigos 7º, 15º, 21º e 24º citados abaixo, devem ser considerados na formulação dos contratos com os provedores de nuvem, já que exigem que haja controle de acesso, áreas restritas e informações tempestivas sobre quebras de segurança.

> Art. 7º O acesso, a divulgação e o tratamento de informação classificada em qualquer grau de sigilo ficarão restritos a pessoas que tenham necessidade de conhecê-la e que tenham Credencial de Segurança segundo as normas fixadas pelo GSI/PR, por intermédio do NSC, sem prejuízo das atribuições de agentes públicos autorizados por Lei.
>
> Parágrafo único. O acesso à informação classificada em qualquer grau de sigilo à pessoa não credenciada ou não autorizada por legislação poderá, excepcionalmente, ser permitido mediante assinatura de Termo de Compromisso de Manutenção de Sigilo - TCMS, conforme Anexo I do Decreto no 7.845, de 2012, pelo qual a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da Lei.
>
> [...]
>
> Art. 15 As áreas e instalações que contenham documento com informação classificada em qualquer grau de sigilo, ou que, por sua utilização ou finalidade, demandarem proteção, terão seu acesso restrito às pessoas autorizadas pelo órgão ou entidade. Parágrafo único. As áreas ou instalações do Posto de Controle de cada órgão de registro e de entidades privadas são consideradas de acesso restrito.
>
> [...]

> Art. 21. Na hipótese de troca e tratamento de informação classificada em qualquer grau de sigilo, com país ou organização estrangeira, o credenciamento de segurança no território nacional, se dará somente se houver tratado, acordo, memorando de entendimento ou ajuste técnico firmado entre o país ou organização estrangeira e a República Federativa do Brasil.
>
> [...]
>
> Art. 24. Toda quebra de segurança de informação classificada, em qualquer grau de sigilo, deverá ser informada, tempestivamente, pela Alta Administração do órgão ou entidade ao GSI/PR, relatando as circunstâncias com o maior detalhamento possível
>
> (BRASIL, 2013b, Artigos 7º, 15, 21 e 24)

4.3.3 Instrução Normativa GSI/PR nº 3, de 06 de março de 2013

A Instrução Normativa GSI/PR nº 3, de 06 de março de 2013 dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.

No artigo 2º são feitas diversas definições, em especial, a de Algoritmo de Estado, como "função matemática utilizada na cifração e na decifração, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades do Poder Executivo Federal" (BRASIL, 2013c, art. 2º, inciso II).

Uma questão a ser avaliada é se é necessário no Poder Legislativo fazer uso de Algoritmo de Estado, ou se um algoritmo de criptografia de mercado pode ser utilizado, desde que atenda aos padrões da NC 09/IN01/DSIC/GSI/PR (Revisão 01) como requerido pelo artigo 4º:

> Art. 4º A cifração e decifração de informações classificadas, em qualquer grau de sigilo, devem utilizar recurso criptográfico baseado em algoritmo de Estado em conformidade com os padrões e parâmetros mínimos estabelecidos na NC 09/IN01/DSIC/GSI/PR (Revisão 01), de fevereiro de 2013 (BRASIL, 2013c, art. 4º)

Caso se entenda que o Senado Federal deve utilizar Algoritmo de Estado, deverá também aplicar o previsto no artigo 5º:

> Art. 5º O recurso criptográfico baseado em algoritmo de Estado deverá ser de desenvolvimento próprio ou por órgãos e entidades do Poder Executivo Federal, mediante acordo ou termo de cooperação, vedada a participação e contratação de empresas e profissionais externos, para tal finalidade.
>
> § 1º Excepcionalmente, com anuência da Alta Administração do órgão ou entidade, o previsto no caput poderá ser terceirizado, desde que atendidas obrigatoriamente as seguintes condições:
>
> I - seja realizado exclusivamente por meio de Contrato Sigiloso, nos termos dos arts. 48 e 49 do Decreto no 7.845, de 14 de novembro de 2012;

> II - seja previsto em cláusula contratual que fica vedado ao contratado os direitos de propriedade e de exploração comercial, do recurso criptográfico com algoritmo de estado, objeto do presente contrato;
>
> (BRASIL, 2013c, art. 5º)

Segundo o artigo 6º, dentre as competências da Alta Administração dos órgãos e entidades do Poder Executivo Federal estão:

> IV - prever explicitamente nos entendimentos, contratos, termos ou acordos de aquisição e manutenção de equipamentos, dispositivos móveis, sistemas, aplicativos ou serviços que disporão de recurso criptográfico baseado em algoritmo de Estado, o fiel cumprimento do disposto na presente Instrução Normativa, sem prejuízo da legislação vigente; (BRASIL, 2013c, Art. 6º, Inciso IV)

> VI - informar ao GSI/PR, tempestivamente, o comprometimento do sigilo de qualquer recurso criptográfico baseado em algoritmo de Estado;
>
> (BRASIL, 2013c, Art. 6º, Inciso VI)

Apesar da norma estar explicitamente definindo competências para os órgãos e entidades do Poder Executivo Federal, a preocupação com a correta utilização dos recursos criptográficos e a informação tempestiva de quebra de sigilo são aspectos que se deve levar em conta na contratação de serviços em nuvem em qualquer esfera de poder.

> Art. 9º Todo recurso criptográfico baseado em algoritmo de Estado constitui material de acesso restrito e requer procedimentos especiais adequados de controle para o seu acesso, manutenção, armazenamento, transferência, trânsito e descarte, em conformidade com a legislação vigente, sob pena de responsabilização da Alta Administração.
>
> Parágrafo único. O Gestor de Segurança da Informação e Comunicações e todo Agente Responsável, usuários de recurso criptográfico baseado em algoritmo de Estado, devem possuir credencial de segurança, ou excepcionalmente, assinar o Termo de Compromisso de Manutenção de Sigilo - TCMS, conforme Anexo I do Decreto n o 7.845, de 14 de novembro de 2012. (BRASIL, 2013c, Art. 9º)

4.3.4 Instrução Normativa nº 1, de 4 de abril de 2019

Nos estudos citados na página 47 é constante a menção à Instrução Normativa SLTI/MP 4/2014, contudo, quando da elaboração deste estudo, a mesma já havia sido revogada pela Instrução Normativa nº 1, de 4 de abril de 2019 da Secretaria de Governo Digital do Ministério da Economia, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação – TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP do Poder Executivo Federal.

A IN 1/2019 regulamenta todos os aspectos comuns da contratação de serviços de TI em geral no âmbito do Poder Executivo, e suas predecessoras têm sido utilizadas como "Boas Práticas de Contratação de TI". Por isso, mesmo não sendo de aplicação vinculada ao Poder Legislativo, será adotada como fonte na elaboração dos critérios de contratação de serviços em computação em nuvem para o Senado Federal.

Diferentemente das suas predecessoras que não tinham nenhuma referência à contratação de serviços em nuvem, a IN 1/2019 traz em seu anexo as seguintes diretrizes:

> DIRETRIZES ESPECÍFICAS DE PLANEJAMENTO DA CONTRATAÇÃO
>
> 4. CONTRATAÇÃO DE INFRAESTRUTURA DE CENTRO DE DADOS, SERVIÇOS EM NUVEM, SALA-COFRE E SALA SEGURA:
>
> 4.1. Os órgãos e entidades que necessitem criar, ampliar ou renovar infraestrutura de centro de dados deverão fazê-lo por meio da contratação de serviços de computação em nuvem, salvo quando demonstrada a inviabilidade em estudo técnico preliminar da contratação.
>
> 4.2. As contratações de serviços em nuvem devem observar o disposto na Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, e suas Normas Complementares, notadamente a Norma Complementar 14/IN01/DSIC/SCS/GSIPR.
>
> 4.2.1. Os órgãos e entidades devem exigir mediante justificativa prévia, no momento da assinatura do contrato, que fornecedores privados de serviços em nuvem possuam certificações de normas de segurança da informação aplicáveis ao objeto da contratação, assim como outros requisitos que objetivem mitigar riscos relativos à segurança da informação.
>
> 4.2.2. Os órgãos e entidades devem assegurar, por meio de cláusulas contratuais, que os serviços em nuvem a serem contratados permitirão a portabilidade de dados e softwares e que as informações do contratante estarão disponíveis para transferência de localização, em prazo adequado.
>
> 4.3. É vedada a contratação para criação ou ampliação de salas-cofre e salas seguras, salvo nos casos em que o órgão ou entidade tenha obtido autorização prévia do Órgão Central do SISP.
>
> 4.3.1. Considera-se sala segura sistema modular composto por painéis remontáveis, formando um ambiente autoportante e estanque para proteção física de equipamentos de hardware, construído no interior da edificação existente, podendo ser ampliado ou removido e remontado em outro local, preservando suas características de proteção. Esse ambiente inclui sistemas de infraestrutura elétrica, de climatização, de monitoramento ambiental, de detecção e alarme de incêndio e demais subsistemas relacionados à proteção contra ameaças físicas.
>
> 4.3.2. Considera-se sala cofre ambiente que possui todas as características de uma sala segura, devendo ser certificado pela norma ABNT NBR 15.247 (Unidades de armazenagem segura - Salas-cofre e cofres para hardware - Classificação e métodos de ensaio de resistência ao fogo).
>
> (BRASIL, 2019, Anexo)

A vedação expressa no item 4.3, citado acima, é uma iniciativa do governo brasileiro de adotar um programa semelhante ao *Cloud First* do governo americano, que foi uma política que pretendia acelerar o ritmo de adoção de computação em nuvem pelos órgãos

governamentais, ao exigir que as agências avaliassem opções de computação em nuvem seguras e protegidas antes de fazer novos investimentos.

A IN 1/2019 divide ainda as contratações de TIC em três fases: Planejamento da Contratação, Seleção do Fornecedor e Gestão do Contrato (BRASIL, 2019, art. 8º). Dessa forma, os critérios elaborados neste estudo serão divididos de acordo com as fases das contratações de TIC e procuraram servir de guia para a contratação de serviços em nuvem.

4.4 Normas Complementares

As normas complementares que analisaremos nesta seção 4.4 foram elencadas no Quadro 23 do Apêndice A, página 173, e são complementares à Instrução Normativa GSI/PR nº 1 que foi analisada na subseção 4.3.1.

4.4.1 Norma Complementar nº 06/IN01/DSIC/GSIPR

A NC nº 06/IN01/DSIC/GSIPR estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações e procura normatizar a continuidade de negócios na Administração Pública Federal.

Com relação à contratação de serviços em computação em nuvem, deve ser seguida a sugestão expressa no item 5.7 (BRASIL, 2009, item 5.7)]

> Sugere-se que os contratos firmados com empresas terceirizadas que suportem atividades críticas contenham cláusula segundo a qual as referidas empresas possuam Planos de Continuidade dos seus Negócios, bem como as evidências dos testes realizados.

4.4.2 Norma Complementar nº 07/IN01/DSIC/GSIPR

A NC nº 07/IN01/DSIC/GSIPR estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta e foi baseada na NBR ISO/IEC 27001:2013 e na NBR ISO/IEC 27002:2013.

Quanto ao acesso lógico aos ativos de informação a norma estabelece no item 6.3 que devem:

> 6.3.1. Conter ferramentas de proteção contra acesso não autorizado aos ativos de informação, que favoreça, preferencialmente, a administração de forma centralizada.
>
> 6.3.2. Respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação;
>
> 6.3.3. Utilizar ativo de informação homologado nas aplicações de controle de acesso, de tratamento das informações sigilosas e de criptografia;

> 6.3.4. Registrar eventos relevantes, previamente definidos, para a segurança e rastreamento de acesso às informações sigilosas.
>
> 6.3.5. Criar mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.
>
> (BRASIL, 2014b, item 6.3)

Quanto ao acesso físico dos dos ativos de informação a norma estabelece no item 7.3 que devem, entre outras:

> 7.3.1. Estabelecer distância mínima de segurança para manutenção das mídias contendo as cópias de segurança (backups);
>
> 7.3.2. Classificar os ativos de informação em níveis de criticidade, considerando o tipo de ativo de informação, o provável impacto no caso de quebra de segurança, tomando como base a gestão de risco e a gestão de continuidade de negócios relativa aos aspectos da segurança da informação e comunicações da APF,
>
> [...]
>
> 7.3.4. Os ativos de informação classificados como sigilosos requerem procedimentos especiais de controles de acesso físico em conformidade com a legislação vigente.
>
> (BRASIL, 2014b, item 7.3)

4.4.3 Norma Complementar nº 14/IN01/DSIC/GSIPR

A NC nº 14/IN01/DSIC/GSIPR é uma norma específica para a utilização de tecnologias de Computação em nuvem e será essencial neste estudo. Ela estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Segundo a norma, qualquer órgão ou entidade da APF ao adotar Computação em Nuvem deve observar, no mínimo:

> 5.1.1 A prevalência dos direitos e garantias fundamentais no tratamento das informações pessoais;
>
> 5.1.2 As diretrizes estabelecidas em sua Política de Segurança da Informação e Comunicações (POSIC) e normas complementares;
>
> 5.1.3 As diretrizes relativas à sua Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC);
>
> 5.1.4 As informações tratadas em ambiente de computação em nuvem devem passar por um processo de GRSIC;
>
> 5.1.5 As diretrizes relativas à sua Gestão de Continuidade, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC);
>
> 5.1.6 As legislações vigentes para contratação de Solução de Tecnologia da Informação;
>
> 5.1.7 As legislações vigentes relativas à Gestão de Segurança da Informação e Comunicações;
>
> 5.1.8 As diretrizes para implementação de controles de acesso relativos à SIC; e
>
> 5.1.9 A prevalência da legislação brasileira sobre qualquer outra.

O TCU no acórdão 1.739/2015 faz a seguinte ressalva:

> 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.
>
> (BRASIL. TCU, 2015, parágrafo 140)

Segundo a NC nº 14/IN01/DSIC/GSIPR, deve haver também a garantia quanto ao tratamento da informação de acordo com os seguintes critérios:

> 5.2.1 Informação sem restrição de acesso: pode ser tratada, a critério do órgão ou entidade da APF, em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC;
>
> 5.2.2 Informação sigilosa: como regra geral, deve ser evitado o tratamento em ambiente de computação em nuvem, conforme disposições a seguir:
>
> 5.2.2.1. Informação classificada: é vedado o tratamento em ambiente de computação em nuvem;
>
> 5.2.2.2. Conhecimento e informação contida em material de acesso restrito: é vedado o tratamento em ambiente de computação em nuvem;
>
> 5.2.2.3. Informação com restrição de acesso prevista em legislação vigente: a critério do órgão ou entidade da APF, pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. O órgão ou entidade da APF deve adotar medidas que assegurem a **disponibilidade**, **integridade**, **confidencialidade** e **autenticidade** (**DICA**) (grifo nosso);
>
> 5.2.2.4. Documento Preparatório: a critério do órgão ou entidade da APF, pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. O órgão ou entidade da APF deve adotar medidas que assegurem a DICA;
>
> 5.2.2.5. Documento preparatório que possa originar informação classificada deve ser tratado conforme o item 5.2.2.1; e
>
> 5.2.2.6. Informação pessoal relativa à intimidade, vida privada e imagem: a critério do órgão ou entidade da APF, pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. O órgão ou entidade da APF deve adotar medidas que assegurem a DICA.

O item 5.3 da NC nº 14/IN01/DSIC/GSIPR estabelece que "dados, metadados, informações e conhecimento, produzidos ou custodiados por órgão ou entidade da APF, bem como suas cópias de segurança, residam em território brasileiro"(BRASIL, 2018d, item 5.3), e o item 5.4 reforça ainda que as informações referentes aos itens 5.2.2.3, 5.2.2.4 e 5.2.2.6, devem residir exclusivamente em território brasileiro;

Ao adotar serviços de computação em nuvem, o órgão ou entidade da APF deve garantir a definição em instrumento contratual dos seguintes itens:

> 5.5.1 Requisitos que garantam a DICA das informações tratadas em ambiente de computação em nuvem;
>
> 5.5.2 Processo de comunicação e tratamento de incidentes de segurança em redes computacionais, considerando as exigências da legislação vigente;
>
> 5.5.3 Requisitos necessários para a realização de auditorias;
>
> 5.5.4 Que os dados, metadados, informações e conhecimento, tratados pelo provedor, não poderão ser fornecidos a terceiros e/ou usados por este provedor para fins diversos do previsto no referido instrumento contratual ou similar, sob nenhuma hipótese, sem autorização formal do órgão ou entidade da APF;
>
> 5.5.5 Requisitos necessários para a continuidade de negócio;
>
> 5.5.6 Requisitos necessários, para os casos de cancelamento, descontinuidade, portabilidade e renovação do referido instrumento contratual ou similar, bem como substituição de ambiente, que visem à eliminação e/ou à destruição definitiva dos dados, metadados, informações e conhecimento; e
>
> 5.6 É vedado o tratamento de informação em ambientes de computação em nuvem não autorizados pela Alta Administração do respectivo órgão ou entidade da APF. (BRASIL, 2018d)

A vedação presente no item 5.6 leva em consideração que a Alta Administração de cada órgão ou entidade entidade da APF é responsável pela segurança das informações tratadas em ambiente de computação em nuvem, e que o Gestor de Segurança da Informação e Comunicação do órgão é responsável pelas ações de implementação da gestão de risco de segurança das informações tratadas em ambiente de computação em nuvem.

4.4.4 Norma Complementar nº 19/IN01/DSIC/GSIPR

A NC nº 19/IN01/DSIC/ GSIPR define que as soluções de infraestrutura em nuvem para os Sistemas Estruturantes[6] deverão adotar somente os modelos de implementação de Nuvem Própria ou de Nuvem Comunitária, em todos os modelos de serviços desde que restritas às infraestruturas de órgãos ou entidades da administração pública federal (BRASIL, 2014c, item 4.2.3).

4.4.5 Norma Complementar nº 21/IN01/DSIC/GSIPR

A NC Nº 21/IN01/DSIC/ GSIPR estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta. Destaca-se o item 6 desta norma, que deve ser considerado na elaboração do modelo de contratação de serviços em nuvem, em especial o item 6.1:

[6] 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

> 6.1 O horário dos ativos de informação deve ser ajustado por meio de mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a "Hora Legal Brasileira (HLB)", de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).
>
> (BRASIL, 2014d, item 6)

Deve-se garantir ainda que os ativos de informação sejam configurados de forma a registrar todos os eventos relevantes de SIC, que o provedor de serviços em nuvem tenha procedimentos para coleta e preservação de evidências, e que os incidentes de segurança em redes sejam reportados aos órgãos e entidades da Administração Pública Federal.

4.5 Outros Normativos e documentos

Ao decorrer desta seção serão analisados os documentos e normativos apresentados no Quadro 24 do Apêndice A na página 174, como acórdãos, portarias e normas técnicas e manuais de boas práticas.

4.5.1 Acórdão (TCU) 1.739/2015

O Acórdão nº 1.739/2015 do TCU teve como objetivo:

> 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.
>
> (BRASIL. TCU, 2015, parágrafo 6)

O Acórdão é um trabalho extenso e aprofundado sobre a computação em nuvem e os riscos associados, que teve seu fundamento no relatório da SEFTI. No relatório em seu Anexo II foi apresentada uma matriz de auditoria, onde estão relacionadas questões de auditoria, critérios e procedimentos para as fiscalizações do TCU, que foram apresentadas no Quadro 1.

Quadro 1 – Matriz de auditoria de contratação de serviços de computação em nuvem

Questão de Auditoria
1. A gestão da segurança da informação, o controle dos ativos e os riscos de segurança relativos à adoção de cloud foram tratados de forma efetiva pela organização?

Continua na próxima página

Quadro 1 – Continuação

Questão de Auditoria
2. Os mecanismos de governança de TI foram revistos, adaptados e implementados adequadamente, de maneira a abranger a adoção de computação em nuvem e gerenciar riscos inerentes à cloud?
3. Foram definidos dispositivos contratuais e mecanismos de gestão contratual adequados para a contratação de serviços de computação em nuvem?
4. Foram abordados e endereçados adequadamente aspectos e processos de gestão relacionados à arquitetura e infraestrutura de computação em nuvem?

Fonte: (TCU, 2015, Anexo II)

As questões acima, procuram responder se e como os órgãos trataram os riscos que foram identificados no Acórdão, e que servirão de subsídios para a elaboração dos critérios de contratação de serviços em nuvem no SF. Os riscos foram apontados pelo TCU na Tabela 4 – Riscos de contratação de serviços de computação em nuvem, que se encontra dividida nesta seção em quadros, cada um relacionado a um dos temas elencados pelo TCU.

No Quadro 2, estão os riscos do tema "Segurança da Informação", no Quadro 3 os relativos à "Governança e gestão de riscos", no Quadro 4 os relativos à "Contratação e gestão contratual" e no Quadro 5 os relativos à "Infraestrutura de TI".

Quadro 2 – Riscos de contratação de serviços de computação em nuvem - Segurança da Informação

Descrição
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

Continua na próxima página

Quadro 2 – Continuação

Descrição
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

Fonte: (BRASIL. TCU, 2015, Tabela 4)

Quadro 3 – Riscos de contratação de serviços de computação em nuvem - Governança e gestão de riscos

Descrição
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

Fonte: (BRASIL. TCU, 2015, Tabela 4)

Deve-se atentar para o fato de que o risco 24 não será considerado pelo fato do Decreto 8.135/2013 ter sido revogado.

Quadro 4 – Riscos de contratação de serviços de computação em nuvem - Contratação e gestão contratual

Descrição
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

Continua na próxima página

Quadro 4 – Continuação

Descrição
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

Fonte: (BRASIL. TCU, 2015, Tabela 4)

Quadro 5 – Riscos de contratação de serviços de computação em nuvem - Infraestrutura de TI

Descrição
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

Fonte: (BRASIL. TCU, 2015, Tabela 4)

Os riscos apresentados endereçam não somente aqueles decorrentes da contratação dos serviços em nuvem e sua gestão, como também, questões do próprio planejamento estratégico e orçamentário do órgão para suportar a adoção da tecnologia de computação

em nuvem.

4.5.2 Acórdão (TCU) 2.659 /2018

O Acórdão do TCU 2.659/2018 (BRASIL. TCU, 2018) foi resultado de fiscalização do tipo auditoria operacional, conforme previsto no art. 239 do Regimento Interno do Tribunal de Contas da União (RITCU) e no art. 1º da Portaria - Segecex 4/2010 e o seu objeto era avaliar as práticas comerciais adotadas por grandes fabricantes de tecnologia da informação (TI) na relação com a Administração Pública, quando da contratação de licenciamento de *software* e seus serviços agregados.

Durante os levantamentos das contratações de licenciamento de *software*, o TCU considerou oportuno avaliar o impacto que a contratação de serviços em nuvem pode trazer a essas contratações no âmbito da APF, especialmente porque a comercialização de *softwares* como serviço tem se tornado prática cada vez mais adotada pelos fabricantes (BRASIL. TCU, 2018, parágrafos 6 e 36).

O TCU chama a atenção para o fato de que "o Gartner Group prevê que, até o ano de 2020, 80% dos fabricantes irão mudar para um modelo baseado em serviço" (BRASIL. TCU, 2018, parágrafo 374), o que possivelmente irá gerar uma pressão dos fabricantes para que os clientes migrem para esse novo modelo.

Ainda segundo o TCU, a mudança de modelo já é percebida também pelas organizações auditadas, como o Banco do Brasil, a Eletrobras, o Serpro e o Tribunal Regional da 1ª Região (TRF1). Pois segundo eles, já existem fabricantes que oferecem alguns de seus *softwares* apenas na modalidade de assinatura ou em nuvem, como são os casos da Adobe, Red Hat e VMware. Ressalta ainda que, Oracle e Microsoft informaram que "o foco das empresas e o desenvolvimento de soluções estão voltados aos serviços em nuvem, sendo que uma transição significativa para o novo modelo deverá ocorrer em poucos anos" (BRASIL. TCU, 2018, parágrafo 375). Porém, o Acórdão alerta para os riscos que os novos modelos de comercialização podem trazer, entre eles: valores elevados das subscrições; a dificuldade para portabilidade em função da heterogeneidade de tecnologias; e um aumento da dependência em relação aos fabricantes (BRASIL. TCU, 2018, parágrafo 376).

O Acórdão ressalta que "as organizações auditadas encontram dificuldades para enfrentar os riscos relacionados aos novos modelos de comercialização de software, em especial também em relação à conformidade das contratações" (BRASIL. TCU, 2018, parágrafo 379). Segundo o Acórdão, no entendimento do Serpro, há uma mudança de paradigma, já que o modelo inverte a lógica das licitações, ao pagar pelo consumo ao invés de comprar para depois usar. Outro dificultador é a regra de limitação de empenho prevista na legislação que se opõe ao princípio da elasticidade, que é um dos grandes benefícios da nuvem. Assim também apontou o CNJ, acrescentando a dificuldade de que o

empenho pode ser muito superior ou inferior ao valor efetivamente utilizado.

O Acórdão conclui que:

> "há risco de as organizações públicas não estarem preparadas tempestivamente para mudança ampla nas formas de comercialização motivada por fatores externos, em função de aspectos orçamentários, de conformidade com normativos e de dificuldades para operacionalizar modelo eficiente de gestão baseado em software como serviço" (BRASIL. TCU, 2018, parágrafo 388).

As principais causas apontadas são:

> a) Não há experiências consistentes de adoção de software baseados totalmente em serviços ou no modelo de computação em nuvem pela Administração Pública;
>
> b) Falta orientação aos gestores sobre o marco legal aplicável à contratação de serviços baseados em computação em nuvem, que receiam incorrer em alguma ilegalidade;
>
> c) Dificuldades de estabelecer modelos de contratação por falta padronização no mercado sobre formas de comercialização de serviços baseados em computação em nuvem.

Por esses motivos, estão entre as recomendações do Acórdão o aprimoramento das orientações já existentes sobre contratação de Serviços de Computação em Nuvem, endereçando as questões identificadas sobre contratações de software baseadas em modelos voltados totalmente para serviços, inclusive com a elaboração de padrões para as aquisições e a avaliação do impacto orçamentário e financeiro das contratações de software baseadas nesses modelos de forma a subsidiar o planejamento para a mudança na forma de custeio da TI governamental ao longo dos anos.

4.5.3 Portaria MP/STI nº 20 , de 14 de junho de 2016 e Anexo "Boas Práticas, Orientações e Vedações para Contratação de Serviços de Computação em Nuvem"

A Portaria MP/STI nº 20 , de 14 de junho de 2016 dispõe sobre orientações para contratação de soluções de Tecnologia da Informação no âmbito da APF e apresenta Boas Práticas para contratação de diversos itens. Para este estudo, o foco é o documento chamado "Boas Práticas, Orientações e Vedações para Contratação de Serviços de Computação em Nuvem".

Todos os 12 itens apresentados devem ser considerados na elaboração do modelo. Percebe-se que o documento se baseia na legislação e normas que foram referenciadas neste estudo, mas incorpora algumas recomendações mais práticas, das quais ressaltamos as seguintes:

> 1. Fica vedada a contratação de salas-cofre e salas seguras por órgãos integrantes do SISP.
>
> i. Solicitações de excepcionalização ao disposto no caput deverão ser submetidas pelo órgão, com as devidas justificativas, à apreciação da STI.
>
> [...]
>
> 4. Os órgãos deverão exigir, no momento da contratação de serviços em nuvem de fornecedores privados, que o ambiente do serviço contratado esteja em conformidade com a norma ABNT NBR ISO/IEC 27001:2013, sem prejuízo de outras exigências, objetivando mitigar riscos relativos à segurança da informação.
>
> [...]
>
> 6. A contratação de serviços em nuvem deverá respeitar a seguinte ordem de prioridade, quanto a capacidade de serviços que possa atender as necessidades do contratante: i. Software como Serviço (SaaS); ii. Plataforma como Serviço (PaaS); iii. Infraestrutura como Serviço (IaaS).
>
> [...]
>
> 10. Na contratação de serviços em nuvem com empresas privadas os órgãos deverão exigir disponibilidade de no mínimo, 99,741% para os data centers onde os serviços estarão hospedados, aceita a comprovação por meio de certificação TIA 942 Tier II.
>
> (BRASIL. MP, 2016b)

4.5.4 ABNT NBR ISO/IEC 27001:2013

A ABNT NBR ISO/IEC 27001:2013 (ABNT, 2013a) especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Essa Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização.

A ISO 27001 é uma norma de gestão, isto é, define como administrar um sistema, no caso o sistema de gestão da segurança de informação (SGSI). Sendo uma norma de gestão, é possível para as empresas tirarem certificação.

A certificação ISO 27001 garante que a empresa implementou controles para proteger a confidencialidade, integridade e disponibilidade da informação. Isso é feito por meio de avaliação de risco e procedimentos de mitigação e/ou tratamento de risco.

No Anexo A da norma são descritos 114 controles divididos em 14 seções. No Quadro 6, vemos como estão divididas as seções e seus objetivos. Percebe-se que os controles atendem a diversos quesitos que foram levantados em relação às Instruções Normativas do GSI/PR e suas Normas Complementares, o que simplifica o modelo a ser desenvolvido, sendo necessário apenas exigir que o provedor de serviços em nuvem tenha a Certificação ISO 27001, para garantir que o mesmo esteja em conformidade com os normativos.

Quadro 6 – Seções e subseções dos controles da ABNT NBR ISO/IEC 27001:2013

Seção	Subseção
A.5 Políticas de segurança da informação	A.5.1 Orientação da Direção para segurança da Informação
A.6 Organização da segurança da informação	A.6.1 Organização interna A.6.2 Dispositivos móveis e trabalho remoto
A.7 Segurança em Recursos humanos	A.7.1 Antes da contratação A.7.2 Durante a contratação A.7.3 Encerramento e mudança da contratação
A.8 Gestão de ativos	A.8.1 Responsabilidade pelos ativos A.8.2 Classificação da informação A.8.3 Tratamento de mídias
A.9 Controle de acesso	A.9.1 Requisitos do negócio para controle de acesso A.9.2 Gerenciamento de acesso do usuário A.9.3 Responsabilidade dos usuários A.9.4 Controle de acesso ao sistema e à aplicação
A.10 Criptografia	A.10.1 Controles criptográficos
A.11 Segurança física e do ambiente	A.11.1 Áreas Seguras A.11.2 Equipamentos
A.12 Segurança nas operações	A.12.1 Responsabilidades e procedimentos operacionais A.12.2 Proteção contra *malware* A.12.3 Cópias de segurança A.12.4 Registros e monitoramento A.12.5 Controle de software operacional A.12.6 Gestão de vulnerabilidades técnicas A.12.7 Considerações quanto à auditoria de sistema de informação
A.13 Segurança nas comunicações	A.13.1 Gerenciamento da segurança em redes A.13.2 Transferência de informação
A.14 Aquisição, desenvolvimento e manutenção de sistemas	A.14.1 Requisitos de segurança de sistemas de informação A.14.2 Segurança em processos de desenvolvimento e de suporte A.14.3 Dados para teste
A.15 Relacionamento na cadeia de suprimento	A.15.1 Segurança da informação na cadeia de suprimento

Continua na próxima página

Quadro 6 – Continuação

Seção	Subseção
	A.15.2 Gerenciamento da entrega do serviço do fornecedor
A.16 Gestão de incidentes de segurança da informação	A.16.1 Gestão de incidentes de segurança da informação e melhoria
A.17 Aspectos da segurança da informação na gestão da continuidade do negócio	A.17.1 Continuidade da segurança da informação A.17.2 Redundâncias
A.18 Conformidade	A.18.1 Conformidade com requisitos legais e contratuais A.18.2 Análise crítica da segurança da informação

Fonte: (ABNT, 2013a, Anexo A)

4.5.5 ABNT NBR ISO/IEC 27002:2013

A ABNT NBR ISO/IEC 27002:2013 (ABNT, 2013b) fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

As normas ISO 27001 e ISO 27002 são muitos semelhantes, sendo a ISO 27002 mais detalhada. Cabe ressaltar ainda que a ABNT NBR ISO/IEC 27002:2013 não é uma norma de gestão, não sendo possível para as organizações se certificarem nesta norma, contudo, é possível a certificação por profissionais.

4.5.6 ABNT NBR ISO/IEC 27017:2016

A ABNT NBR ISO/IEC 27017:2016 (ABNT, 2016) fornece diretrizes para os controles de segurança da informação aplicáveis à prestação e utilização de serviços em nuvem, fornecendo o seguinte: diretrizes adicionais para implementação de controles relevantes especificados na ABNT NBR ISO/IEC 27002; controles adicionais com diretrizes de implementação que são relacionadas especificamente a serviços em nuvem.

A ISO/IEC 27017:2015 define diretrizes para os controles de segurança da informação aplicáveis ao provisionamento e ao uso de serviços de nuvem fornecendo os sete seguintes novos controles com numeração compatível com a estrutura existente da ISO 27001/ISO 27002:

- 6.3.1 Funções e responsabilidades compartilhadas em um ambiente de computação em nuvem;

- 8.1.5 Remoção de ativos de clientes do serviço de nuvem (garantindo a remoção/devolução de ativos quando um contrato é rescindido);
- 9.5.1 Segregação em ambientes de computação virtual;
- 9.5.2 Configuração de máquina virtual;
- 12.1.5 Segurança operacional do administrador;
- 12.4.5 Monitoramento de serviços em nuvem;
- 13.1.4 Alinhamento do gerenciamento de segurança para redes virtuais e físicas.

Esse padrão é relevante para organizações que fornecem serviços baseados em nuvem e para qualquer organização que armazene informações na nuvem.

Qualquer provedor de nuvem que receba dados confidenciais do cliente e que observa a ISO 27017 se beneficia deste uso, já que, entre outros controles, existe a definição de funções e responsabilidades dentro de um ambiente de computação em nuvem, além disso, a utilização da norma ajuda a reduzir o risco inerente aos serviços em nuvem e o custo potencial de uma violação.

Deve-se considerar a exigência da Certificação ISO 27017 na definição do modelo de contratação a ser proposto.

4.5.7 ABNT NBR ISO/IEC 27018:2018

A ABNT NBR ISO/IEC 27018:2018 (ABNT, 2018) estabelece objetivos de controle, controles e diretrizes comumente aceitos para implementação de medidas para proteger as Informações de Identificação Pessoal (PII) de acordo com os princípios de privacidade descritos na ISO/IEC 29100, para o ambiente de computação em nuvem pública.

A ISO 27018 fornece os seguintes controles para complementar aqueles definidos dentro da ISO 27001 e ISO 27002:

a) direitos de controle do cliente e do usuário final;

b) restrição à divulgação ou acesso de terceiros a PII;

c) tratamento de mídia contendo PII.

Abaixo estão descritos os padrões publicados pela ISO que os serviços de nuvem pública devem cumprir:

a) os dados pessoais devem ser processados de acordo com as instruções do cliente;

b) o consentimento válido deve ser obtido antes de usar as informações pessoais de um indivíduo para marketing ou publicidade;

c) deve-se ajudar os clientes a atender solicitações quando os indivíduos reivindicam seu direito de acessar seus dados;

d) a informação só deve ser dada aos órgãos de aplicação da lei quando legalmente obrigados a fazê-lo;

e) antes de permitir que um cliente entre em um contrato de nuvem, deve-se divulgar os nomes de todos os sub-processadores e os locais onde os dados pessoais podem ser processados;

f) se ocorrer uma violação de dados, deve-se ajudar os clientes a reportá-la aos órgãos responsáveis pela aplicação da lei. Ter planos para quando as violações de dados ocorrem facilita a continuidade dos negócios;

g) políticas devem estar em vigor para retornar, transferir e descartar dados pessoais com segurança;

h) deve-se conduzir revisões de segurança independentes em intervalos programados;

i) é sua responsabilidade garantir que os funcionários que têm acesso a dados pessoais assinem acordos de confidencialidade e sejam treinados adequadamente.

A exigência da Certificação ISO 27018 irá facilitar a implementação e verificação de conformidade com a lei 13.709/2018 (BRASIL, 2018c, LGPD), simplificando os critérios que deverão constar no modelo.

4.6 Conclusão do capítulo

Neste capítulo foram identificadas as legislações e normas vigentes para a contratação de serviços em nuvem na Administração Pública Federal (APF). Foram destacadas as leis, decretos, instruções normativas, normas complementares e outros documentos como acórdãos, portarias, normas técnicas e manuais de boas práticas. Procurou-se apontar em cada um deles os pontos principais a serem considerados na elaboração dos critérios de contratação de serviços em nuvem, de forma a garantir que esses critérios sejam aderentes ao arcabouço jurídico e normativo existente.

No próximo capítulo serão destacados trabalhos acadêmicos que procuraram estudar a adoção da computação em nuvem na APF.

5 Trabalhos Acadêmicos Relacionados

O segundo objetivo específico deste estudo era "Analisar trabalhos acadêmicos relacionados", para tanto, foi realizada uma pesquisa no Google Acadêmico buscando artigos e dissertações que abordassem o tema da contratação de serviços em nuvem no âmbito da Administração Pública Federal, por meio dos termos "Computação em nuvem", "APF" e "governo". Foram selecionados então os trabalhos que mais estavam relacionados com o tema, os quais encontram-se listados no Quadro 25 do Apêndice B, na página 177.

Nesse capítulo se encontram as análises de dois desses trabalhos. Esses trabalhos foram selecionados porque continham pontos que foram julgados relevantes para este estudo após um exame mais apurado.

5.1 Requisitos para a Contratação de Serviços em Computação em Nuvem pela APF

Durante o levantamento de referenciais teóricos, foi encontrada a tese de mestrado "Requisitos para a Contratação de Serviços em Computação em Nuvem pela Administração Pública Federal.", onde Lopes (2015) define requisitos para a contratação de serviços em computação em nuvem, por meio da análise dos normativos vigentes à época. Seus requisitos estão listados no Quadro 7 e tiveram como referências as seguintes normas:

a) NC Nº 14/IN01/DSIC/GSIPR (BRASIL, 2018d);

b) ABNT NBR ISO/IEC 27002:2013 (ABNT, 2013b);

c) Decreto Nº 7.845/2014 artigo 48 (BRASIL, 2012b);

d) Lei 12.527/2011 (BRASIL, 2011);

e) IN GSI/PR Nº 3 (BRASIL, 2013c);

f) IN GSI/PR Nº 2 (BRASIL, 2013b);

g) NC Nº 07/IN01/DSIC/GSIPR (BRASIL, 2014b);

h) NC Nº 21/IN01/DSIC/GSIPR (BRASIL, 2014d).

Quadro 7 – Requisitos para a contratação dos serviços de computação em nuvem pela APF

Nº.	**Requisito**
1	O centro de dados do provedor onde os dados serão hospedados deverá estar instalado no Brasil

Continua na próxima página

Quadro 7 – Continuação

Nº.	**Descrição**
2	Possuir Termo de Compromisso de Manutenção de Sigilo (TCMS) assinado e com os seguintes tópicos: a) Responsabilidades da contratada; b) Obrigação de manter sigilo a todas as informações que possuir acesso; c) Fluxo de acionamento e escalonamento, com o contado dos responsáveis; d) Possibilidade de alteração do objeto para inclusão ou alteração de cláusula de segurança não estipulada previamente; e) Obrigação de adotar procedimentos de segurança adequados, no âmbito das atividades sob seu controle, para a manutenção do sigilo relativo ao objeto; f) Obrigação de receber inspeções para habilitação de segurança e sua manutenção; g) Responsabilidade em relação aos procedimentos de segurança, relativa à subcontratação, no todo ou em parte.
3	Treinamento dos funcionários envolvidos na prestação do serviço na POSIC do órgão e em segurança da informação, com rotinas de atualização periódicas
4	Gerenciamento de acesso com os seguintes itens: a) Política de acesso; b) Processo; c) Controle dos privilégios, respeitando o princípio do menor privilégio; d) Procedimento seguro de entrada;
5	Os dados criptografados devem obedecer aos seguintes requisitos: a) Política de controle e gerenciamento de chaves; b) O algoritmo deve ser baseado no de Estado; c) A criptografia deverá ser fornecida pelo órgão ou excepcionalmente criado pela empresa desde que exista TCMS;
6	As instalações físicas do centro de dados deverão possuir as seguintes características: a) Perímetro demarcado; b) Controle de acesso; c) Possuir proteção física contra desastres naturais, ataques maliciosos ou acidentes.
7	As mudanças relacionadas ao serviço devem ser controladas
8	Possuir controle contra softwares mal-intencionados
9	Realizar cópia de segurança das informações e guarda-las em centro de dados diferentes.

Continua na próxima página

Quadro 7 – Continuação

Nº.	Descrição
10	Registrar os eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos e mantidos de forma automatizada
11	Os sistemas e todos os recursos utilizados por ele deverá possuir o horário sincronizado de forma automática com a Hora Legal Brasileira no Observatório Nacional.
12	As falhas de segurança nos equipamentos, seja por questões inerentes ao mesmo ou por falhas humanas deverão ser tempestivamente comunicadas
13	Os registros de operação e utilização do serviço deverão ser encaminhados periodicamente para a APF

Fonte: Adaptado de Lopes (2015, pp.53–68)

Lopes (2015) afirma em seu trabalho que teve limitações pelo fato de a computação em nuvem ainda ser à época incipiente, e por ter se baseado somente em legislação e normas técnicas. Sugere que o modelo seja submetido à avaliação dos gestores da APF para confirmação dos requisitos e/ou inclusão de requisitos adicionais. Sugere também que seria importante discutir com a equipe que elaborou os editais para verificar porque motivo não foram incluídos todos os requisitos definidos por ele.

5.2 Modelo de avaliação da capacidade das organizações da APF para a adoção de SaaS público

O artigo "Modelo de avaliação da capacidade das organizações da administração pública federal para a adoção de software as a service (SaaS) público" de Wellington Galdino Evangelista e João Souza Neto (EVANGELISTA; SOUZA NETO, 2016) teve como objetivo geral identificar quais são os critérios que devem ser considerados no momento em que uma entidade da administração pública federal (APF) decidir adotar a computação em nuvem. Esses critérios foram divididos em dois quadros, um referente às questões relacionadas à organização, reproduzido abaixo no Quadro 8, e um referente às questões relacionadas à tecnologia, que foi reproduzido no Quadro 9.

Quadro 8 – Questões relacionadas à organização

Operação	Q.1: A área de tecnologia da informação do órgão possui ANS acordados com as áreas de negócio?

Continua na próxima página

Quadro 8 – Continuação

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

Fonte: Evangelista e Souza Neto (2016, p. 193, Quadro 2)

Quadro 9 – Questões relacionadas à tecnologia

Operação	Q. 1: Existe plano de contingência para os negócios em caso de interrupção do funcionamento do aplicativo que os apoia e que será fornecido pelo provedor da nuvem?

Continua na próxima página

Quadro 9 – Continuação

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

Fonte: Evangelista e Souza Neto (2016, p. 194, Quadro 3)

Evangelista e Souza Neto (2016, pp. 199–200) destacam que "o fato de a computação em nuvem ser assunto incipiente na APF, ao mesmo tempo que motivou a pesquisa, foi um fator que limitou as discussões do grupo focal", e sugerem que o trabalho pode ser aplicado em outras pesquisas na área de computação em nuvem no setor público, podendo dessa maneira ser validado, ou até mesmo "pode ser complementado com as ações necessárias para que uma determinada organização possa galgar melhores resultados na avaliação".

5.3 Conclusão do capítulo

Foram consultados diversos artigos e dissertações do meio acadêmico, dos quais foram selecionados por afinidade com o assunto da pesquisa aqueles listadas no Quadro 25 do Apêndice B, que se encontra na página 177. Alguns desses trabalhos serviram como ponto de partida para a pesquisa de legislação aplicada, como foi referenciado na introdução do Capítulo 4, sendo que, os dois trabalhos listados neste capítulo, apresentaram um potencial de serem utilizados com maior profundidade neste trabalho.

O trabalho de Evangelista e Souza Neto permitirá avaliar as ações necessárias a serem incluídas no processo de contratação para aumentar a chance de sucesso da implementação de um serviço de computação em nuvem e o trabalho de Lopes servirá de base para um modelo de avaliação dos editais do TCU e MP, que será o embrião do modelo de contratação de serviços em nuvem para o Senado Federal.

6 Especificidades das contratações do Senado Federal

A Constituição Federal (BRASIL, 2018a), em seu art. 52, determina as competências privativas do Senado Federal. Dentre elas estão no inciso XII a competência de elaborar o seu regimento interno, e no inciso XIII a de **dispor sobre sua organização e funcionamento**. Em virtude dessas competências, o Senado Federal não é obrigado a seguir as instruções normativas e normas complementares instituídas pelos órgãos do Poder Executivo, podendo editar Resoluções, Normas e Atos para regulamentar sua organização e funcionamento.

Em virtude da autonomia normativa do Senado Federal, foi definido como o terceiro objetivo específico deste estudo "Identificar as especificidades das contratações do Senado Federal", para tanto foram levantadas as normas específicas do Senado Federal, que se encontram relacionadas no Quadro 26 do Apêndice C na página 181. Neste capítulo serão apresentados quais são os detalhes das normas específicas do Senado Federal que devem ser considerados na elaboração dos critérios para contratação de serviços em nuvem no âmbito desta Casa Legislativa.

6.1 Resoluções

O primeiro normativo que será analisado é a Resolução nº 13/2018 (SF, 2018), pois a mesma consolida todo Regulamento Administrativo do Senado Federal (RASF), que regula todo o funcionamento interno da parte administrativa do Senado Federal e que em seu Anexo V institui a Política de Contratações do Senado Federal.

Como o Senado Federal não tem que seguir obrigatoriamente a IN 1/2019, não são designadas formalmente, no âmbito do Senado Federal, as equipes de planejamento da contratação. O RASF traz uma característica diferenciada do Senado Federal em relação ao Poder Executivo, que é a existência em sua estrutura de um núcleo que tem como competência a gestão dos contratos de Tecnologia da Informação do Senado Federal, o Núcleo de Gestão e Apoio às Contratações de Tecnologia da Informação (NGACTI). Como podemos perceber em suas atribuições, esse núcleo atua com relação à IN 1/2019 como se fosse o fiscal administrativo da equipe de planejamento da contratação e como gestor e fiscal administrativo dos contratos de TI:

> Art. 215. A Diretoria-Executiva de Contratações tem os seguintes órgãos diretamente subordinados:
>
> [...]

> VI – Núcleo de Gestão e Apoio às Contratações de Tecnologia da Informação.
>
> [...]
>
> VI – ao Núcleo de Gestão e Apoio às Contratações de Tecnologia da Informação compete gerir, ressalvada a competência do Núcleo de Gestão de Contratos de Terceirização, com o auxílio do fiscal e do tomador do serviço, os contratos de Tecnologia da Informação, bem como aqueles designados pela Diretoria-Executiva de Contratações; resolver sobre a padronização de atos de gestão de contratos de TI; orientar e esclarecer os fiscais de contratos de TI sobre a execução dos serviços e as obrigações contratuais; participar, sempre que possível, dos atos preparatórios e conclusivos que resultarão nas contratações sob sua responsabilidade; auxiliar o fiscal ou o usuário tomador do serviço na elaboração de projetos básicos ou termos de referência para novas contratações; alimentar e manter atualizado sistema informatizado de gerenciamento e o Portal da Transparência; verificar a regularidade fiscal das contratadas antes de autorizar pagamentos de faturas, notas fiscais e correlatos; executar outras ações de gestão necessárias ao acompanhamento, à fiscalização e ao controle das atividades desempenhadas pelas contratadas, a fim de garantir o fiel cumprimento das obrigações pactuadas, observados a legislação e regulamentos do Senado Federal; e auxiliar tecnicamente, se necessário, o Núcleo de Gestão de Contratos de Terceirização.

O Anexo V do RASF, estabelece a Política de Contratações do Senado Federal, por meio da qual fica estabelecido que o Senado Federal obedecerá aos limites, valores e percentuais previstos na Lei nº 8.666, de 21 de junho de 1993, bem como em normativo legal ou infralegal, editado pelo Poder Executivo, que vier a substituí-la ou alterá-la.

O Senado Federal também já está alinhado a algumas exigências da IN 1/2019, como o fato de que, a contratação de obra, bens ou serviços deverá integrar o Plano de Contratações do Senado Federal, deve estar alinhada às diretrizes institucionais, ao Plano Estratégico Institucional do Senado Federal e sujeita à programação orçamentária e financeira.

Na Política de Contratações do Senado Federal há cinco atores principais: o Primeiro-Secretário, O Comitê de Contratações, o Diretor-Geral, o Diretor Executivo de Contratações, e a Comissão Permanente de Licitações, que têm suas competências definidas no Anexo V do RASF.

6.2 Atos da Comissão Diretora

A Comissão Diretora do Senado Federal é constituída dos titulares da Mesa Diretora do Senado Federal, que é composta de Presidente, dois Vice-Presidentes e quatro Secretários. Cabe a Comissão Diretora do Senado Federal, entre outras competências, exercer a administração interna do SF, conforme as atribuições definidas no RASF. A Comissão Diretora, em virtude dessa competência, regulamenta as atividades de natureza administrativa por meio dos Atos da Comissão Diretora.

Os Atos da Comissão Diretora que se aplicam a este estudo estão listados no Quadro 26 do Apêndice C, na página 181 e serão discutidos nas subseções seguintes.

6.2.1 Ato da Comissão Diretora nº 2/2008

O Ato da Comissão Diretora (ATC) nº 2/2008 (SF, 2008b) dispõe sobre a gestão de Contratos no Senado Federal e faz as seguintes definições:

> III - gestão de contrato: conjunto de ações e procedimentos destinados a promover o acompanhamento, a fiscalização e o controle efetivo do fiel cumprimento do objeto contratado e das condições pactuadas;
>
> IV - gestor de contrato: servidor que, na condição de representante do Senado Federal, desenvolve, mediante registro próprio, as atividades de gestão de contrato, nos termos deste Ato;
>
> V - gestão compartilhada: gestão de contrato realizada por mais de um gestor com responsabilidade solidária.

É importante ressaltar as definições do ATC nº 2/2008, pois são diferentes das definidas na IN 1/2019 e transcritas abaixo (BRASIL, 2019, Art. 2º):

> V - Equipe de Fiscalização do Contrato: equipe responsável pela fiscalização do contrato, composta por:
>
> a) Gestor do Contrato: servidor com atribuições gerenciais, preferencialmente da Área Requisitante da solução, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente;
>
> b) Fiscal Técnico do Contrato: servidor representante da Área de TIC, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato;
>
> c) Fiscal Administrativo do Contrato: servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos; e
>
> d) Fiscal Requisitante do Contrato: servidor representante da Área Requisitante da solução, indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista de negócio e funcional da solução de TIC;

6.2.2 Ato da Comissão Diretora nº 16/2008

O ATC nº 16/2008 (SF, 2008a) institui, no âmbito do Senado Federal e de suas Secretarias Especiais e Órgãos Supervisionados, as minutas-padrão (edital e contrato) constantes do Anexo do Ato e dá outras providências. No caso da utilização de alguma das minutas-padrão é dispensável a conferência prévia da Advocacia do Senado e dos órgãos jurídicos das Secretarias Especiais, desde que o Edital se enquadre em uma das minutas-padrão aprovadas pelo Ato, observados o objeto e a modalidade licitatória escolhida. Compete à Secretaria de Administração de Contratações o controle dos editais constantes do Anexo do Ato e sempre que houver necessidade de alteração das minutas-padrão, os

respectivos processos deverão ser encaminhados para manifestação da Advocacia do Senado e posterior aprovação do Diretor-Geral.

6.2.3 Ato da Comissão Diretora nº 9/2012

O ATC nº 9/2012 (SF, 2012) regulamenta, no âmbito do Senado Federal, a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso aos dados, informações e documentos de interesse da sociedade e do Estado. Os artigos abaixo transcritos são os que estão mais afetos à este estudo:

> Art. 2º Os procedimentos previstos neste Ato se destinam a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com as seguintes diretrizes:
>
> I - observância da publicidade como preceito geral e do sigilo como exceção;
>
> II - divulgação de informações de interesse público, independentemente de solicitações;
>
> III - utilização de meios de comunicação viabilizados pela tecnologia da informação;
>
> IV - desenvolvimento do controle social do Senado Federal; e
>
> V - garantia ao direito de acesso à informação, que será franqueada, mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão.
>
> [...]
>
> Art. 3º Fica designada a Diretoria-Geral do Senado Federal para exercer a função de autoridade responsável pela implantação e supervisão do sistema de acesso à informação no âmbito do Senado Federal, com as seguintes atribuições:
>
> I - assegurar o cumprimento das normas relativas ao acesso à informação, de forma eficiente e adequada aos objetivos da Lei nº 12.527, de 2011;
>
> II - monitorar a implementação do disposto na lei e apresentar relatórios periódicos sobre o seu cumprimento;
>
> III - recomendar as medidas indispensáveis à implementação e ao aperfeiçoamento das normas e procedimentos necessários ao correto cumprimento do disposto na referida lei;
>
> IV - orientar as respectivas unidades técnicas no que se refere ao cumprimento do disposto na lei e em seus regulamentos;
>
> V - promover campanha interna de esclarecimento e fomento à cultura da transparência na administração pública e conscientização do direito fundamental de acesso à informação;
>
> VI - determinar o treinamento de servidores no que se refere ao desenvolvimento de práticas relacionadas à transparência na administração pública;
>
> VII - publicar periodicamente as informações estatísticas nos termos do art. 30 da Lei nº 12.527, de 2011; e
>
> VIII - consolidar o relatório anual de informações atinentes à implementação da Lei.
>
> [...]

> Art. 24. O grau de sigilo dos documentos produzidos ou sob a guarda do Senado Federal será declarado pelas seguintes autoridades:
>
> I - ultrassecreto, pelo Presidente e Vice-Presidentes do Senado Federal;
>
> II - secreto, pelas autoridades do inciso I, pelos presidentes de comissão ou dos demais órgãos colegiados do Senado Federal;
>
> III - reservado, pelas autoridades dos incisos I e II, pelos Senadores, no âmbito de seus respectivos gabinetes e, ainda, pelo Secretário-Geral da Mesa, pelo Diretor-Geral e pelos titulares dos órgãos de assessoramento superior do Senado Federal, no âmbito de suas respectivas unidades.
>
> Parágrafo único. As competências previstas nos incisos II e III, poderão ser delegadas a agente público, vedada a subdelegação.
>
> [...]
>
> Art. 26. É dever do Senado Federal controlar o acesso e a divulgação de dados, documentos e informações sigilosos produzidos ou sob sua guarda, assegurando sua proteção.
>
> § 1º O acesso, a divulgação e o tratamento de informação classificada como sigilosa ficarão restritos a pessoas que tenham necessidade de conhecê-la e que sejam devidamente credenciadas, sem prejuízo das atribuições dos agentes públicos autorizados por lei.
>
> § 2º O acesso à informação classificada como sigilosa cria a obrigação para aquele que a obteve de resguardar o sigilo.
>
> § 3º O Senado Federal respeitará a classificação e prazos de restrição de acesso dos dados, informações e documentos sigilosos recebidos.
>
> [...]
>
> Art. 29. Fica criada a Comissão Permanente de Acesso a Dados, Informações e Documentos do Senado Federal.
>
> Art. 30. Compete à Comissão de que trata o art. 29:
>
> I - assessorar a alta direção na regulamentação do acesso e da salvaguarda de dados, informações e documentos sigilosos do Senado Federal;
>
> II - atuar como órgão consultivo, sob demanda das autoridades competentes, nos procedimentos de fixação de categorias de sigilo de dados, informações e documentos, bem como nos processos de revisão ou desclassificação de sigilo;
>
> III - emitir parecer técnico sobre manifestações ou recomendações de órgãos externos, bem como nos casos omissos ou situações não contempladas pela legislação;
>
> IV - propor, quando julgar necessário, alterações nos procedimentos de acesso, classificação, tratamento e armazenamento de dados, informações e documentos sigilosos.

6.2.4 Ato da Comissão Diretora nº 16/2013

O ATC nº 16/2013 (SF, 2013) institui a Política de Gestão de Riscos Organizacionais do Senado Federal, cujo interesse deste estudo está expresso na seção V "Da Segurança da Informação" que estabelece:

> Art. 7º O modelo de segurança da informação no Senado Federal deve assegurar a disponibilidade, a integridade e a preservação das informações

> segundo os critérios institucionais, observada a Lei nº 12.527, de 18 de novembro de 2011 e o Ato da Comissão Diretora 9, de 2012.
>
> Art. 8º O acesso dos servidores ou colaboradores à informação é decorrência da relação funcional entre estes e o Senado Federal e da necessidade de conhecer, não constituindo prerrogativa da própria pessoa.
>
> Parágrafo único. Responderá administrativa e penalmente quem divulgar, em desacordo com as normas legais e administrativas pertinentes, informação de que tenha ciência em razão do disposto no caput deste artigo.
>
> Art. 9º As diretrizes constantes neste Ato são de observância obrigatória por todas as pessoas que tenham acesso às informações do Senado Federal.

6.2.5 Ato da Comissão Diretora nº 8/2015

O ATC nº 8/2015 (SF, 2015a) regulamenta a atuação dos servidores que atuam como fiscais de contratos no âmbito do Senado Federal, especificamente nas contratações de TI, pois há alguns contratos nos quais os fiscais são apenas do órgão técnico e em outros, há também um fiscal da área demandante. Não existem no âmbito do Senado Federal fiscais administrativos, pois o NGACTI atua tanto como gestor do contrato como fiscal administrativo.

6.2.6 Ato da Comissão Diretora nº 9/2017

O Ato da Comissão Diretora nº 9 de 2017 instituiu a Política Corporativa de Segurança da Informação do Senado Federal (PCSI) que tem como objetivo:

> estabelecer princípios, diretrizes estratégicas, responsabilidades, competências e subsídios para a implantação do sistema de gestão de segurança da informação, a fim de viabilizar e assegurar a disponibilidade, a integridade, a autenticidade e a confidencialidade das informações recebidas, produzidas, processadas, armazenadas e transmitidas pelo Senado Federal, observada a Lei nº 12.527, de 18 de novembro de 2011.
>
> (SF, 2017a, art. 1º)

A PCSI estabelece princípios de transparência, garantia da DICA[7] das informações tratadas pelo SF, a confidencialidade quando for exigência legal, além do planejamento de ações de segurança da informação. Institui ainda os seguintes órgãos:

I - Comitê de Segurança da Informação – CSI;

II - Comitês Temáticos de Segurança da Informação – CTSIs;

III - Núcleo de Segurança da Informação em Tecnologia da Informação – NSITI.

Prevê ainda que cada um dos seguintes órgãos indiquem um membro titular e um suplente, para designação por Portaria da Diretoria-Geral, para compor o CSI:

[7] Sigla para disponibilidade, integridade, confidencialidade e autenticidade

> I - Diretoria-Geral;
> II - Secretaria-Geral da Mesa;
> III - Secretaria de Tecnologia da Informação - Prodasen;
> IV - Secretaria de Gestão de Informação e Documentação;
> V - Secretaria de Polícia.

A classificação da informação, disposta em norma específica, é pressuposto para o seu correto tratamento e tem por objetivo assegurar nível adequado de proteção em relação a suas propriedades. Os controles físicos, administrativos e tecnológicos necessários para assegurar a DICA das informações deverão ser implementados conforme a classificação a elas atribuída. O acesso de usuários colaboradores e externos a dados, documentos ou instalações que contenham informações sensíveis, sigilosas ou de acesso restrito deve ser precedido de assinatura de termo de confidencialidade.

O processo de análise e avaliação de riscos é pressuposto para o estabelecimento de controles adequados ao tratamento dos principais riscos de segurança da informação. A gestão de riscos de segurança da informação alinha-se com a Política de Gestão de Riscos Organizacionais do Senado Federal, definida no Ato da Comissão Diretora nº 16 de 2013.

A gestão da continuidade de negócios tem por objetivo, em relação à segurança da informação, garantir níveis adequados de disponibilidade, integridade, confidencialidade e autenticidade às informações essenciais ao funcionamento dos processos críticos de negócio do Senado Federal.

Os recursos de informação do Senado Federal devem ser utilizados para os fins institucionais, respeitados a legislação vigente, a PCSI, as normas complementares de segurança da informação, as obrigações contratuais e os direitos autorais. Deve-se destacar que as normas complementares aqui referenciadas, são normas editadas pelo próprio Senado Federal, e não as normas complementares do Gabinete de Segurança Institucional da Presidência da República tratadas na seção 4.4 do Capítulo 4.

A gestão de incidentes de segurança da informação deve priorizar a restauração do funcionamento adequado dos recursos de informação do Senado Federal.

A gestão de áreas seguras e instalações físicas críticas tem por objetivo, em relação à segurança da informação, prevenir danos e interferências nas instalações do Senado Federal que possam causar perda, roubo ou comprometimento de informações.

Ao Comitê de Segurança da Informação – CSI compete:

> I - planejar, coordenar, acompanhar, monitorar e avaliar, em conjunto com os setores competentes, a implementação da PCSI e das normas complementares e as ações de segurança da informação;
>
> II- analisar e formular ações de segurança da informação para o Senado Federal, considerando a conformidade com a legislação e as recomendações e boas práticas pertinentes;

> III- fomentar a cultura de segurança da informação no Senado Federal;
>
> IV- planejar a capacitação dos usuários em segurança da informação;
>
> V - apresentar propostas de compatibilização das normas do Senado Federal que tenham impacto em segurança da informação com a PCSI;
>
> VI- prestar assessoria em segurança da informação ao Senado Federal;
>
> VII- propor alocação de recursos necessários às ações de segurança da informação;
>
> VIII- apoiar as áreas competentes do Senado Federal na definição de metodologias, processos e tecnologias em segurança da informação, contemplando a classificação da informação, a gestão de riscos em segurança da informação, o uso dos recursos de informação, a gestão da continuidade de negócios e a gestão de incidentes de segurança da informação;
>
> IX - formular, avaliar, monitorar e divulgar indicadores de segurança da informação no âmbito do Senado Federal;
>
> X - instituir CTSI para tratar de assunto específico afeto à segurança da informação, o qual será integrado por servidores indicados pelos titulares das áreas temáticas relacionadas;
>
> XI - revisar a PCSI no máximo a cada três anos;
>
> XII - estabelecer permanente interlocução com outros comitês de segurança da informação criados no âmbito da Administração Pública.

Ao Núcleo de Segurança da Informação em Tecnologia da Informação (NSITI) integrante da estrutura organizacional da Secretaria de Tecnologia da Informação – Prodasen compete:

> I - secretariar o CSI;
>
> II- atuar como gestor de segurança da informação do Senado Federal;
>
> III - receber e encaminhar ao CSI as demandas de ações corporativas de segurança da informação;
>
> IV - oficiar as áreas envolvidas no âmbito dos CTSIs para a indicação de participantes;
>
> V- propor e coordenar, em conjunto com as demais áreas competentes do Senado Federal:
>
> a) a formulação, a avaliação e o monitoramento de indicadores de segurança da informação em tecnologia da informação - TI;
>
> b) ações de segurança da informação em TI;
>
> c) processos de gestão da continuidade de TI;
>
> d) processos de gestão de riscos de segurança da informação em TI;
>
> e) processos de tratamento de incidentes de segurança da informação em TI;
>
> VI- prestar assessoria em segurança da informação em TI às demais áreas do Senado Federal;
>
> VII - prospectar tecnologias aplicáveis à segurança da informação em TI, sem prejuízo da atuação das demais áreas competentes do Senado Federal;
>
> VIII - reportar os incidentes de segurança da informação em TI ao CSI;
>
> IX - apresentar os indicadores de segurança da informação em TI ao CSI.
>
> (SF, 2017a, art. 16)

Porém, até o presente momento o NSITI não foi implantado e não se encontra em funcionamento.

6.3 Atos do Primeiro Secretário

O APS nº 31/2009 (SF, 2009) simplesmente estabelece a possibilidade de realização das compras e contratações eletrônicas do Senado Federal por meio do Portal de Compras do Governo Federal – COMPRASNET.

6.4 Atos da Diretoria Geral

6.4.1 Ato da Diretoria Geral nº 9/2015

O ADG nº 9/2015 (SF, 2015d) estabelece, no âmbito do Senado Federal, normas procedimentais para contratações. Ele define que as as aquisições de bens e serviços comuns serão preferencialmente por meio de pregão eletrônico. Define ainda que o processo de contratações do Senado Federal é composto pelas seguintes etapas:

> I - Iniciação da Contratação: procedimentos com objetivo de formalizar a necessidade de contratação por meio da elaboração do Documento de Oficialização da Demanda;
>
> II - Desenvolvimento da Contratação: procedimentos para especificação da contratação por meio da elaboração do Termo de Referência ou do Projeto Básico;
>
> III - Pesquisa de preços: procedimentos com o fim de estimar o valor de referência para a futura contratação;
>
> IV - Coordenação dos Trâmites: procedimentos e medidas a serem executados e cumpridos para a tramitação e distribuição dos autos de contratação para:
>
> (SF, 2015d, art. 4º)

Cabe à Secretaria de Administração de Contratações (SADCON) a elaboração da minuta do Calendário de Contratações, ouvidos os Órgãos Técnicos. O Calendário de Contratações do Senado Federal foi instituído a partir de 1º de janeiro de 2016.

Para instruir as contratações os órgãos técnicos do Senado Federal deverão elaborar Termo de Referência contendo as seguintes informações:

> a) número do contrato vigente ou vencido para o mesmo objeto, se for o caso;
>
> b) data de vencimento do contrato para o mesmo objeto, se for o caso;
>
> c) objeto, perfeitamente definido, com características, quantidades e respectivos padrões de medida, descrição circunstanciada da situação atual e previsão da situação futura, ou a relação entre custo e benefício;
>
> d) critérios e práticas de sustentabilidade relacionados ao objeto, quando cabíveis;

e) justificativas, inclusive da qualidade e da quantidade, e, quando se tratar de material estocável, com saldo em estoque e histórico de consumo médio emitido pela SPATR;

f) forma e local de execução dos serviços, ou do fornecimento do produto;

g) prazo para início do fornecimento do produto ou serviço;

h) condições de recebimento do produto ou serviço, com Acordo de Níveis de Serviço - ANS, quando for o caso;

i) formalização e prazo de vigência do contrato;

j) prazo de garantia ou validade;

k) previsão dos materiais, instalações ou equipamentos necessários, quando for o caso;

l) indicação de pessoal técnico adequado, quando necessário;

m) capacidade técnica necessária e, quando as atividades concernentes ao objeto da futura contratação referirem-se a atos privativos de profissões regulamentadas em lei, para definição da capacidade técnica profissional, indicar a área de formação do responsável técnico e do respectivo conselho de fiscalização profissional;

n) estimativa de custo, baseada nos procedimentos constantes do Capítulo VI deste Ato, e respectiva planilha de composição, observada a exceção a que se referem os §§ 9º e 10;

o) vistoria técnica e respectivas regras, quando for o caso;

p) indicação sobre a necessidade ou não de amostras, assim como os critérios de aceitação das amostras, condições e prazos de devolução à licitante;

q) obrigações da contratada e do contratante;

r) condições de pagamento;

s) indicação dos gestores e fiscais do contrato;

t) número sequencial do Plano de Contratações;

u) previsão de subcontratação, se permitida;

v) indicação justificada quanto à vedação da possibilidade de participação de consórcio;

w) sugestão justificada da modalidade de licitação, do critério de julgamento e de adjudicação, bem como da opção pela utilização ou não do sistema de registro de preços (SRP);

x) assinatura dos responsáveis pela sua elaboração, inclusive do diretor do órgão técnico;

y) preço ou valor de referência, obtido com base nos procedimentos constantes do Capítulo VI;

z) informar se há óbice ou não quanto ao tratamento diferenciado para microempresa e empresa de pequeno porte, previsto na Lei Complementar nº 123/2006, conforme art. 105 deste Ato.

[...]

§ 4º O ANS conterá:

I - os procedimentos de fiscalização e de gestão da qualidade do serviço, especificando-se os indicadores e instrumentos de medição que serão adotados pelo órgão ou entidade contratante;

II - os registros, controles e informações que deverão ser prestados pela contratada; e

> III - as respectivas adequações de pagamento pelo não atendimento das metas estabelecidas.
>
> § 5º As contratações de soluções de Tecnologia da Informação atenderão, quando houver conveniência e oportunidade, à Instrução Normativa nº4 da SLTI/MPOG, de 2010 e suas alterações.
>
> § 6º O Projeto Básico ou Termo de Referência deverá ser aprovado pelo Diretor-Geral. (SF, 2015d, art. 11)

Existe no Senado Federal uma padronização das contratações por meio do instituto de minutas-padrão, como podemos ver no artigo 63:

> Art. 63. Serão adotadas minutas-padrão de editais, atas de registro de preços, contratos, acordos, convênios ou ajustes, devidamente examinadas pela Advocacia do Senado Federal e aprovadas pelo Diretor-Geral.
>
> § 1º A minuta de edital, ata de registro de preços, contrato, acordo, convênio ou qualquer outra forma de ajuste que divergir do texto da minuta-padrão será submetida ao exame da Advocacia do Senado Federal e à aprovação do Diretor Geral.
>
> (SF, 2015d, art. 63)

O modelo proposto neste estudo poderá servir de base para a criação de uma minuta-padrão para aquisição de serviços em nuvem, padronizando e facilitando sua adoção no Senado Federal.

6.4.2 Ato da Diretoria Geral nº 20/2015

O ADG nº 20/2015 (SF, 2015b) dispõe sobre a fiscalização e a gestão dos contratos de prestação de serviços terceirizados de natureza continuada no âmbito do Senado Federal. Nesse ato estão definidas as responsabilidades de fiscalização e gestão do contrato de prestação de serviços terceirizados. Define que para cada contrato deverá ser designado o fiscal e identificado servidor ou unidade do SF como gestora.

Ressalte-se que, não há um ato que define as competências específicas de um fiscal de contrato de TI, assume-se que as competências do fiscal do contrato seguem o definido no ADG nº 20/2015, que são:

> I - verificar a conformidade da prestação dos serviços e da alocação dos recursos necessários, de acordo com o objeto do contrato;
>
> II - atestar as notas fiscais e as faturas correspondentes à prestação dos serviços;
>
> III - prestar informações a respeito da execução dos serviços e apontar ao gestor do contrato eventuais glosas nos pagamentos devidos à contratada;
>
> IV - quando cabível, manter o controle das ordens de serviço emitidas e cumpridas;
>
> V - prestar informações sobre a qualidade dos serviços, bem como atestar a frequência dos terceirizados.

6.4.3 Ato da Diretoria Geral nº 27/2015

O ADG nº 27/2015 (SF, 2015c) dispõe sobre procedimentos a serem adotados na gestão de contratos entre eles o acompanhamento dos procedimentos de prorrogação ou nova contratação, repactuação, revisão, atestado de capacidade técnica, entre outros. São procedimentos meramente operacionais, que não terão impacto sobre o modelo a ser implementado.

6.5 Conclusão do capítulo

Neste capítulo foram apresentadas as normas específicas do Senado Federal, entre elas Resoluções, Atos da Comissão Diretora, Atos do Primeiro Secretário e Atos da Diretoria Geral. Essas normas deverão ser consideradas na elaboração dos critérios para contratação de serviços em nuvem no âmbito desta Casa Legislativa.

No próximo capítulo, serão analisadas as contratações de serviços em nuvem do TCU e do MP, para que estas experiências possam servir de base para a elaboração dos critérios de contratação de serviços em nuvem para o Senado Federal.

7 Análise das Contratações do TCU e do MP

Neste capítulo são analisadas as contratações do TCU e do MP. Para poder fazer esta análise, na seção 7.1, são selecionados quais os critérios que devem constar no edital de forma a atender aos normativos legais e técnicos que foram levantados no Capítulo 4 e no Capítulo 5.

Na seção 7.2 são detalhadas as características da contratação do TCU e como tem sido a execução do contrato. Na seção 7.3 são elencadas as características da contratação do MP e ao final do capítulo, na seção 7.4 é realizada a análise das contratações com base nos critérios definidos na seção 7.1.

7.1 Critérios de análise dos editais do TCU e MP

Para se poder avaliar os editais do TCU e MP, um dos objetivos específicos deste estudo era "Elaborar critérios de análise dos editais do TCU e MP por meio das legislações e normas vigentes identificadas". Como ponto de partida desses critérios de análise, foram utilizados os definidos por Lopes (2015), que estão listados no Quadro 7, página 73.

Contudo, do momento da definição desses critérios até a presente data, alguns dos normativos foram revogados e substituídos por outros, além disso, algumas normas técnicas foram publicadas, implicando na necessidade de inclusão de requisitos adicionais e na avaliação da continuidade dos requisitos definidos. Avalia-se também que alguns dos critérios utilizados, apesar de necessários, podem ser substituídos pela exigência de certificação específica dos provedores de nuvem. Por exemplo, um provedor que tenha certificação ISO 27001 e 27017 atende os critérios de Lopes de 3 a 13.

Outra questão a ser avaliada é que, em virtude da legislação, em especial à LAI e à LGPD, temos tipos de informação classificados em diferentes em graus de sigilo, o que induz à necessidade de requisitos diferenciados para implementação de serviços em nuvem dependendo da classificação. Por esse motivo, alguns dos critérios utilizados por Lopes dependem de uma avaliação prévia e não são critérios obrigatoriamente aplicáveis para todas as contratações.

Quanto aos riscos apresentados pelo TCU (BRASIL. TCU, 2015, pp. 36–37, Tabela 4) e os controles possíveis para mitigá-los, presentes no relatório da Secretaria de Fiscalização de Tecnologia da Informação (SEFTI) do TCU (2015, pp. 50–61, Anexo I), percebe-se que são critérios importantes de balizamento do processo. Nem todos os riscos e controles podem ser utilizados para avaliação do edital, já que existem alguns que devem ser aplicados antes da contratação e outros que fazem parte do dia-a-dia da organização

e de como é sua forma de gestão e governança, não sendo possível aferi-los analisando o edital. Para a análise foram separados os critérios em 2 grupos. A separação dos grupos teve como objetivo identificarmos quais os critérios que deveriam ser observados durante a fase de seleção do fornecedor e os critérios que fazem parte do contrato ou de sua gestão.

Os 19 (dezenove) critérios para a seleção do fornecedor se encontram listados no Quadro 10 e os 39 (trinta e nove) critérios para a execução contratual e gestão do serviço no Quadro 11, na página 94.

Quadro 10 – Critérios para a seleção do fornecedor

Ref.	**Critério**	**Origem**
SF1	Deve ser representante de pelos menos dois provedores de nuvem	AC 1.739/15 do TCU - risco 1
SF2	Deve possuir pessoal qualificado para trabalhar com o(s) provedor(es) de nuvem da solução	AC 1.739/15 do TCU - riscos 1 e 15
SF3	Deve trabalhar com multirregiões e poder transferir carga de uma região para outra	AC 1.739/15 do TCU - risco 1
SF4	Deve implementar políticas e procedimentos para o uso de criptografia, incluindo gerenciamento de chaves criptográficas	AC 1.739/15 do TCU - risco 5 e Lopes 5
SF5	Possibilitar o armazenamento das chaves criptográficas fora do ambiente de nuvem	AC 1.739/15 do TCU - risco 5
SF6	O provedor deve garantir e demonstrar isolamento de recursos e de dados de seus clientes	AC 1.739/15 do TCU - risco 7
SF7	O provedor deve garantir controles eficazes e compatíveis com as políticas e procedimentos do cliente para gerenciamento de identidades de usuários e controle de acessos	AC 1.739/15 do TCU - risco 8, Lopes 4 e 5
SF8	O acesso e uso de ferramentas de auditoria que interajam com os sistemas de informação das organizações deverão estar devidamente segmentados e restritos para evitar comprometimentos e uso indevido de dados de *log*	AC 1.739/15 do TCU - risco 12
SF9	O modelo de segurança das interfaces do provedor deve ser desenvolvido com base em padrões de mercado, incluindo mecanismos de autenticação forte de usuários e controle de acesso para restringir o acesso aos dados do cliente	AC 1.739/15 do TCU - risco 13 e Lopes 4 e 5

Continua na próxima página

Quadro 10 – Continuação

Ref.	Critério	Origem
SF10	Políticas, procedimentos e mecanismos devem ser estabelecidos e implementados pelo provedor para gerenciamento de vulnerabilidades conhecidas e atualizações de software, garantindo que aplicações, sistemas e vulnerabilidades de dispositivos de rede sejam avaliadas, e que atualizações de segurança fornecidas sejam aplicadas em tempo hábil, priorizando os *patches* mais críticos	AC 1.739/15 do TCU - risco 16
SF11	O processo de gestão de vulnerabilidades do provedor deve ser transparente ao cliente	AC 1.739/15 do TCU - risco 27
SF12	Os provedores devem utilizar pacotes modulares, usar formatos abertos ou populares para dados e serviços, e serem transparentes em regulações e taxas aplicadas à transferência de dados	AC 1.739/15 do TCU - riscos 30, 31, 32 e 33
SF13	Processos, procedimentos e recursos devem ser estabelecidos e testados, de maneira a viabilizar a transferência de operações de um provedor de computação em nuvem para outro provedor alternativo	AC 1.739/15 do TCU - riscos 30, 31, 32 e 33
SF14	O provedor deve possuir programa de formação de profissionais aberto para o mercado	AC 1.739/15 do TCU - riscos 30, 31, 32 e 33
SF15	O provedor deve implementar controles para isolamento e segurança de sistema operacional	AC 1.739/15 do TCU - riscos 37 e 38
SF16	O provedor deve utilizar soluções de virtualização que sejam padrões ou referências de mercado	AC 1.739/15 do TCU - riscos 37 e 38
SF17	O provedor deve implementar política de atualização de versão de software e aplicação de correções	AC 1.739/15 do TCU - riscos 37 e 38
SF18	O provedor deve possuir certificação ISO 27001 e 27017	NC nº 6, 7 e 14 da IN01 DSIC/GSIPR e Lopes 3 a 13

Continua na próxima página

Quadro 10 – Continuação

Ref.	Critério	Origem
SF19	O provedor deve possuir certificação ISO 27018	LGPD, IN02 e IN03 DSIC/GSIPR

Fonte: elaboração própria baseado no TCU (2015)

Quadro 11 – Critérios para a Execução contratual e Gestão do serviço

Ref.	Critério	Origem
CG1	Os SLAs com o provedor de nuvem devem ser cuidadosamente definidos e exequíveis, o que inclui penalidades em caso de não cumprimento	AC 1.739/15 do TCU - riscos 1 e 42
CG2	Os dados devem ser submetidos à classificação prévia da informação, antes de serem transmitidos para a nuvem	AC 1.739/15 do TCU - risco 3
CG3	Implementar controle de acesso lógico apropriado ao grau de confidencialidade dos dados armazenados na nuvem	AC 1.739/15 do TCU - risco 3
CG4	Implementar controles para transferência de dados, como criptografia e uso de VPN adequada	AC 1.739/15 do TCU - risco 4
CG5	As chaves criptográficas não devem ser armazenadas na nuvem	AC 1.739/15 do TCU - risco 5
CG6	Estabelecer limites do acesso do provedor aos dados do cliente	AC 1.739/15 do TCU - risco 5
CG7	Os dados armazenados devem estar criptografados, sendo que o esquema criptográfico deve ser adequado à classificação das informações	AC 1.739/15 do TCU - risco 5 e 6 e Lopes 5
CG8	O provedor deve assegurar que dados sujeitos a limites geográficos não sejam migrados para além de fronteiras definidas em contrato	AC 1.739/15 do TCU - risco 6 e Lopes 1
CG9	Estabelecer responsabilidade do provedor em garantir o isolamento de recursos e dados contra acesso indevido por outros clientes	AC 1.739/15 do TCU - risco 7
CG10	A política para gestão de mudanças deve ser acordada entre provedor e cliente, e este último deve ser comunicado com antecedência sobre mudanças (por exemplo, utilizando processos do ITIL)	AC 1.739/15 do TCU - risco 9 e Lopes 7

Continua na próxima página

Quadro 11 – Continuação

Ref.	Critério	Origem
CG11	*Logs* de auditoria do provedor que registram atividades de acesso de usuários privilegiados, tentativas de acesso autorizados e não autorizados, exceções do sistema, e eventos de segurança da informação devem ser mantidos em conformidade com as políticas e regulamentos aplicáveis, e devem estar de acordo com as políticas do cliente	AC 1.739/15 do TCU - risco 10 e Lopes 10
CG12	Definir políticas e procedimentos que devem ser estabelecidos para triagem dos eventos relacionados à segurança e garantir o gerenciamento de incidentes completo e ágil	AC 1.739/15 do TCU - risco 10
CG13	Quaisquer eventos de segurança de informação devem ser comunicados através de canais predefinidos de comunicação, de maneira rápida e eficiente, e de acordo com os requisitos legais, regulatórios e contratuais	AC 1.739/15 do TCU - risco 10 e Lopes 12
CG14	O cliente deve prever cópia dos *logs* fornecidos pelo provedor, de acordo com sua própria política de retenção; deve haver, da parte do provedor, um mecanismo para filtragem e cópia dos *logs* gerados pelo fornecedor para a área do cliente	AC 1.739/15 do TCU - risco 11 e Lopes 9
CG15	Estabelecer direitos claros e exclusivos de propriedade e acesso aos dados, inclusive referentes a *logs*	AC 1.739/15 do TCU - risco 12
CG16	Definir as obrigações do provedor quanto a requisitos mínimos de autorização e transparência de acesso do provedor aos ativos físicos e virtuais do cliente, bem como a respeito da necessidade de divulgação ao cliente de suas políticas e orientações específicas	AC 1.739/15 do TCU - risco 14
CG17	Definir as obrigações do provedor quanto a requisitos mínimos de contratação de pessoal e de monitoramento de suas atividades, bem como a respeito da necessidade de divulgação ao cliente de suas políticas e orientações específicas	AC 1.739/15 do TCU - risco 15
CG18	Definir a necessidade de realização de avaliações periódicas independentes, com a finalidade de verificar a adequação dos controles do provedor a um conjunto de critérios pré-definidos	AC 1.739/15 do TCU - riscos 20 e 21

Continua na próxima página

Quadro 11 – Continuação

Ref.	Critério	Origem
CG19	Especificar mecanismos de segurança e proteção de propriedade intelectual, e quaisquer requisitos legais ou regulatórios	AC 1.739/15 do TCU - riscos 20 e 21
CG20	Especificar nível esperado dos serviços (SLA) e mecanismos clássicos de gestão contratual de serviços terceirizados (comunicações formais, multas, rescisão etc)	AC 1.739/15 do TCU - riscos 20 e 21
CG21	Estabelecer processos ágeis de migração para provedores alternativos, em caso de falhas do provedor principal	AC 1.739/15 do TCU - riscos 20 e 21
CG23	Deve assegurar a conformidade dos dados e aplicações hospedadas na nuvem com os requisitos de padrões, legais e regulatórios, aos quais o negócio está sujeito, de maneira contínua e atualizada	AC 1.739/15 do TCU - risco 23
CG23	Avaliar quais informações serão hospedadas na nuvem, considerando o processo de classificação da informação, o valor do ativo de informação, os controles de acesso físicos e lógicos, o modelo de serviço e de implementação de computação em nuvem e a localização geográfica onde as informações serão armazenadas (item 5.3 da Norma Complementar 14/IN01/DSIC/GSIPR)	AC 1.739/15 do TCU - risco 25 e NC 14 da IN01 DSIC/GSIPR
CG24	Deve prever soluções de contingência independentes de provedor específico (portabilidade do serviço para outro provedor)	AC 1.739/15 do TCU - risco 26
CG25	Assegurar os níveis de serviço no caso de interrupções de serviço planejadas ou não planejadas	AC 1.739/15 do TCU - risco 26
CG26	Prever modelo de remuneração vinculada aos níveis de serviço estabelecidos, prevendo glosas no caso de descumprimento de parâmetros mínimos	AC 1.739/15 do TCU - risco 26
CG27	Definir sanções no caso de descumprimento reiterado de parâmetros mínimos de níveis de serviço estabelecidos	AC 1.739/15 do TCU - risco 26
CG28	Assegurar que todas as vulnerabilidades sejam priorizadas e corrigidas dentro de SLAs acordados contratualmente entre cliente e provedor	AC 1.739/15 do TCU - risco 27
CG29	Definir divisão clara de papéis de cliente e provedor	AC 1.739/15 do TCU - risco 28

Continua na próxima página

Quadro 11 – Continuação

Ref.	Critério	Origem
CG30	Estabelecer indicadores claros e precisos tanto de ambiente como de segurança, com responsáveis pelo seu monitoramento e disponibilização	AC 1.739/15 do TCU - risco 28
CG31	O contrato deverá prever verificações intermediárias do nível de uso da capacidade contratada, alertas quando atingidos patamares de recursos e tetos de recursos máximos utilizáveis em função do orçamento disponível	AC 1.739/15 do TCU - risco 29
CG32	Prever condições e limites claros de custos para saída do provedor	AC 1.739/15 do TCU - riscos 30, 31, 32 e 33
CG33	Especificar que os direitos de propriedade sobre os dados armazenados na nuvem pela organização são exclusivos da organização	AC 1.739/15 do TCU - risco 34
CG34	Definir em quais países os dados do cliente podem ser armazenados	AC 1.739/15 do TCU - risco 35 e Lopes 1
CG35	Definir que o provedor deve atender à política de exclusão de dados do cliente	AC 1.739/15 do TCU - risco 36
CG36	Utilizar criptografia para proteger os dados de acesso indevido	AC 1.739/15 do TCU - risco 36
CG37	Utilizar técnicas de marca d'água para identificar origens de vazamento de informações sigilosas	AC 1.739/15 do TCU - risco 36
CG38	O contrato deve detalhar definições específicas de incidentes, eventos, ações a serem tomadas e responsabilidades do provedor e do cliente	AC 1.739/15 do TCU - riscos 39 e 40
CG39	O contrato deve definir requisitos de interoperabilidade entre as ferramentas de gestão de incidentes do provedor e do cliente	AC 1.739/15 do TCU - riscos 39 e 40

Fonte: elaboração própria baseado no TCU (2015, Anexo I)

Após a definição dos critérios de avaliação, na próxima seção será detalhada a contratação do Tribunal de Contas da União (TCU) e na seção 7.3 a contratação do Ministério do Planejamento, Desenvolvimento e Gestão (MP), para na seção 7.4 ser realizada a análise dessas contratações com base nos critérios que foram elaborados e se encontram listados acima.

7.2 Contratação do Tribunal de Contas da União (TCU)

O TCU partiu na vanguarda das contratações de serviços em nuvem no setor público e publicou o Edital do Pregão Eletrônico nº 22/2017 no ano de 2017, e assinou o Contrato nº 24/2018 em 23 de abril de 2018, nas subseções seguintes detalharemos as características do edital e como têm sido a execução do contrato.

7.2.1 Características do Edital do Pregão Eletrônico nº 22/2017

O pregão eletrônico nº 22/2017 do TCU teve como objeto a contratação de serviço de computação multi-nuvem, suporte técnico especializado e treinamento, em regime de empreitada por preço unitário. Os serviços de computação multi-nuvem tiveram seus preços avaliados em Unidade de Serviço em Nuvem (USN) e os serviços de suporte técnico especializado em Unidade de Serviço Técnico (UST). Os serviços que estavam sendo licitados são os que estão listados no Quadro 12 e descritos nas próximas subseções.

Quadro 12 – Referência para elaboração das propostas

Item	**Subitens**	**Descrição**	**Unidade**	**Quantidade estimada para 30 meses**	**Valor unitário (R$)**	**Valor total para 30 meses (R$)**
1	1	Serviços de computação multi-nuvem	USN	1.000.000	2,02	2.020.000,00
	2	Serviços de suporte técnico especializado	UST	3.500	253,00	885.500,00
	3	Turmas de treinamento	Turma	3	10.666,00	31.998,00
	Total					2.937.498,00

Fonte: Edital do TCU (2017, p. 16)

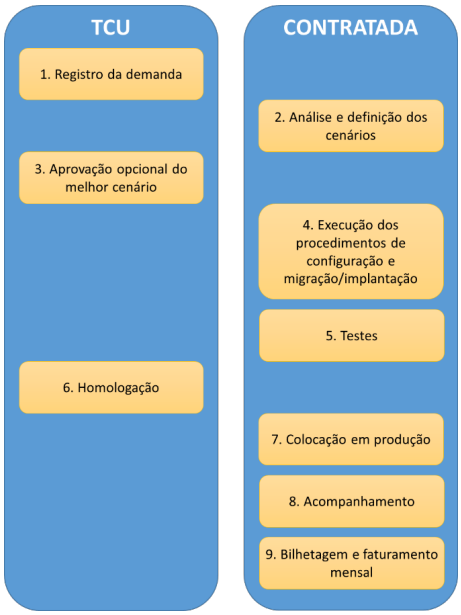
7.2.1.1 Serviços de computação multi-nuvem

Os serviços de computação multi-nuvem são os serviços que são provisionados nos provedores de serviços de computação em nuvem, ou seja, são o consumo de fato da tecnologia de computação em nuvem. Para esse serviço o TCU exigiu que a empresa contratada pelo TCU que iria atuar como *broker*, intermediasse o serviço de dois provedores de serviços de computação em nuvem, e assinasse os contratos associados com os provedores para utilização dos serviços pelo TCU.

O processo de demanda dos serviços segue o processo da Figura 5.

O Edital prevê um rol mínimo de serviços que os dois provedores devem atender. Exige ainda, que um dos provedores forneça todos os serviços por meio de *data center*

Figura 5 – Processo de demanda de serviço de nuvem do TCU



Fonte: TCU (2017, p. 17)

instalado fisicamente em território nacional, incluindo o armazenamento de todos os dados pertencentes ao TCU.

O valor dos serviços em Unidade de Serviço em Nuvem (USN) foi calculado utilizando o preço em dólar comercial do dia do pregão, fixo ao longo do contrato, acrescido dos percentuais de impostos, contribuições, tributos, lucro e custos da empresa dividido pelo valor da USN cotada no pregão.

Para evitar o *vendor lock-in*, os serviços prestados devem ser implementados de modo a serem capazes de migrar de um provedor para o outro. Porém, o TCU se reserva o direito de decidir utilizar um serviço não migrável quando for tecnicamente justificável.

O *broker* deveria fazer uso de ferramenta de gestão multinuvem com no mínimo as seguintes funcionalidades:

> 4.13.1. Cadastrar dois ou mais *cloud providers*, definir centros de custos (unidades virtuais às quais podem ser atribuídos projetos, e às quais podem ser associadas despesas) e o orçamento para o projeto, e provisionar todos os recursos a serem utilizados, respeitando o orçamento atribuído.
>
> 4.13.2. Atribuir usuários e permissões de acesso, monitoramento e alertas de custos e de níveis de uso.
>
> 4.13.3. Isolar financeira e logicamente os recursos computacionais dos *cloud providers* utilizados em diferentes projetos, de modo a não haver nenhum tipo de interferência entre os projetos.
>
> 4.13.4. Permitir a visualização a servidores do TCU de todos os projetos e recursos.
>
> 4.13.5. Configurar a governança do projeto, com possibilidade de restrição ou orientação de uso de recursos em regiões e /ou países pré-determinados.

> 4.13.6. Possibilidade de movimentar os serviços do TCU de uma nuvem para outra, de forma automática. A movimentação inclui recursos, códigos fonte, serviços, dados, metadados, configurações e quaisquer outras informações necessárias à execução de qualquer serviço de uma nuvem para a outra, mediante acionamento manual por parte de operador humano. Uma vez dado o comando pelo operador humano, a ferramenta deverá ser capaz de realizar a migração sem intervenção humana.
>
> 4.13.7. Emitir relatório com todos os custos de recursos relacionados a determinado projeto, ainda que esteja em execução nos dois *cloud providers*.
>
> 4.13.8. Emitir relatório gerencial por centro de custos, com informações referentes ao orçamento, valores utilizados e saldo restante.
>
> (TCU, 2017, pp.19–20)

O TCU garante a prevalência da legislação brasileira por meio do item 4.22 do edital ao definir o foro da contratação como nacional.

No contrato há a exigência de que os dois provedores de nuvem (referenciados no edital como *cloud providers*) deverão atender, no mínimo, aos seguintes requisitos técnicos:

> 4.25.1. Possuir, no mínimo, as certificações ISO 27017 e ISO 27018 ou, alternativamente, demonstrar atender a todos os objetivos e controles dos itens 5 a 18 das referidas normas, mediante apresentação de políticas, procedimentos, e outros documentos. Qualquer documento deverá ser apresentado em nome do provedor, sendo facultado ao TCU promover diligência destinada a esclarecer ou complementar informações.
>
> 4.25.2. Prover serviços de *autoscaling*, baseado em *triggers* pré-configurados, permitindo que soluções tenham acesso automático a maior ou menor quantidade de recursos computacionais, em função da demanda.
>
> 4.25.3. Níveis mínimos de serviços (NMS) são critérios objetivos e mensuráveis estabelecidos com a finalidade de aferir e avaliar fatores como qualidade, desempenho e disponibilidade dos serviços. Os NMS (Níveis Mínimos de Serviço) de disponibilidade de todos os serviços listados na Tabela 1 (reproduzida abaixo, após o item 4.26) deve ser igual ou superior a 99,90%. Serão considerados, para fins de atendimento a este item, os NMS oficialmente publicados por cada *cloud provider*. Caso algum item da tabela 1 não tenha seu NMS publicado pelo *cloud provider*, não será levado em consideração no cálculo de apuração do NMS de que trata este item.
>
> 4.25.4. Prover a funcionalidade de reiniciar máquinas virtuais de forma automática após falha no *host*. Em caso de falha de *host*, o *cloud provider* pode tentar recuperar o mesmo e reiniciar a máquina virtual no *host* original. Caso não seja possível recuperar o *host* imediatamente, o *cloud provider* deve transferir a máquina virtual para outro *host* saudável. A detecção da falha do *host* deve acontecer em até um minuto, e a máquina virtual deve estar em operação novamente em no máximo cinco minutos (no mesmo *host*, caso seja possível recuperá-lo imediatamente, ou em outro *host* saudável).
>
> 4.25.5. Possibilitar manutenção dos *hosts* das máquinas virtuais sem necessidade de reiniciá-las, respeitadas as janelas de manutenção programada do *cloud provider*. No caso de manutenção programada, o TCU deverá receber comunicação prévia acerca da janela de manutenção.

4.25.6. Possibilitar provisionamento de máquinas virtuais de forma simultânea e paralela de forma rápida. Por exemplo, deve ser capaz de provisionar 1 VM Linux com 1 vCPU e 4GB de memória em menos que cinco minutos, uma VM *Windows* com 1 vCPU e 4GB de memória em menos que dez minutos, e vinte VMs Linux cada uma com 1 VCPU e 4GB de memória em menos que quinze minutos.

4.25.7. Oferecer serviço de armazenamento de blocos em discos SSD (Solid State Drive).

4.25.8. Oferecer funcionalidade de *marketplace*, com oferta de softwares do mercado e não apenas do *cloud provider*. O *cloud provider* deve oferecer, no mínimo, 40% (quarenta por cento) dos itens listados na tabela a seguir.

Software
Oracle Database Server – 11g ou superior
JBoss Application Server – 6 ou superior
VMWare – 6 ou superior
SQL Server
Lumis – versão 9 ou superior
Lime Survey – versão 2 ou superior
Moodle – versão 3.1 ou superior
Apache
Media Wiki – 1.25 ou superior
Microsoft Active Directory
Docker
Kubernettes
Red Hat OpenShift
GitLab
Jenkins
Zabbix
Aimetis Symphony – versão 6 ou superior
Red Hat Linux – versão 6 ou superior
Oracle Linux – versão 6 ou superior
CentOS – versão 6 ou superior
Microsoft Windows Server – 2012 ou superior
Microsoft IIS – versão 2012 ou superior
Apache SOLR
Informatica Power Center
Informatica Data Quality
Elasticsearch
Kibana

4.25.9. Oferecer calculadora ou simulador público de preços.

4.25.10. Possibilitar estabelecimento de conexões VPN.

4.25.11. Possuir no mínimo três *datacenters*, em localidades diferentes, e possibilitar escolha do local de residência dos dados.

4.25.12. Possuir programa de certificação para arquitetos de solução do *cloud provider* nos termos do item 4.38. Tal programa deverá estar aberto ao mercado, e não apenas para funcionários internos do *cloud provider*. Esse requisito visa permitir que a prestação de serviços seja orientada por padrões técnicos de domínio público e por melhores práticas passíveis de serem avaliados pela equipe técnica do TCU, evitando a entrega de serviços tipo "caixa preta" que utilizem arquitetura não usual. Visa também facilitar a transição contratual, no caso de mudança de *broker*,

> ou mesmo no caso de a, que gestão dos serviços de nuvem passar a ser de responsabilidade do próprio TCU, e não mais de algum *broker*.

O Tribunal criou uma relação de 13 (treze) serviços básicos de computação em nuvem que os provedores devem atender contendo uma estimativa de valor máximo em USN e sua estimativa de uso durante o contrato. Apesar de haver uma estimativa de uso, o TCU deixa claro que é mera estimativa, não se constituindo em obrigação contratual. A tabela inclui entre outros, serviços de máquinas virtuais Linux e Windows, armazenamento em blocos e objetos, e tráfego de rede.

7.2.1.2 Serviço de Suporte Técnico Especializado

Os serviços de suporte técnico especializado consistem na prestação de serviços pelo *broker*. O TCU listou 23 (vinte e três) serviços que deveriam ser atendidos e que podem ser consumidos para o planejamento de uma nova solução ou suporte e operação de solução implantada.

Os serviços serão prestados remotamente quando possível, e presencialmente quando necessário. Os serviços são quantificados por meio de Unidades de Serviço Técnico (UST), que corresponde ao esforço padronizado para determinada complexidade, independentemente da quantidade de recursos humanos alocados. O pagamento é condicionado à prestação dos serviços e atendimento aos níveis de serviços especificados e seus valores são ajustados de acordo com a natureza da solicitação e sua complexidade.

Foi exigido no edital que os profissionais que executassem os chamados de planejamento, criação e diagnóstico deveriam ter certificação de arquiteto de soluções do provedor de nuvem no qual os serviços estivessem sendo executados (por exemplo, AWS *Certified Solutions Architect* ou Azure *Solutions Architect*). A empresa concorrente deveria ainda apresentar pelo menos um profissional certificado em cada um dos provedores de nuvem que intermediasse no momento da demonstração dos serviços, e a empresa contratada deveria entregar ao TCU listagem dos profissionais certificados antes do início da prestação dos serviços.

O TCU deixa claro que a lista de serviços não é exaustiva, e apenas indica os itens básicos de serviço de suporte técnico especializado. Esses serviços serão prestados pela contratada e não pelo provedor de nuvem.

7.2.1.3 Serviço de Treinamento

O serviço de treinamento objetivava capacitar servidores do TCU na administração e uso do provedor de nuvem. Ao final do treinamento, os usuários da solução deveriam estar aptos a utilizar os recursos do provedor de nuvem, e ser capazes de efetuar a operação e configuração básica de serviços do provedor. O conteúdo programático do treinamento

deveria abranger, no mínimo, como criar e realizar a manutenção dos treze serviços básicos de computação multi-nuvem e sua especificação deveria ser desenvolvida em conjunto pelas equipes da contratada e do TCU.

O treinamento deveria ser presencial, com duração mínima de três dias e máxima de cinco dias, com no máximo oito horas diárias em horário comercial. Não poderia ser meramente expositivo, devendo contemplar também o uso prático da solução e o desenvolvimento de estudos de caso. O treinamento seria prestado nas dependências do TCU em instalações e equipamentos providos por ele. A preparação do ambiente de treinamento deveria ser realizada em conjunto pelas equipes da contratante e da contratada, de forma a garantir a correta configuração e disponibilidade do ambiente de treinamento.

Caso a qualidade do treinamento em alguma turma fosse considerada insatisfatória pela maioria dos alunos, o TCU poderia exigir que fosse refeito, sem ônus.

7.2.1.4 Modelo de Execução

Nas subseções seguintes será descrito como é o modelo de execução do contrato do TCU, explicando como acontece a solicitação dos serviços contratados.

7.2.1.4.1 Solicitação, execução e acompanhamento dos serviços

O modelo de execução do contrato do TCU envolve abertura de ordens de serviço que contemplem combinação dos serviços referentes ao item 1 e ao item 2. Enquanto os serviços de computação multi-nuvem (item 1) são prestados pelos provedor de nuvem, os serviços de suporte técnico especializado (item 2) são prestados diretamente pela contratada, que deve combinar os serviços do provedor de nuvem com seu conhecimento técnico de modo a entregar a solução demandada pelo TCU. É possível que uma única ordem de serviço contenha serviços relativos ao item 1 e ao item 2, ainda que, em certos casos, possa conter apenas serviços relativos ao item 1 ou ao item 2.

A contratada deve realizar os devidos escalonamentos de acordo com o nível de atendimento dos chamados, reportados pelo TCU ou pelo sistema de monitoramento da contratada. Em caso de qualquer mudança na situação de chamados, deve ser encaminhada uma notificação ao TCU contendo as informações de registro do chamado, inclusive quando houver mudança de status interrompendo a contagem de Nível Mínimo de Serviço (NMS). Mensalmente a contratada envia o relatório de fechamento mensal, acompanhado da correspondente nota fiscal/fatura.

O relatório de fechamento mensal deve conter a relação de chamados abertos até o término do mês anterior e os indicadores de nível de serviço alcançados de cada chamado. O relatório também deve trazer o NMS de todos os serviços naquele mês. Por fim, o

relatório deve trazer comprovação de quitação das obrigações da contratada para com os provedores de nuvem dos serviços listados no relatório de fechamento anterior.

7.2.1.4.2 Chamados de planejamento/criação/diagnóstico

Quando é aberto um chamando de planejamento/criação/diagnóstico, é realizada uma reunião presencial ou virtual para tratar da demanda solicitada. Nessa reunião é explicada a demanda e a contratada terá até cinquenta horas úteis, contadas a partir do dia útil subsequente ao da realização da reunião para apresentar dois planos de arquitetura de solução para implementação dos serviços demandados. Cada plano na plataforma de um dos dois provedores de nuvem que a contratada intermediar. Cada plano de arquitetura trará, no mínimo, as seguintes informações:

a) Descrição detalhada do serviço demandado.

b) Arquitetura proposta pela contratada para implementação do serviço demandado.

c) Orçamento detalhado dos serviços do provedor de nuvem que serão usados para implementação do serviço demandado, com o preço original do fabricante, em dólar, e com o preço efetivamente cobrado pela contratada.

d) Orçamento detalhado dos serviços da contratada que serão usados para implementação do serviço demandado.

e) Prazo para entrega dos serviços em perfeita operação.

f) Descrição detalhada de restrições, dependências e quaisquer informações relevantes acerca do plano proposto.

O TCU analisará os planos de arquitetura de modo a verificar se contêm todos os requisitos técnicos demandados. Caso contrário, solicitará à contratada que refaça os planos de arquitetura, sem reinício de contagem de prazo. Durante a análise realizada pelo TCU, o prazo da contratada será suspenso. Após o aceite dos planos de arquitetura, o Tribunal analisará os dois orçamentos e decidirá se os serviços demandados serão implementados. Caso decida pela implementação dos mesmos, fará a opção, via de regra, pelo orçamento de menor preço, exceto quando existirem fatores técnicos ou de prazo que justifiquem a adoção do orçamento de maior preço. Nesse último caso, o TCU justificará a sua escolha de forma detalhada.

Os serviços referentes à elaboração dos planos de arquitetura serão pagos independentemente da decisão de implementar os serviços ou não.

7.2.1.4.3 Chamados de execução/alteração/implantação ou exclusão

Quando é aberto um chamado de execução/alteração/implantação ou exclusão, é agendada uma reunião presencial ou virtual em até dez horas úteis após a abertura do chamado. Após a execução dos serviços o TCU realiza uma análise para verificar se estão em conformidade com o plano de arquitetura. Caso contrário, solicitará à contratada que refaça os serviços, sem reinício de contagem de prazo. Durante a análise realizada pelo TCU, o prazo da contratada será suspenso.

O TCU poderá solicitar à contratada demanda de execução/alteração/implantação ou exclusão sem que tenha existido correspondente demanda de planejamento/criação/diagnóstico. Sendo assim, a demanda de execução/alteração/implantação ou exclusão poderá ter como fonte algum plano de arquitetura elaborado pela contratada em chamado prévio de planejamento/criação/diagnóstico ou plano de arquitetura elaborado por servidor do TCU. A fonte da demanda deverá fazer parte da OS de execução/alteração/implantação ou exclusão.

7.2.1.4.4 Chamados de monitoração

Os chamados de monitoração são classificados por severidade e seus NMS serão mensurados por indicadores relacionados à severidade e ao estado dos chamados, para os quais foram estabelecidas metas quantificáveis a serem cumpridas pela contratada e pelo TCU, conforme tabela presente no edital. Os chamados terão início da contagem de prazo no momento da comunicação do chamado à contratada.

Será admitida solução de contorno na resolução de chamados de severidade 1 e 2 (que são os mais críticos) para fins de atendimento dos prazos estipulados na tabela do edital. Solução de contorno é a redução ou eliminação do impacto de um incidente ou problema para o qual uma resolução completa ainda não está disponível. Para fins de verificação do atendimento, os chamados serão agrupados por nível de severidade e seus prazos de atendimento serão contabilizados mensalmente. De acordo com o grau de severidade o edital estabelece um objetivo mensal de atendimentos que devem ser atendidos dentro do prazo do Nível Mínimo de Serviço (NMS).

Após a entrada em produção de uma aplicação ou serviço na nuvem, deverá haver período de estabilização de sessenta dias para que os níveis de serviço descritos na no edital sejam totalmente aferidos e entregues ao TCU. O prazo terá início a partir do primeiro dia em que os serviços estiverem em produção. Durante o período e estabilização, não haverá desconto ou sanção por descumprimento dos prazos estabelecidos, mas os serviços serão remunerados.

O TCU previu no edital que o vencedor da etapa de lances demonstrasse a execução dos serviços descritos para verificar se atendiam aos requisitos exigidos na licitação. A

licitante deveria configurar ambientes de serviços de computação em nuvem nos dois provedores de nuvem que intermediasse. O ambiente envolveria os serviços listados no edital, de acordo com o plano detalhado que receberia do TCU. Após configurados os ambientes, a licitante receberia ordens de serviço consecutivas que envolveriam os serviços especificados no edital.

Caso não configurasse o ambiente nos dois provedores de nuvem, ou não cumprisse qualquer das ordens de serviço, a licitante seria desclassificada. A licitante deveria ainda apresentar pelo menos um profissional que possuísse a certificação exigida pelo TCU em cada um dos provedores de nuvem que intermediasse.

7.2.1.5 Itens Contratuais

Na Cláusula sétima – "DOS ENCARGOS DAS PARTES" o TCU se preocupa com as questões do sigilo das informações, como podemos perceber nos itens abaixo:

> 2.6. **comprometer-se a não reproduzir e/ou dar conhecimento a terceiros, sem a anuência formal e expressa do TCU, das informações restritas reveladas**. A expressão "informação restrita" abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, dentre outros.
>
> 2.7. **comprometer-se a não utilizar**, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no contrato de prestação de serviços ao TCU, **as informações restritas reveladas**.
>
> 2.8. **cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos** nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços ao TCU, **devendo cientificá-los da natureza confidencial das informações restritas reveladas**.
>
> 2.9. **possuir ou firmar acordos por escrito** com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos **termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo**.
>
> 2.10. **informar** imediatamente **ao TCU qualquer violação das regras de sigilo** estabelecidas neste Termo que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como qualquer incidente de segurança ou existência de vulnerabilidades relativas ao objeto da contratação;
>
> 2.10.1. **A quebra do sigilo** das informações restritas reveladas, devidamente comprovada, sem autorização expressa do TCU, **possibilitará a imediata rescisão de contrato firmado entre o TCU e a Contratada sem qualquer ônus para o TCU**. Nesse caso, a Contratada

> estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo TCU, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.
>
> (TCU, 2017, pp. 53–54, grifo nosso)

Na cláusula décima quarta – "DAS SANÇÕES" percebe-se a preocupação com o acordo de nível de serviço estabelecido, já que estão definidas sanções em caso de descumprimento do ANS tanto para os serviços de computação multi-nuvem, quanto para os serviços de suporte técnico especializado.

7.2.2 Execução do contrato nº 24/2018, firmado em 23/04/2018

Em entrevista não estruturada com a fiscal do contrato do TCU foram levantadas informações sobre a execução do contrato nº 24/2018. A servidora esclareceu que o objetivo do contrato foi o de proporcionar um primeiro contato com a tecnologia de computação em nuvem. Esclarece ela que apesar de ter um pouco mais de um ano de contrato, o projeto para contratar serviços de computação em nuvem foi iniciado há aproximadamente quatro anos. Por esse motivo, algumas das propostas que constam para adoção de nuvem no livro que é coautora não foram contempladas, como por exemplo a atividade "1.1.1 - Criar equipe de nuvem" do Processo Primeira Nuvem (COSTA et al., 2019, p. 150).

Um dos desafios colocados para a implantação do projeto era como comparar qual era a melhor proposta, já que cada provedor de nuvem tinha uma forma de comercialização diferente e oferecia serviços distintos. Chamou a atenção também que os grandes provedores de nuvem mundiais, apesar de terem filiais no Brasil, não tinham interesse em contratar com o governo diretamente. Optou-se então pela contratação por meio de um *broker* de dois provedores de nuvem, com a intenção de evitar o *vendor lock-in*. Para conseguir comparar as propostas, optou-se por selecionar entre os grandes provedores os serviços que possuíam em comum e gerar uma unidade de comparação, que foi a Unidade de Serviços em Nuvem (USN).

Uma das grandes dificuldades do projeto tem sido o faturamento, já que a ferramenta de orquestração utilizada, o Cisco Cloud Center, não consegue fornecer um relatório de faturamento em USN, nem fornecer um agrupamento por projeto. Outro fator dificultador é que a granularidade dos relatórios de faturamento é muito alta, tornando a verificação uma tarefa muito complexa.

Explicou ainda que, o processo de tratamento das solicitações de serviço do *broker* não estavam bem definidos, o que ocasionou um retardo das implementações e um nível de serviço abaixo do esperado. Detectou-se que faltava no contrato mecanismos para mensurar melhor a qualidade do serviço ofertado pela contratada. Essa dificuldade, junto com os problemas de faturamento, acabaram levando a uma subutilização do contrato, já que por

não saber o que já se havia consumido e não ter a possibilidade de acompanhar de perto o consumo, optou-se por uma implantação cautelosa do serviço.

Apontou um caso de sucesso de utilização do *marketplace* onde o TCU pôde implantar por um curto período de tempo uma versão do seu site com caracteres em arábe em virtude de um evento, onde se pagou apenas pelo uso, evitando a aquisição de uma licença de software de valor elevado e que teria pouca utilização.

Quanto à questão de dados sensíveis em *datacenters* fora do país, lembrou que a transparência é a regra e o sigilo a exceção. Portanto, a classificação dos dados ficou a cargo do usuário, o qual deveria informar a necessidade quando da fase de projeto do *workload*, para poder ser determinado onde hospedar os dados. A possibilidade de hospedar dados no exterior foi considerada vantajosa, pois os custos no exterior são menores do que nos *datacenters* em território nacional.

Apesar de todas as dificuldades encontradas, o projeto atendeu ao seu principal objetivo, que era trazer mais conhecimento sobre a tecnologia. Essa experiência demonstrou também a necessidade de se **definir uma equipe interna para trabalhar diretamente com a tecnologia de computação em nuvem**, de uma melhor definição de nível de serviço do *broker*, de uma melhoria dos controles e das solicitações de serviço, com a implementação de indicadores. Ficou claro também que os documentos de solicitação de serviços, faturamento e acompanhamento do contrato necessitavam ter sido melhor detalhados no edital, por meio de um modelo de relatório, ou pelo menos ter as definições das informações mínimas. Outros aprimoramentos que foram destacados são: a necessidade de elaborar melhor os procedimentos para o fim do contrato e transição entre os contratados e uma lista maior de serviços pré-definidos.

7.3 Contratação do Ministério do Planejamento, Desenvolvimento e Gestão

7.3.1 Características do Edital do Pregão Eletrônico nº 29/2018

O pregão eletrônico nº 29/2018 do MP (2018a) teve como objeto a contratação de empresa especializada (integrador) para prestação de serviços de computação em nuvem, sob demanda, incluindo desenvolvimento, manutenção e gestão de topologias de aplicações de nuvem e a disponibilização continuada de recursos de Infraestrutura como Serviço (IaaS) e Plataforma como Serviço (PaaS) em nuvem pública. Os serviços que estavam sendo licitados são os que estão descritos no Quadro 13 e que serão detalhados nas subseções seguintes.

Foi exigido das empresas atestados de capacidade técnica para comprovar a qualificação das empresas. Os atestados deveriam comprovar que a licitante já forneceu

Quadro 13 – Objeto do Edital do MP

Grupo	Item	Unidade	Quantidade estimada	Valor unitário (R$)	Valor total por item (R$)
1	1. Serviços de computação em nuvem	USN	7.297.319	7,96	58.086.659,24
	2. Serviços técnicos especializados	UST	45.505	281,18	12.795.095,90
	3. Treinamento	Turma de Treinamento	31	16.987,00	526.597,00
Total para 30 meses (R$):					**71.408.352,14**

Fonte: MP (2018b, p. 4)

satisfatoriamente os serviços de implantação, administração e operação de serviços de nuvem, comprovando a implantação, administração e operação de, no mínimo, 100 instâncias de máquina virtual em nuvem em um período mínimo de 12 meses.

Além disso, deveria também informar o provedor de serviços em nuvem que comporia a solução e apresentar declaração emitida pelo provedor, assegurando ser capaz de prover os serviços objetos desta contratação a partir de infraestrutura de *datacenter* localizada no Brasil.

A contratação do MP tinha como objetivo também:

> a) Padronização tecnológica na Administração Pública;
>
> b) Redução de custos de manutenção e melhor eficiência pelo uso racional dos recursos, uma vez que estes foram definidos de forma a atender as necessidades do usuário;
>
> c) Ganho de economia de escala, pois, ao prospectar grandes volumes licitados, a Administração Pública amplia seu poder de compra junto aos fornecedores e reduz consideravelmente os preços, fato que certamente não ocorreria quando do fracionamento de certames.
>
> (MP, 2018b, p. 2, item 2.6)

Para atingir esses objetivos, o pregão era para assinatura de uma ata de registro de preços com diversos órgãos partícipes, com os quantitativos listados no Quadro 14.

7.3.1.1 Serviços de computação em nuvem

Os serviços de computação em nuvem são os serviços que são provisionados no provedor de serviços de computação em nuvem, ou seja, são o consumo de fato da tecnologia de computação em nuvem. A empresa contratada pelo MP atua como integrador (*broker*)

Quadro 14 – Quantitativos para o órgão gerenciador e órgãos partícipes

UASG	**ÓRGÃO**	**USN (item 1)**	**UST (item 2)**	**TREINAMENTO (item 3)**
201004	Ministério do Planejamento	1.768.350	10.698	5
370003	Ministério da Transparência, Fiscalização e CGU	686.188	1.952	2
114702	Fundação Escola Nacional de Adm. Pública	168.630	486	2
200109	Departamento de Polícia Rodoviária Federal/DF	122.505	1.180	6
170009	Escola de Administração Fazendária/DF	435.198	2.276	2
253002	Agência Nacional de Vigilância Sanitária	914.612	12.020	5
343026	Instituto do Patrimônio Hist. e Art. Nacional	558.750	3.247	2
303001	Conselho Administrativo de Defesa Econômica	949.104	1.644	1
170531	Superintendência de Administração do MF - DF	708.838	7.248	1
158146	Inst. Fed. de Educ., Ciênc. e Tecnologia Piauí	605.586	3.055	3
443033	Inst. Chico Mendes de Conser. da Biodiversidade	292.389	1.171	1
926397	ABGF - Agência Brasileira Gestora de Fundos Garantidores e Garantias S.A.	87.169	528	1

Fonte: Termo de Referência do MP (2018b, pp. 4–5)

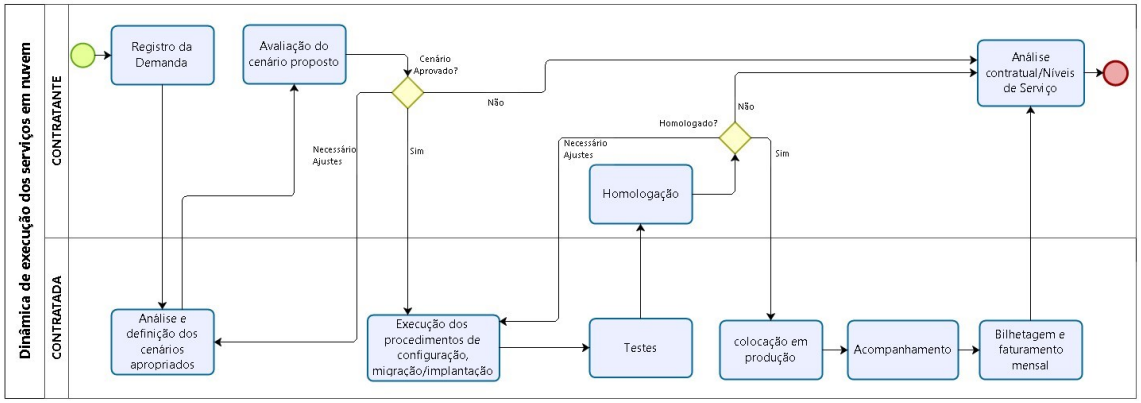
de um provedor de serviços de computação em nuvem que deve prover em seu catálogo de serviços todos os 32 (trinta e dois) serviços listados no edital.

O *broker* deverá comprovar ser empresa autorizada a comercializar os serviços e prestar suporte técnico do provedor no momento da assinatura do contrato. Esta comprovação se dá por meio de declaração do provedor. O *broker* deverá ainda disponibilizar conta no provedor por meio da qual será feito o provisionamento dos serviços.

O processo de demanda dos serviços segue o processo da Figura 6.

Os serviços listados no edital deverão ser executados no Brasil, o que inclui armazenar os dados e informações do MP em *data centers* instalados fisicamente no Brasil, incluindo replicação e cópias de segurança (*backups*), conforme disposto na Norma Complementar nº 14/IN01/DSIC/SCS/GSIPR, de modo que o MP disponha de todas as garantias da legislação brasileira enquanto tomadora do serviço e responsável pela guarda das informações armazenadas em nuvem. Todos os serviços técnicos especializados prestados pelo *broker* deverão estar aderentes às regras descritas no Guia de Gestão de Riscos de

Figura 6 – Processo de demanda de serviço de nuvem do MP



Fonte: MP (2018b, p. 6)

Aplicações em Nuvem Pública, definido no Anexo V do Termo de Referência.

Deverá ser disponibilizado pelo *broker* um portal contendo informações sobre:

a) Planilha de preços: valores praticados pelo *broker* com os preços de todos os serviços (em USN); informar também quais serviços do provedor são gratuitos;

b) Relatório de Faturamento: relatórios com consumo de serviços do provedor;

c) Informações sobre o contrato: detalhamento do contrato, tipos de serviços;

d) Relatórios de avaliação de otimização e performance, contendo sugestões de melhorias, ajustes em diversos aspectos da infraestrutura; Os relatórios deverão ser disponibilizados pelo portal, com periodicidade diária, semanal ou mensal, a depender das características do serviço ou recurso avaliado.

Conforme especificado no edital, o *broker* fará uso de ferramenta de gestão de nuvem com, no mínimo, as seguintes funcionalidades:

> 5.1.10.1. Definir centros de custos (unidades virtuais às quais podem ser atribuídos projetos, e às quais podem ser associadas despesas) e o orçamento para o projeto, e provisionar todos os recursos a serem utilizados, respeitando o orçamento atribuído;
>
> 5.1.10.2. Permitir a criação, modificação e exclusão de usuários e grupos de usuários, aos quais poderão ser atribuídas permissões de acesso;
>
> 5.1.10.3. Isolar financeira e logicamente os recursos computacionais do provedor utilizados em diferentes projetos, de modo a não haver nenhum tipo de interferência entre os projetos;
>
> 5.1.10.4. Armazenar logs de acesso para fins de auditoria. Os logs deverão ser mantidos durante toda a vigência do contrato, devendo ser entregues à CONTRATANTE quando solicitados e no encerramento do contrato; O prazo de retenção desses logs poderão a qualquer tempo ser alterado de acordo com a determinação da CONTRATANTE.
>
> 5.1.10.5. Permitir que, a partir de uma interface personalizada, o usuário com as devidas permissões tenha acesso aos recursos disponíveis no provedor e consiga executar ao menos tarefas básicas (criar/alterar/excluir servidores virtuais, volumes de armazenamento, configurações de rede,

> etc.) relacionadas aos serviços de computação em nuvem, listados na Tabela 1;
>
> 5.1.10.6. Permitir monitorar as informações sobre a quantidade e o status das instâncias, bem como, o uso de seus recursos computacionais (CPU e RAM) e de outros serviços (tráfego de saída de rede, armazenamento, banco de dados, etc.), isoladamente por projeto;
>
> 5.1.10.7. Permitir o monitoramento dos custos dos serviços;
>
> 5.1.10.8. Permitir a emissão de alertas de gastos para cada projeto. Os alertas deverão ser apresentados na ferramenta e enviados por e-mail para os usuários responsáveis, previamente cadastrados;
>
> 5.1.10.9. Emitir relatório com todos os custos de recursos relacionados a determinado projeto.
>
> 5.1.10.10. Emitir relatório gerencial por centro de custos, com informações referentes ao orçamento por projeto, valores utilizados e saldo restante;
>
> MP (2018b, pp. 7–8, item 5.1.10)

Todas as ferramentas, soluções, software e *scripts* fornecidos pelo *broker* deverão ser executados em infraestrutura do MP ou do próprio provedor de nuvem, não terão custos de aquisição e manutenção durante o contrato e ao final deverão ser de propriedade do MP. O ambiente tecnológico provido durante a execução do contrato deve ser independente da ferramenta de Gestão de Nuvem, sendo possível a inclusão, exclusão, alteração da infraestrutura ou serviços por meio do portal do próprio provedor de nuvem a qualquer tempo.

O edital estabelece quais são os serviços mínimos que deverão ser disponibilizados pelo provedor de nuvem. Um dos serviços incluídos é o de *autoscaling*, que permite que as soluções tenham acesso automático a maior quantidade de recursos computacionais, em função da demanda.

Níveis mínimos de serviços (NMS) são critérios objetivos e mensuráveis estabelecidos com a finalidade de aferir e avaliar fatores como qualidade, desempenho e disponibilidade dos serviços. O NMS de disponibilidade das instâncias deve ser igual ou superior a 99,741% para cada período de 1 mês.

O *broker* deve oferecer calculadora ou simulador público de preços do provedor que integra a solução para cada um dos 32 (trinta e dois) serviços de computação em nuvem listados no edital.

Os serviços de multi-nuvem na modalidade *upfront*[8] só poderão ser demandados e colocados em operação até 9 (nove) meses antes do final da vigência do contrato, ainda que a duração do serviço venha a extrapolar a vigência do contrato. O máximo de tempo que o serviço poderá ficar em operação após o encerramento do contrato será de 3 (três) meses, estando adequado ao prazo de retenção da garantia contratual.

[8] Modalidade *upfront* é uma modalidade na qual o pagamento pelo uso dos recursos é feito adiantado, ou seja, antes da prestação do serviço, ficando o provedor de nuvem obrigado a garantir o uso do recurso pelo prazo contratado e pago.

Todos os dados decorrentes de serviços solicitados pelo MP ao *broker* e operacionalizados no provedor serão de propriedade apenas do MP, a quem deverá ser assegurado acesso irrestrito a qualquer momento do contrato. Durante todo o período do contrato, e particularmente ao final desse, independente da razão que tenha motivado o seu término, o *broker* repassará ao MP todas as informações necessárias à continuidade da operação dos serviços em nuvem.

Todos os serviços prestados pelo *broker* devem ser realizados de modo que as aplicações provisionadas na nuvem sejam portáveis para outros provedores, sem nenhuma possibilidade de aprisionamento (*vendor lock-in*), automatizando toda a inteligência de provisionamento de infraestrutura virtual do MP por meio da ferramenta de gestão de nuvem. Além disso, não deverão ser utilizados serviços, protocolos ou ferramentas nativos de apenas um provedor (proprietários), salvo quando justificável tecnicamente ou por decisão de projeto/operação e autorizados formalmente pelo MP.

7.3.1.2 Serviços Técnicos Especializados

Os serviços técnicos especializados são serviços de suporte, planejamento e provisionamento de responsabilidade do *broker*. O MP listou 33 (trinta e três) serviços, entre eles a elaboração da arquitetura da solução e a configuração de diversos serviços no provedor, que devem ser prestados presencialmente. Existem alguns serviços que podem ser prestados remotamente, desde que previamente autorizados pelo MP. A remuneração se dá por meio de Unidades de Serviço Técnico (UST), que correspondem ao esforço padronizado para determinada complexidade, independentemente da quantidade de recursos humanos alocados. O seu pagamento é condicionado à prestação dos serviços e atendimento aos níveis de serviços especificados.

A equipe técnica do MP poderá a qualquer tempo ativar ou desativar serviços, plataformas ou infraestrutura, provisionar e gerenciar recursos em nuvem, utilizando para isso a ferramenta de gestão de nuvem fornecida na solução, sem o assessoramento ou autorização por parte do *broker*. As ações realizadas pela equipe técnica do MP não geram ordens de serviços referentes à execução de serviços técnicos especializados. Somente serão emitidas ordens de serviços relativas ao consumo dos recursos que forem provisionados pela equipe técnica do *broker*.

Para realização de todos os serviços técnicos especializados o *broker* deverá possuir um ou mais profissionais diretamente envolvidos na execução de cada ordem de serviço que detenham em conjunto os seguintes perfis:

a) Possuir certificação ou experiência profissional de Arquiteto de Soluções, ou papel equivalente, relacionados ao Provedor de Nuvem (Marca de Nuvem Pública) ou Plataforma de Nuvem (Tecnologia de Nuvem) no qual os serviços estiverem sendo executados (por exemplo, *AWS Certified Solutions Architect,*

OpenStack Solution Architect, Azure Solutions Architect, VMWare Solution Architect, etc.);

b) Possuir certificação ou experiência profissional de Arquiteto de Soluções, ou papel equivalente, relacionados à ferramenta de Gestão de nuvem provida pelo *broker*.

Ao final do contrato, o *broker* será responsável pelo processo de migração para a infraestrutura da nova contratada, se for o caso, garantindo o funcionamento e níveis de serviços das aplicações e infraestruturas de produção. Essa demanda será realizada por meio da contratação de USTs.

O *broker* quando demandado na criação de ambientes, implementação de soluções ou serviços que envolvam estruturas de IaaS, deve comprovar a utilização racional dos recursos ofertados, evitando assim desperdícios de USNs em infraestrutura subutilizada. Cada arquitetura ou projeto será implementado e monitorado mensalmente, e caso haja a necessidade de alteração da infraestrutura para otimização de recursos, esses serão realizados sem ônus para o MP.

7.3.1.3 Treinamento

O treinamento é destinado aos servidores técnicos do MP, visando capacitá-los no gerenciamento e no uso do gerenciador de nuvem. Ao final do treinamento, os treinandos devem estar aptos a utilizar os recursos, efetuando operação e configuração básica das funcionalidades do gerenciador de nuvem.

Exige-se que o treinamento seja presencial e dividido em etapas. O treinamento não poderá ser meramente expositivo. Deve contemplar também o uso prático da solução e o desenvolvimento de estudos de caso. O treinamento fornecido deve ser apresentado em língua portuguesa. O material didático deve ser fornecido em formato digital e/ou impresso para todos os participantes com o conteúdo abordado durante o treinamento em língua portuguesa ou, opcionalmente, em língua inglesa, desde que justificado e aceito pelo MP.

O instrutor responsável pela execução do treinamento deve possuir experiência comprovada como instrutor da solução e pleno conhecimento da solução alvo do treinamento. A comprovação da capacitação do instrutor se dará com base na apresentação de certificados de treinamentos.

7.3.1.4 Suporte Técnico

O *broker* deverá obter suporte técnico, no regime de 365x24x7[9], do provedor de nuvem que venha a fornecer soluções para o MP. O suporte deverá incluir resposta a chamados críticos em tempo inferior a sessenta minutos e permitir a comunicação por meio de *e-mail*, chat e telefone (devendo o *broker* fornecer um número telefônico para chamada local em Brasília ou gratuita).

Os serviços de Suporte Técnico compreendem todos os chamados relativos a um serviço previamente planejado e executado pelo *broker*, bem como todos os chamados que objetivem esclarecer dúvidas na utilização dos serviços prestados diretamente pelo provedor, independentemente de esses serviços terem sido provisionados pelo *broker* ou pelo MP. Os serviços de suporte técnico deverão ser prestados pelo *broker* sem qualquer ônus adicional para o MP. Os chamados de suporte técnico serão classificados por severidade, de acordo com o impacto no ambiente computacional do MP. Para fins de verificação do atendimento, os chamados serão agrupados por nível de severidade e seus prazos de atendimento serão contabilizados mensalmente.

O *broker* não será responsabilizado pelo prazo máximo estabelecido, quando o chamado for originado por: falha, interrupção ou qualquer outra ocorrência nos serviços de telecomunicações ou energia elétrica que atendem à infraestrutura interna do MP; indisponibilidade de dados, inconsistência de dados e informações geradas pelo MP; infraestrutura e capacidade de ambiente de tecnologia do MP. Não se caracterizam, nesses casos, a indisponibilidade dos serviços ou inadimplemento do *broker*.

7.3.1.5 Requisitos de segurança

O Termo de Referência do MP exige que sejam seguidas todas as orientações da NC14/IN01/DSIC/SCS/GSIPR, homologada por meio da Portaria nº 9, de 15 de março de 2018, além disso descreve diversos itens que deverão ser atendidos quanto à segurança da informação, segurança de identidades, segurança nas requisições/dados e segurança de chaves.

7.3.1.6 Modelo de Execução

Nas subseções seguintes será descrito como é o modelo de execução do contrato do MP, explicando como acontece a solicitação dos serviços contratados.

[9] Regime no qual o suporte ficará disponível 365 (trezentos e sessenta e cinco) dias ao ano, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana

7.3.1.6.1 Solicitação, execução e acompanhamento dos serviços

O modelo de execução do objeto proposto envolve abertura de ordens de serviço que contemplam serviços referentes aos itens de computação em nuvem e serviços técnicos especializados. Enquanto os serviços de computação em nuvem são prestados pelo provedor, os serviços técnicos especializados são prestados diretamente pelo *broker*, que deve combinar os serviços do provedor com seu conhecimento técnico de modo a entregar a solução demandada. É possível que uma ordem de serviço (OS) contenha somente serviços relativos aos serviços de computação em nuvem ou aos serviços técnicos especializados e, em certos casos, a mesma ordem de serviço poderá ser composta por serviços relativos a ambos os serviços.

7.3.1.6.2 Chamados de planejamento, criação e/ou diagnóstico para o serviço de Arquitetura de Soluções

Para chamados de planejamento, criação e/ou diagnóstico para o serviço de Arquitetura de Soluções, é agendada uma reunião com o MP para tratar da demanda solicitada. Após explicada a demanda o *broker* em até cinco dias úteis apresenta o plano de arquitetura de solução para implementação dos serviços demandados.

O plano de arquitetura contém, no mínimo, as seguintes informações:

a) Descrição detalhada do serviço demandado;

b) Arquitetura proposta pelo *broker* para implementação do serviço demandado;

c) Orçamento detalhado dos serviços que serão usados pelo provedor para implementação do serviço demandado com o preço efetivamente cobrado pelo *broker*;

d) Orçamento detalhado dos serviços do *broker* que serão usados para implementação do serviço demandado e planilha de comparação de custos em ambiente *on-premises*;

e) Prazo para entrega dos serviços em perfeita operação;

f) Descrição detalhada de restrições, dependências e quaisquer informações relevantes acerca do plano proposto.

O MP analisa o plano de arquitetura de modo a verificar se contêm todos os requisitos técnicos listados acima. Caso contrário, solicita ao *broker* que refaça o plano de arquitetura, sem reinício de contagem de prazo. Após o aceite do plano de arquitetura, o MP analisa o plano e decide se os serviços demandados serão implementados. Quando uma aplicação ou serviço na nuvem entra em produção, há um período de estabilização de um mês para que os níveis de serviço sejam totalmente aferidos e entregues ao MP.

7.3.1.6.3 Chamados de planejamento, criação e/ou diagnóstico para os demais serviços e de execução, alteração, implantação e/ou exclusão

Se necessário, para os chamados de planejamento, criação e/ou diagnóstico (exceto o de Arquitetura de Solução) e de execução, alteração, implantação e/ou exclusão, o *broker* pode agendar reunião presencial ou virtual para tratar da demanda solicitada. A contagem do prazo para execução do serviço terá início no dia útil subsequente ao da realização da reunião. Após a execução dos serviços, o MP realiza a análise dos serviços implementados, para verificar se estão em conformidade com o plano de arquitetura. Caso contrário, solicita ao *broker* que refaça os serviços, sem reinício de contagem de prazo. Durante a análise o prazo do *broker* será suspenso.

O MP pode solicitar demanda de execução, alteração, implantação e/ou exclusão sem que tenha existido correspondente demanda de planejamento, criação e/ou diagnóstico. Sendo assim, a demanda pode ter como fonte algum plano de arquitetura elaborado em chamado prévio de planejamento, criação, diagnóstico e/ou plano de arquitetura elaborado por servidor do MP. A fonte da demanda deve fazer parte da ordem de serviço de execução, alteração, implantação e/ou exclusão.

7.3.1.6.4 Chamados de Suporte Técnico

Exige-se que o *broker* mantenha central de atendimento para abertura de chamados no regime 365x24x7 para atendimento dos chamados de suporte técnico. A central é acionada, preferencialmente, por meio de ligação gratuita ou ligação local em Brasília, podendo o *broker* disponibilizar abertura de chamados pela internet. O atendimento deve ser realizado em língua portuguesa. Na abertura do chamado, o *broker* deve fornecer um número de registro único para acompanhamento de cada chamado. O chamado é registrado em sistema de acompanhamento de chamados do MP, e o número de registro é fornecido ao *broker* em cada interação que envolva o chamado. Em qualquer mudança na situação de chamados é encaminhada uma notificação ao MP, contendo as informações de registro do chamado, para endereço de e-mail previamente designado, inclusive quando há mudança de status interrompendo a contagem de Nível Mínimo de Serviço (NMS). Os chamados abertos somente podem ser concluídos e fechados após autorização do MP.

7.3.1.6.5 Alteração dos Catálogos de serviços

Os catálogos referentes aos serviços de computação em nuvem e aos serviços técnicos especializados somente poderão ser alterados pelo órgão gerenciador da Ata de Registro de Preços. A alteração dos catálogos deverá ser formalizada por meio de aditivo contratual.

A alteração dos catálogos consiste somente na inclusão de novos serviços, contendo a motivação, a descrição do serviço, sua unidade e valor de referência (USN). Os novos

serviços não poderão redundar na execução majoritária em relação aos demais itens do contrato. A inclusão ficará limitada a 8 (oito) serviços para os serviços de computação em nuvem e 8 (oito) serviços para os serviços técnicos especializados. O valor de referência de USN será dimensionado utilizando-se como referência valores adotados por no mínimo três provedores de nuvem e o valor de referência de UST será dimensionado utilizando-se como referência valores adotados por no mínimo três integradores de nuvem.

7.3.1.7 Prova de Conceito

Para fins de Prova de Conceito, o Ministério do Planejamento, Desenvolvimento e Gestão (MP) solicitou à ofertante do menor preço que demonstrasse a execução dos serviços para verificar se atendiam aos seus requisitos. Na prova de conceito a empresa licitante configurou ambientes de serviços de computação em nuvem no provedor integrante da solução, e executou as ordens de serviços conforme plano de demonstração constante do edital. O Plano de demonstração de serviços era composto de três ordens de serviço que abrangiam uma grande gama dos serviços listados no edital, além da ferramenta de gestão de nuvem.

Caso não configurasse o ambiente no provedor, ou não cumprisse qualquer um dos itens das ordens de serviço, nos termos e prazos estabelecidos pelo MP a empresa seria desclassificada e a licitante classificada na posição imediatamente posterior seria convocada para a demonstração dos serviços.

7.3.1.8 Avaliação e recebimento do objeto

O *broker* apresenta, até o quinto dia útil do mês, relatório com todas as ordens de serviços executadas e homologadas no mês anterior. O relatório deve listar, quando couber, os serviços do provedor de nuvem, e a respectiva quantidade de USNs utilizadas, bem como os serviços de suporte técnico do *broker*, e a respectiva quantidade de USTs utilizadas e o serviço de Treinamento.

O relatório é enviado aos fiscais técnicos, por e-mail, antes da emissão da fatura, para validação, e deve constar a aferição dos Níveis de Serviços, assim como o cálculo das glosas, para posterior validação dos demais fiscais do contrato, procedendo-se ao aceite se estiver em conformidade.

A entrega dos relatórios mensais é condição fundamental e necessária para o pagamento referente a cada mês de prestação dos serviços. O relatório deverá conter no mínimo:

a) número da(s) Ordem(ns) de Serviço;

b) descrição dos serviços;

c) período de execução dos serviços;

d) quantidade (USN, UST ou Turma de Treinamento);

e) aferição dos Níveis de Serviços;

f) valor total devido.

7.3.1.9 Sanções

O contrato do MP inclui penalidades para inexecução parcial do contrato e outras sanções recorrentes em contratos de contratações públicas, destacamos porém, que referentes ao serviço de computação em nuvem, constituem motivação para aplicação de multa de 5% (cinco por cento) sobre o valor total do contrato e rescisão unilateral por descumprimento contratual, sem prejuízo de outras sanções cabíveis:

a) processamento, armazenamento ou replicação dos dados e informações fora do território brasileiro;

b) vazamento ou permissão de acesso por terceiros às informações sem prévia autorização formal do órgão proprietário e do MP ou autorização legal pela Justiça Brasileira;

c) não informação ao MP de solicitação de acesso aos dados e informações por parte de terceiros ou governos estrangeiros, mesmo se respaldado em autorização judicial não respaldada pela Justiça Brasileira;

d) falhas de criptografia ou armazenamento de chaves que possibilitem o acesso indevido às informações sob a guarda do *broker* ou do provedor;

e) falha no serviço de backup que impeça a restauração de dados copiados, sem prejuízo da cobrança pelo serviço de recuperação das informações eventualmente perdidas e outras ações inclusive judiciais cabíveis;

f) impedimento por qualquer motivo à descarga dos dados e informações de propriedade do MP para efeito de migração de aplicação para outro provedor.

Constam ainda no contrato, multas por atraso para conclusão dos serviços técnicos especializados e não comprovação de contar com o(s) profissional(is) com a formação exigida para a prestação dos Serviços técnicos especializados.

7.3.2 Contratos da Ata de Registro de Preços nº 06/2018

A ata de registro de preços nº 06/2018 foi assinada no dia 21 de dezembro de 2018, portanto não tem ainda um ano de sua assinatura. A partir de fevereiro de 2019 os órgãos partícipes têm assinado seus contratos.

Foram assinados até o final de junho de 2019 os seguintes contratos:

a) Agência Brasileira Gestora de Fundos Garantidores e Garantias S.A. (ABGF), contrato nº 3/2019, assinado em 21/02/2019;

b) Fundação Escola Nacional de Administração Pública (ENAP), contrato nº 1/2019, assinado em 11/03/2019;

c) Conselho Administrativo de Defesa Econômica (CADE), contrato nº 7/2019, assinado em 22/03/2019;

d) Instituto do Patrimônio Histórico e Artístico Nacional (IPHAN), contrato nº 9/2019, assinado em 10/04/2019;

e) Instituto Federal de Educação, Ciência e Tecnologia do Piauí (IFPI), contrato nº 12/2019, assinado em 31/05/2019.

Em 02 de julho de 2019, foi realizada reunião com Douglas Ferreira Fernandes, Gerente de Tecnologia da Informação da ABGF, que foi o primeiro dos partícipes a assinar contrato. A ABGF tinha realizado o treinamento constante do contrato e havia aberto apenas uma OS para utilização dos serviços em nuvem. A OS aberta, em relação ao processo de demanda que está detalhado na Figura 6 da página 111, encontrava-se ainda na fase de aprovação do cenário, o qual havia sido aprovado momentos antes da reunião.

A opinião sobre o contrato e sobre a tecnologia de computação em nuvem é bastante favorável, mas o uso do contrato ainda é insignificante. Contudo, chamou a atenção o fato de que já foi sentida a falta no catálogo de serviços do MP de serviços de banco de dados. O gerente de TI da ABGF informou que foi possível contornar a falta desse serviço no catálogo pela utilização de outros serviços existentes, mas é possível que em outras situações o engessamento do processo de alteração do catálogo de serviços possa ser um impeditivo. Informou ainda que, até o momento não têm a possibilidade de acesso direto ao portal de serviços do provedor. Acreditam ser uma limitação do contrato, pois a interface personalizada restringe o acesso aos serviços contratados. Consideram que o acesso pelo portal de serviços do provedor seria desejável, mesmo que apenas com permissão de leitura.

7.4 Análise das Contratações

Nesta seção foi realizada a análise das contratações do TCU e do MP. A seção foi dividida em subseções, sendo a subseção 7.4.1 para tratar dos critérios para a seleção do fornecedor, a subseção 7.4.2 para tratar dos critérios de execução contratual e gestão dos serviços e a subseção 7.4.3 para a conclusão da análise.

7.4.1 Análise dos critérios de seleção do fornecedor dos editais do TCU e do MP

Com base nos 19 (dezenove) critérios que foram definidos na seção 7.1, no Quadro 10 da página 92, buscou-se localizar no edital uma referência clara ao critério, de forma que os mesmos se encontram listados no Quadro 15 abaixo.

Quadro 15 – Avaliação das Contratações com relação aos critérios para a seleção do fornecedor

Ref.	**Critério**	**TCU**	**MP**
SF1	Deve ser representante de pelos menos dois provedores de nuvem	Sim, 4.1 do anexo I do edital	Não, apenas 1, 5.1.1 do anexo I do edital
SF2	Deve possuir pessoal qualificado para trabalhar com o(s) provedor(es) de nuvem da solução	Sim, 4.38 do anexo I do edital	Sim, 5.2.11 do anexo I do edital
SF3	Deve trabalhar com multirregiões e poder transferir carga de uma região para outra	Sim, 4.25.11 do anexo I do edital	Sim, 5.1.24.17 do anexo I do edital
SF4	Deve implementar políticas e procedimentos para o uso de criptografia, incluindo gerenciamento de chaves criptográficas	Sim, 4.26 do anexo I do edital	Sim, 5.1.24 diversos subitens do anexo I do edital
SF5	Possibilitar o armazenamento das chaves criptográficas fora do ambiente de nuvem	Sim, 4.26 do anexo I do edital	Sim, diversos subitens do 5.1.24 do anexo I do edital
SF6	O provedor deve garantir e demonstrar isolamento de recursos e de dados de seus clientes	Não	Sim, 6.1.19 do anexo I do edital
SF7	O provedor deve garantir controles eficazes e compatíveis com as políticas e procedimentos do cliente para gerenciamento de identidades de usuários e controle de acessos	Sim, 4.39 do anexo I do edital	Sim, 6.2 do anexo I do edital

Continua na próxima página

Quadro 15 – Continuação

Ref.	**Critério**	**TCU**	**MP**
SF8	O acesso e uso de ferramentas de auditoria que interajam com os sistemas de informação das organizações deverão estar devidamente segmentados e restritos para evitar comprometimentos e uso indevido de dados de *log*	Não	Não
SF9	O modelo de segurança das interfaces do provedor deve ser desenvolvido com base em padrões de mercado, incluindo mecanismos de autenticação forte de usuários e controle de acesso para restringir o acesso aos dados do cliente	Não	Sim, 6.1.14 do anexo I do edital
SF10	Políticas, procedimentos e mecanismos devem ser estabelecidos e implementados pelo provedor para gerenciamento de vulnerabilidades conhecidas e atualizações de software, garantindo que aplicações, sistemas e vulnerabilidades de dispositivos de rede sejam avaliadas, e que atualizações de segurança fornecidas sejam aplicadas em tempo hábil, priorizando os *patches* mais críticos	Não	Sim, 6.1.12 do anexo I do edital
SF11	O processo de gestão de vulnerabilidades do provedor deve ser transparente ao cliente	Não	Sim, 6.1.12 do anexo I do edital
SF12	Os provedores devem utilizar pacotes modulares, usar formatos abertos ou populares para dados e serviços, e serem transparentes em regulações e taxas aplicadas à transferência de dados	Não	Sim, 10.3 do anexo I do edital
SF13	Processos, procedimentos e recursos devem ser estabelecidos e testados, de maneira a viabilizar a transferência de operações de um provedor de computação em nuvem para outro provedor alternativo	Sim, 4.12 e 6 do anexo I do edital	Sim, 6.1.8 do anexo I do edital

Continua na próxima página

Quadro 15 – Continuação

Ref.	**Critério**	**TCU**	**MP**
SF14	O provedor deverá possuir programa de formação de profissionais aberto para o mercado	Sim, 4.25.12 do anexo I do edital	Não
SF15	O provedor deve implementar controles para isolamento e segurança de sistema operacional	Não	Sim, 6.1.19 do anexo I do edital
SF16	O provedor deve utilizar soluções de virtualização que sejam padrões ou referências de mercado	Não	Sim, 10.4 do anexo I do edital
SF17	O provedor deve implementar política de atualização de versão de software e aplicação de correções	Não	Sim, 6.1.24.6 do anexo I do edital
SF18	O provedor deve possuir certificação ISO 27001 e 27017	Sim, 4.25.1 do anexo I do edital	Sim, 6.1.16 do anexo I do edital
SF19	O provedor deve possuir certificação ISO 27018	Sim, 4.25.1 do anexo I do edital	Sim, 6.1.16 do anexo I do edital

Fonte: elaboração própria

Após a apuração dos critérios definidos nos editais, deve-se entender, quando for o caso, o porquê de não terem sido previstos alguns critérios específicos. No caso do MP praticamente todos os critérios levantados foram atendidos, só não estando especificados claramente no edital os itens SF1, SF8 e SF14. Já no caso do TCU, foram um total de 9 (nove) dos 19 (dezenove) critérios não atendidos, que foram os critérios SF6, SF8, SF9 a SF12, e SF15 a SF17.

Analisando os não atendidos pelo MP, percebe-se que quanto ao critério SF1, o MP decidiu utilizar apenas um provedor de serviços em nuvem, mas no item 5.1.22 do edital prevê que todas as aplicações sejam portáveis para outros provedores, o que visa atender a um dos objetivos do critério, que é evitar o *vendor lock-in*. Contudo, parece mais segura a opção do TCU, já que, além de ser possível testar a migração entre provedores, se tem a garantia de redundância no caso de falha de um provedor. Quanto ao item SF8, que foi o único item não atendido por nenhum dos dois órgãos, podemos perceber que ele é atendido em parte pelas certificações ISO 27001 e ISO 27017, objetivos e controles A9 – Controle de acesso e A12 – Segurança nas operações, porém depende também de como são feitas as restrições de acesso no próprio órgão, o que pode ser o motivador para a não exigência desse item. Já em relação ao critério SF14, o MP tem a exigência de treinamento no edital, mas não exige que o programa de formação do provedor seja aberto ao mercado.

Essa solução atende no primeiro momento, mas em caso de necessidade de formação de mais servidores, ou contratação de pessoal especializado pode restringir as opções do órgão. Entende-se que essa exigência é interessante até mesmo para o órgão assumir no futuro a função do *broker*.

Pode-se perceber que o TCU não atendeu a um grande número de critérios, pois os mesmos não estão claramente definidos no edital. Porém, quase a totalidade dos itens não atendidos estão cobertos pelas certificações ISO 27001 e ISO 27017, objetivos e controles A9 – Controle de acesso, A10 – Criptografia e A12 – Segurança nas operações. Entretanto, não existe a exigência de utilização de padrões de mercado e transparência das políticas e processos aos clientes. Entende-se que é importante para o órgão, para evitar o *vendor lock-in* e garantir a segurança dos processos estas exigências, o que é plenamente atendido no edital do MP.

A partir desta análise, entende-se que os critérios definidos são os que melhor atendem às exigências a serem feitas para a seleção do fornecedor. Contudo, dependendo da maturidade da organização no processo de auditoria de sistemas, pode-se exigir ou não o critério SF8.

7.4.2 Análise dos critérios de execução contratual e gestão do serviços de nuvem do TCU e do MP

Com base nos 39 (trinta e nove) critérios que foram definidos na seção 7.1, no Quadro 11 da página 94, buscou-se localizar no edital referência clara ao critério, de forma que os mesmos se encontram listados no Quadro 16 abaixo.

Quadro 16 – Avaliação das Contratações com relação aos critérios para execução contratual e gestão dos serviços

Ref.	Critério	TCU	MP
CG1	OS SLAs com o provedor de nuvem devem ser cuidadosamente definidos e exequíveis, o que inclui penalidades em caso de não cumprimento	Sim, 4.25.3, 4.39 do anexo I, 6 e 7 do anexo III do edital	Sim, 21 do edital e 15 do anexo I do edital
CG2	Os dados devem ser submetidos à classificação prévia da informação, antes de serem transmitidos para a nuvem	Não	Sim, anexo III do edital
CG3	Implementar controle de acesso lógico apropriado ao grau de confidencialidade dos dados armazenados na nuvem	Não	Sim, 6.2 do anexo I do edital

Continua na próxima página

Quadro 16 – Continuação

Ref.	**Critério**	**TCU**	**MP**
CG4	Implementar controles para transferência de dados, como criptografia e uso de VPN adequada	Sim, 4.25 do anexo I do edital	Sim, 5.1.24.22 e 6.1.15 do anexo I do edital
CG5	As chaves criptográficas não devem ser armazenadas na nuvem	Não	Sim, 6.4 do anexo I do edital
CG6	Estabelecer limites do acesso do provedor aos dados do cliente	Sim, 4.18 do anexo I do edital	Sim, 6.1.11 do anexo I do edital
CG7	Os dados armazenados devem estar criptografados, sendo que o esquema criptográfico deve ser adequado à classificação das informações	Sim, 4.25 do anexo I do edital	Sim, 6.3 do anexo I do edital
CG8	O provedor deve assegurar que dados sujeitos a limites geográficos não sejam migrados para além de fronteiras definidas em contrato	Sim, 4.25.11 e 6.3.14 do anexo I do edital	Sim, 5.1.8 e 6.1.23 do anexo I do edital
CG9	Estabelecer responsabilidade do provedor em garantir o isolamento de recursos e dados contra acesso indevido por outros clientes	Sim, 4.13.2 e 4.13.3 do anexo I do edital	Sim, 6.1.23 do anexo I do edital
CG10	A política para gestão de mudanças deve ser acordada entre provedor e cliente, e este último deve ser comunicado com antecedência sobre mudanças (por exemplo, utilizando processos do ITIL)	Não	Não
CG11	*Logs* de auditoria do provedor que registram atividades de acesso de usuários privilegiados, tentativas de acesso autorizados e não autorizados, exceções do sistema, e eventos de segurança da informação devem ser mantidos em conformidade com as políticas e regulamentos aplicáveis, e devem estar de acordo com as políticas do cliente	Não	Sim, 5.1.10.4 e 5.1.24.31 do anexo I do edital

Continua na próxima página

Quadro 16 – Continuação

Ref.	**Critério**	**TCU**	**MP**
CG12	Definir políticas e procedimentos que devem ser estabelecidos para triagem dos eventos relacionados à segurança e garantir o gerenciamento de incidentes completo e ágil	Sim, 2.10 do Anexo III do edital	Sim, 6.1.4, 6.1.6 e 6.1.10 do anexo I do edital
CG13	Quaisquer eventos de segurança de informação devem ser comunicados através de canais predefinidos de comunicação, de maneira rápida e eficiente, e de acordo com os requisitos legais, regulatórios e contratuais	Sim, 2.10 do Anexo III do edital	Sim, 6.1.4, 6.1.6 e 6.1.10 do anexo I do edital
CG14	O cliente deve prever cópia dos *logs* fornecidos pelo provedor, de acordo com sua própria política de retenção; deve haver, da parte do provedor, um mecanismo para filtragem e cópia dos *logs* gerados pelo fornecedor para a área do cliente	Não	Sim, 6.1.17 do anexo I do edital
CG15	Estabelecer direitos claros e exclusivos de propriedade e acesso aos dados, inclusive referentes a *logs*	Não	Sim, 5.1.10.4 e 5.1.20 do anexo I do edital
CG16	Definir as obrigações do provedor quanto a requisitos mínimos de autorização e transparência de acesso do provedor aos ativos físicos e virtuais do cliente, bem como a respeito da necessidade de divulgação ao cliente de suas políticas e orientações específicas	Não	Sim, 6.1.23 do anexo I do edital
CG17	Definir as obrigações do provedor quanto a requisitos mínimos de contratação de pessoal e de monitoramento de suas atividades, bem como a respeito da necessidade de divulgação ao cliente de suas políticas e orientações específicas	Sim, 4.31 e 4.38 do anexo I do edital	Sim, 5.2 do anexo I do edital

Continua na próxima página

Quadro 16 – Continuação

Ref.	**Critério**	**TCU**	**MP**
CG18	Definir a necessidade de realização de avaliações periódicas independentes, com a finalidade de verificar a adequação dos controles do provedor a um conjunto de critérios pré-definidos	Não	Sim, 6.1.5 e 6.1.12 do anexo I do edital
CG19	Especificar mecanismos de segurança e proteção de propriedade intelectual, e quaisquer requisitos legais ou regulatórios	Não	Sim, 22.2.10 do anexo I do edital
CG20	Especificar nível esperado dos serviços (SLA) e mecanismos clássicos de gestão contratual de serviços terceirizados (comunicações formais, multas, rescisão etc)	Sim, 5.23 do anexo I, 6 e 7 do anexo III do edital	Sim, 15 do anexo I do edital
CG21	Estabelecer processos ágeis de migração para provedores alternativos, em caso de falhas do provedor principal	Sim, 4.13.6 do anexo I do edital	Sim, 10.2, 10.11 do anexo I e 5 do anexo V do edital
CG22	Deve assegurar a conformidade dos dados e aplicações hospedadas na nuvem com os requisitos de padrões, legais e regulatórios, aos quais o negócio está sujeito, de maneira contínua e atualizada	Sim, 4.22 do anexo I do edital	Sim, 6.1.2 do anexo I do edital
CG23	Avaliar quais informações serão hospedadas na nuvem, considerando o processo de classificação da informação, o valor do ativo de informação, os controles de acesso físicos e lógicos, o modelo de serviço e de implementação de computação em nuvem e a localização geográfica onde as informações serão armazenadas (item 5.3 da Norma Complementar 14/IN01/DSIC/GSIPR)	Não	Sim, 6.1 e subitens do anexo I do edital

Continua na próxima página

Quadro 16 – Continuação

Ref.	**Critério**	**TCU**	**MP**
CG24	Deve prever soluções de contingência independentes de provedor específico (portabilidade do serviço para outro provedor)	Sim, 4.13.6 do anexo I do edital	Sim, 6.1.8 do anexo I do edital
CG25	Assegurar os níveis de serviço no caso de interrupções de serviço planejadas ou não planejadas	Sim, 4.25 e subitens do anexo I do edital	Sim, 5.1.14 do anexo I do edital
CG26	Prever modelo de remuneração vinculada aos níveis de serviço estabelecidos, prevendo glosas no caso de descumprimento de parâmetros mínimos	Sim, Cláusula 13 do anexo III do edital	Sim, 21 do edital
CG27	Definir sanções no caso de descumprimento reiterado de parâmetros mínimos de níveis de serviço estabelecidos	Sim, item 6 e 7 do anexo III do edital	Sim, 15 do anexo I do edital
CG28	Assegurar que todas as vulnerabilidades sejam priorizadas e corrigidas dentro de SLAs acordados contratualmente entre cliente e provedor	Não	Sim 6.1.21 do anexo I do edital
CG29	Definir divisão clara de papéis de cliente e provedor	Sim, 4.39 do anexo I do edital	Sim 6 e subitens do anexo I do edital
CG30	Estabelecer indicadores claros e precisos tanto de ambiente como de segurança, com responsáveis pelo seu monitoramento e disponibilização	Sim, item 4.13.2, 4.36, 4.39, 5.22 e 5.23 do anexo I do edital	Sim, 5.2.11.2 e 5.2.18.25 do anexo I do edital
CG31	O contrato deverá prever verificações intermediárias do nível de uso da capacidade contratada, alertas quando atingidos patamares de recursos e tetos de recursos máximos utilizáveis em função do orçamento disponível	Não	Sim, item 5.1.10 do anexo I do edital
CG32	Prever condições e limites claros de custos para saída do provedor	Não	Não

Continua na próxima página

Quadro 16 – Continuação

Ref.	**Critério**	**TCU**	**MP**
CG33	Especificar que os direitos de propriedade sobre os dados armazenados na nuvem pela organização são exclusivos da organização	Sim, 4.18 do anexo I do edital	Sim, itens 5.1.20 e 10.10 do anexo I do edital
CG34	Definir em quais países os dados do cliente podem ser armazenados	Sim, 4.25.11 do anexo I do edital	Sim, item 5.1.8 do anexo I do edital
CG35	Definir que o provedor deve atender à política de exclusão de dados do cliente	Não	Sim, item 10.9 do anexo I do edital
CG36	Utilizar criptografia para proteger os dados de acesso indevido	Sim, 4.26 do anexo I do edital	Sim, item 6.3 do anexo I do edital
CG37	Utilizar técnicas de marca d'água para identificar origens de vazamento de informações sigilosas	Não	Não
CG38	O contrato deve detalhar definições específicas de incidentes, eventos, ações a serem tomadas e responsabilidades do provedor e do cliente	Sim, 2.10 do Anexo III do edital	Sim, 6.1.4 do anexo I do edital
CG39	O contrato deve definir requisitos de interoperabilidade entre as ferramentas de gestão de incidentes do provedor e do cliente	Não	Sim, 6.1.10 do anexo I do edital

Fonte: elaboração própria

Com relação aos critérios de execução contratual e gestão presentes nos editais dos órgãos, a exemplo do que ocorre com os critérios de seleção do fornedor, deve-se entender o porquê de alguns deles não terem sido utilizados. Novamente, no caso do MP praticamente todos os critérios levantados foram atendidos, só não estando especificados claramente no edital os itens CG10, CG32 e CG37, já no caso do TCU, foram um total de 17 (dezessete) dos 39 (trinta e nove) critérios não atendidos, que foram os critérios CG2, CG3, CG5, CG10, CG11, CG14, CG15, CG16, CG18, CG19, CG23, CG28, CG31, CG32, CG35, CG37 e CG39.

Analisando os não atendidos pelo MP, percebe-se que todos eles também não foram atendidos pelo TCU, o que poderia levar à exclusão dos critérios, porém entende-se que os critérios CG10 e CG32, apesar de não tratados, são essenciais, pois é necessário tanto a comunicação de mudanças no provedor, que podem implicar nas aplicações do órgão, como

ter ciência das condições e custos de saída do provedor. Por esse motivo esses critérios foram mantidos. Apenas o critério CG37 não foi entendido como essencial, mas deve ser avaliado por órgãos onde o conhecimento de onde partiram eventuais vazamentos de informação seja primordial, o que implica em uma avaliação mais criteriosa da relação custo-benefício da adoção.

Pode-se perceber que o TCU não atendeu a 43,59% dos critérios, pois os mesmos não estão claramente definidos no edital. Em relação aos critérios que tratam de classificação de informação, ressalta-se que apesar de não terem sido encontradas referências no edital, em entrevista com a servidora do TCU foi esclarecido que esse passo acontece antes da colocação do serviço em nuvem, pela área responsável pelos dados. Com relação a outros critérios se repete o entendimento de que estão cobertos pelas certificações ISO 27001 e ISO 27017. Dentre todos os critérios não atendidos, a falta de referência aos *logs* foi o que mais se destacou. Entende-se que é importante garantir esta rastreabilidade, o que é atendido no edital do MP.

Com esta análise, entende-se que os critérios definidos são os que melhor atendem às exigências a serem feitas para a execução contratual e gestão dos serviços. Optou-se apenas por retirar o critério CG37 e renumerar os restantes.

7.4.3 Conclusão da análise das contratações do TCU e do MP

Durante a análise das contratações do TCU e do MP que foram feitas nas seções anteriores, pudemos verificar que ambos os contratos, apesar de serem soluções bem estruturadas pelos órgãos, são recentes e seu uso é ainda muito baixo, não proporcionando uma possibilidade de avaliação inconteste dos pontos positivos e negativos de cada um. Contudo, há alguns pontos que devem ser ressaltados.

Quanto à quantidade de provedores contratados, parece ser a decisão do TCU a mais adequada, pois além de possuir a redundância em caso de falha, saída do mercado ou algum outro problema com um provedor, é possível testar efetivamente se os serviços migrados para a nuvem podem ser providos por mais de um provedor buscando mitigar o risco do *vendor lock-in*.

Outro ponto positivo do contrato do TCU é a exigência do programa de formação de profissionais em serviços de nuvem do provedor ser aberto ao mercado, proporcionando a possibilidade de formação do pessoal do órgão, além de possibilitar a contratação de profissionais no mercado.

Parece que a metodologia de quantificação do valor em USN do serviço de nuvem do TCU possibilita a utilização de novos serviços que estão sendo disponibilizados pelos provedores com mais agilidade que a definição do MP de um catálogo de serviços. A solução do TCU parece ser mais flexível e adequada a uma tecnologia que está em constante

inovação como a de serviços em nuvem.

A ferramenta de orquestração é um dos pontos que ainda merece um maior amadurecimento, pois apesar de as entrevistas com a Primesys, TCU e ABGF apontarem para uma solução dos problemas de faturamento enfrentados pelo TCU por meio da utilização do uCloud da Ustore, não houve ainda nenhum faturamento nos contratos do MP para poder confirmar a eficácia da ferramenta.

Outro ponto que merece um aprofundamento é quanto à questão de saída da nuvem ou mudança de provedor ao final de um contrato, pois apesar de ambos os contratos preverem alguns custos de saída e estarem estabelecidos valores para esse serviço, não existe um planejamento real e um provisionamento para esse momento. Não há relatórios que apontem qual o custo real de saída em determinado momento, para que haja uma reserva de recursos para tanto. Corre-se o risco de que ao final do contrato o quantitativo de USTs e USNs remanecentes não seja o suficiente para a migração do serviço, gerando uma despesa sem previsão orçamentária.

Por fim, é necessário que o ANS entre o órgão e o *broker* seja mais detalhado. Já há muitas exigências quanto à qualidade do serviço oferecido pelo provedor, mas há deficiências com relação aos prazos e qualidade dos serviços oferecidos pelo *broker*, principalmente no contrato do TCU, como ficou claro na entrevista.

7.5 Conclusão do capítulo

Neste capítulo foram analisadas as contratações do TCU e do MP. Para poder fazer esta análise, na seção 7.1, foram selecionados quais os critérios que deveriam constar no edital de forma a atender aos normativos legais e técnicos que foram levantados no Capítulo 4 e no Capítulo 5. Sendo apresentados 19 (dezenove) critérios para a seleção do fornecedor e 39 (trinta e nove) critérios para a execução contratual e gestão do serviço.

Na seção 7.2 foram detalhadas as características da contratação do TCU e como tem sido a execução do contrato. Na seção 7.3 foram elencadas as características da contratação do MP e ao final do capítulo, na seção 7.4 foi realizada a análise das contratações com base nos critérios definidos na seção 7.1.

No próximo capítulo utilizaremos a análise realizada neste capítulo e os subsídios normativos apontados no Capítulo 6 para sugerir os critérios de contratação de serviços em nuvem para o Senado Federal.

8 Contratação de Serviços em Nuvem para o Senado Federal

A construção de um modelo de computação em nuvem para a APF é um dos desafios atuais no setor público brasileiro. Apesar de alguns órgãos já terem feito contratações, a quantidade é incipiente e os resultados ainda não puderam ser avaliados.

O Brasil vive um momento de crise econômica e de contingenciamento de recursos, e a Emenda Constitucional nº 95 impõe diversos fatores limitantes, que forçam os órgãos da APF a buscarem cada vez mais aumentar suas eficiências e otimizar a utilização de seus recursos.

Diante deste cenário, cabe ao Senado Federal também buscar a construção de um modelo para a contratação de computação em nuvem, e este estudo tem como objetivo "Propor critérios de contratação de serviços em nuvem para o Senado Federal". E para tanto, no decorrer deste capítulo, com base nos subsídios levantados nos capítulos anteriores serão elencados quais são os critérios essenciais que este estudo entende serem essenciais de forma a minimizar os riscos envolvidos na contratação de serviços de computação em nuvem.

Na formulação dos critérios para um modelo de contratação de serviços em nuvem para o Senado Federal utilizaremos a divisão em fases conforme a IN 1/2019, conforme vimos na análise na subseção 4.3.4. Na seção 8.1, falaremos sobre os critérios a serem adotados na fase de planejamento da contratação; na seção 8.2 serão discutidos os critérios para a fase de seleção do fornecedor; e na seção 8.3 os critérios para o contrato e sua gestão.

8.1 Critérios a serem considerados no planejamento da contratação

Para elaborar os critérios a serem considerados no planejamento da contratação, partiu-se das questões levantadas por Evangelista e Souza Neto (2016, pp. 193–194) e por controles presentes no relatório da Secretaria de Fiscalização de Tecnologia da Informação (SEFTI) do TCU (2015, pp. 50–61, Anexo I).

Nas questões levantadas por Evangelista e Souza Neto percebe-se a necessidade de possuir uma equipe técnica da TI, de aderência ao planejamento estratégico do órgão, de observância da segurança e classificação das informações, de um plano de continuidade de negócios e de um estudo técnico preliminar que analise a viabilidade da contratação. Os critérios para atender a essas questões serão discutidos nas subseções seguintes.

8.1.1 Equipe de Nuvem

Diversos estudos, como por exemplo Evangelista e Souza Neto (2016, p. 193) e Costa et al. (2019, p. 150), que ressalta que "A criação de uma equipe de nuvem é muito importante para o desenvolvimento e a condução do projeto para a Primeira Nuvem", destacam a importância de ter uma equipe designada para a condução da implantação de serviços de computação em nuvem.

A formação dessa equipe é importante para quebrar a resistência à adoção de computação em nuvem, em especial dentro das próprias áreas de TI, e para adaptar a organização às mudanças que a adoção de serviços de computação em nuvem impõe a como são providos e geridos os recursos de TI dentro da organização. Ficará a cargo dessa equipe levantar os ANS acordados com as áreas de negócio, estudar e identificar os provedores de nuvem do mercado que têm condição de atender ao órgão, identificar os processos de negócio que poderão ser impactados pela migração ou adoção de serviços de computação em nuvem e iniciar os estudos de implantação do serviço.

Diante dessa necessidade, destacamos os seguintes critérios a serem adotados para garantir o sucesso da iniciativa de adoção de serviços de computação em nuvem:

a) definir, alocar e treinar equipe de nuvem;

b) levantar os ANS acordados com as áreas de negócio;

c) identificar os provedores de nuvem que tem condição de atender ao Senado Federal;

d) identificar os processos de negócio que poderão ser impactados pela migração ou adoção de serviços de computação em nuvem.

8.1.2 PCSI, Gestão de Riscos, PDTI e Plano de contratações

A organização deve estar preparada para a adoção de serviços de computação em nuvem, e para tanto, essa adoção deve constar no plano estratégico de TI. O que no caso do Senado Federal já é percebido no Plano Diretor de Tecnologia da Informação do SF (2017b, p.12), no qual consta como ação estruturante de prioridade alta o "Plano de adoção gradual de serviços de computação em nuvem". Porém, não consta no plano de contratações do ano de 2019 nenhum projeto que aponte neste sentido. Até onde foi possível apurar, apenas a contratação de licenças do Office 365 aconteceu até agora. Devemos ainda levar em consideração, que o Office 365 trata-se de um serviço da Microsoft de ferramentas de escritório disponibilizadas em nuvem, que se caracteriza como *Software as a Service* (SaaS) e não atende ao propósito mais amplo aqui buscado. No sentido de propiciar ainda esta adoção gradual, o Prodasen adotou a plataforma de contêineres *Rancher*, está realiazando testes com o ambiente de orquestração de *cloud VMWARE*, algumas reuniões

com provedores de serviços em nuvem têm sido conduzidas e está sendo agendada uma Prova de Conceito (POC) para avaliar a possibilidade de adoção da tecnologia.

Segundo o item 5.1 da Norma complementar 14/IN01/DSIC/GSIPR (BRASIL, 2018d, item 5.1), o órgão ou entidade antes de adotar a tecnologia de computação em nuvem, deve observar as diretrizes da sua Política de Segurança da Informação e Comunicações (SIC), do seu processo de Gestão de Riscos de SIC e do seu processo de Gestão de Continuidade de Negócios nos aspectos relacionados à SIC.

Dentre os controles presentes no relatório da SEFTI do TCU (2015, risco 18), ainda encontramos a indicação de que o planejamento orçamentário deve estar alinhado com as condições de contratação de serviços de computação em nuvem, particularmente quanto à transformação de verba de investimento na compra de equipamentos de TIC para verba de custeio dos serviços de nuvem.

Para contemplar essas normas e recomendações, os seguintes critérios devem ser adotados:

a) garantir que os requisitos da contratação de nuvem estejam alinhados com a Política Corporativa de Segurança do Senado Federal e com seu processo de Gestão de Riscos de SIC;

b) as diretrizes relativas à Gestão de Continuidade deverão ser atendidas;

c) o plano de contratações do Senado Federal deverá incluir verba de custeio para serviços de nuvem.

8.1.3 Classificação e Segurança das Informações

Ao adotar o modelo de computação em nuvem, o processo de classificação de informação se reveste de uma importância fundamental, pois, segundo o item 5.2 da Norma complementar 14/IN01/DSIC/GSIPR (BRASIL, 2018d, item 5.2), são definidos critérios de tratamento a serem considerados para cada um dos tipos de informação segundo o seu grau de sigilo.

Portanto, é necessário avaliar quais informações serão hospedadas na nuvem, considerando o processo de classificação da informação, o valor do ativo de informação, os controles de acesso físicos e lógicos, o modelo de serviço e de implementação de computação em nuvem e a localização geográfica onde as informações serão armazenadas.

Para o caso do Senado Federal, a Comissão Permanente de Acesso a Dados, Informações e Documentos do Senado Federal deverá ser consultada quanto à classificação das informações que se pretende transmitir para a nuvem. E deverão ser adotados os seguintes critérios:

a) os dados devem ser submetidos à classificação prévia da informação, antes de serem transmitidos para a nuvem;

b) deverão ser implementados controle de acesso lógico apropriado ao grau de confidencialidade dos dados armazenados na nuvem;

c) deverão ser implementados controles para transferência de dados, como criptografia e uso de VPN adequada;

d) deverá ser utilizada criptografia para proteger os dados de acesso indevido;

e) deve ser assegurado que dados, metadados, informações e conhecimento, produzidos ou custodiados pelo Senado Federal, bem como suas cópias de segurança, residam em território brasileiro.

8.1.4 Plano de Contingência e Continuidade de Negócios

Para garantir a aderência ao plano de continuidade de negócios do Senado Federal, diversas questões devem ser tratadas, como: qual será a contingência para a indisponibilidade dos serviços em nuvem, que podem ocorrer por falhas no provedor, falhas na infraestrutura de rede necessária, ou até mesmo pelo encerramento do contrato com o provedor? Para garantir que as potenciais falhas não impactem na continuidade dos negócios sugere-se adotar os seguintes critérios:

a) o plano de continuidade de negócio para nuvem deve considerar mais de um provedor como contingência;

b) deve ser considerada a utilização da infraestrutura própria de TI como contingência;

c) o plano de continuidade de negócio deve considerar as partes do negócio que estão na nuvem e levar em consideração tanto as características do negócio como do provedor;

d) deve ser definido e documentado um método para determinar o impacto de qualquer indisponibilidade à organização, incluindo de serviços que estão na nuvem, que deverá, também, estabelecer prioridades para recuperação e período máximo tolerável para a indisponibilidade;

e) deverão ser estabelecidos processos ágeis de contratação e migração para provedores alternativos, em caso de falhas do provedor principal;

f) deverão ser previstas soluções de contingência independentes de provedor específico (portabilidade do serviço para outro fornecedor, contrato de contingência em caso de falha do fornecedor principal, espelhamento do serviço em infraestrutura própria etc);

g) em caso de informações críticas para o negócio, deverá ser executado plano de backup independente do fornecedor, duplicando dados em intervalos periódicos.

8.1.5 Estudo Técnico Preliminar

Durante a fase de planejamento da contratação deverá será ser realizado o estudo técnico preliminar, que irá definir o escopo e a viabilidade da contratação. Esse estudo deverá avaliar se o Senado Federal possui infraestrutura adequada e quais os requisitos necessários para a implementação do serviço.

O estudo técnico preliminar deverá avaliar se os contratos com os provedores de rede do Senado Federal estão adequados à adoção de serviços de computação em nuvem, já que os serviços que antes eram executados dentro de nossa infraestrutura e dependentes apenas da nossa rede interna, passarão a ser dependentes da Internet, e da latência e qualidade do serviço de conexão existente. É importante levantar também se o monitoramento dos provedores de rede é adequado, para que possamos identificar futuramente se uma dificuldade de acesso a um serviço de computação em nuvem é realmente uma falha do provedor de nuvem ou do provedor de rede.

Levando em conta estes fatores, os seguinte critérios deverão ser atendidos:

a) o estudo técnico preliminar deve avaliar alternativas de mercado e soluções disponíveis que se adéquam à arquitetura do Senado Federal;

b) os requisitos do Senado Federal para portabilidade e interoperabilidade devem ser cuidadosamente avaliados antes da contratação de nuvem frente às alternativas disponíveis no mercado, a fim de mitigar relações de dependência com o provedor;

c) analisar os contratos com provedores de rede a fim de adequá-los a novos parâmetros, como latência e perda de pacotes, próprios de requisitos das aplicações pretendidas em nuvem;

d) garantir que o ambiente, incluindo infraestrutura e canal de comunicação, esteja aderente às diretrizes e normas de SIC do GSI/PR, que a legislação brasileira prevaleça e que o contrato de prestação de serviço contenha cláusulas de segurança quanto às informações hospedadas na nuvem;

e) analisar se a infraestrutura de TI está dimensionada para consumir os serviços de computação em nuvem;

f) analisar se a demanda apresenta picos de processamento em curtos períodos de tempo ou, ainda, se há previsão para que a sua utilização seja aumentada ou diminuída periodicamente;

8.1.6 Critérios propostos para o planejamento da contratação

Conclui-se então que os critérios propostos para o planejamento da contratação são os dispostos no Quadro 17.

Quadro 17 – Critérios propostos para o Planejamento da Contratação

Nº	**Critério**
PC1	definir, alocar e treinar equipe de nuvem
PC2	levantar os ANS acordados com as áreas de negócio
PC3	identificar os provedores de nuvem que tem condição de atender o Senado Federal
PC4	identificar os processos de negócio que poderão ser impactados pela migração ou adoção de serviços de computação em nuvem
PC5	garantir que os requisitos da contratação de nuvem estejam alinhados com a Política Corporativa de Segurança do Senado Federal e com seu processo de Gestão de Riscos de SIC
PC6	as diretrizes relativas à Gestão de Continuidade deverão ser atendidas
PC7	o plano de contratações do Senado Federal deverá incluir verba de custeio para serviços de nuvem
PC8	os dados devem ser submetidos à classificação prévia da informação, antes de serem transmitidos para a nuvem
PC9	deverão ser implementados controle de acesso lógico apropriado ao grau de confidencialidade dos dados armazenados na nuvem
PC10	deverão ser implementados controles para transferência de dados, como criptografia e uso de VPN adequada
PC11	deverá ser utilizada criptografia para proteger os dados de acesso indevido
PC12	deve ser assegurado que dados, metadados, informações e conhecimento, produzidos ou custodiados pelo Senado Federal, bem como suas cópias de segurança, residam em território brasileiro
PC13	o plano de continuidade de negócio para nuvem deve considerar mais de um provedor como contingência
PC14	deve ser considerada a utilização da infraestrutura própria de TI como contingência
PC15	o plano de continuidade de negócio deve considerar as partes do negócio que estão na nuvem e levar em consideração tanto as características do negócio como do provedor

Continua na próxima página

Quadro 17 – Continuação

Nº	Critério
PC16	deve ser definido e documentado um método para determinar o impacto de qualquer indisponibilidade à organização, incluindo de serviços que estão na nuvem, que deverá, também, estabelecer prioridades para recuperação e período máximo tolerável para a indisponibilidade
PC17	deverão ser estabelecidos processos ágeis de contratação e migração para provedores alternativos, em caso de falhas do provedor principal
PC18	deverão ser previstas soluções de contingência independentes de provedor específico (portabilidade do serviço para outro fornecedor, contrato de contingência em caso de falha do fornecedor principal, espelhamento do serviço em infraestrutura própria etc)
PC19	em caso de informações críticas para o negócio, deverá ser executado plano de backup independente do fornecedor, duplicando dados em intervalos periódicos
PC20	o estudo técnico preliminar deve avaliar alternativas de mercado e soluções disponíveis que se adéquam à arquitetura do Senado Federal
PC21	os requisitos do Senado Federal para portabilidade e interoperabilidade devem ser cuidadosamente avaliados antes da contratação de nuvem frente às alternativas disponíveis no mercado, a fim de mitigar relações de dependência com o provedor
PC22	analisar os contratos com provedores de rede a fim de adequá-los a novos parâmetros, como latência e perda de pacotes, próprios de requisitos das aplicações pretendidas em nuvem
PC23	garantir que o ambiente, incluindo infraestrutura e canal de comunicação, esteja aderente às diretrizes e normas de SIC do GSI/PR, que a legislação brasileira prevaleça e que o contrato de prestação de serviço contenha cláusulas de segurança quanto às informações hospedadas na nuvem
PC24	analisar se a infraestrutura de TI está dimensionada para consumir os serviços de computação em nuvem
PC25	analisar se a demanda apresenta picos de processamento em curtos períodos de tempo ou, ainda, se há previsão para que a sua utilização seja aumentada ou diminuída periodicamente

Fonte: elaboração própria

8.2 Critérios a serem considerados na seleção do fornecedor

Com relação ao critérios a serem considerados na seleção do fornecedor, a base desses critérios são os que estão definidos no Quadro 10 da página 92, contudo por meio

da análise das contratações do TCU e do MP, que se encontra na seção 7.4, em especial na subseção 7.4.1 da página 121, optou-se por retirar o critério SF8 e renumerar os demais já que o mesmo não foi atendido por nenhum dos órgãos, e tampouco foi citado como ponto de melhoria nas entrevistas, e renumerar os demais.

8.2.1 Objeto da contratação

Quanto ao objeto da contratação, tanto o pregão eletrônico nº 22/2017 do TCU como o pregão eletrônico nº 29/2018 do MP, tiveram como objeto a contratação de um *broker*, que intermediaria serviços de computação em nuvem sob demanda, prestaria serviços técnicos especializados e treinamento. O TCU informou que a contratação por meio de *broker* se deu porque os provedores de nuvem de mercado não assinariam os contratos diretamente com a APF e sim por meio de parceiros.

O grande diferencial entre os dois contratos nesse sentido, é a exigência pelo TCU de que o *broker* fornecesse serviço de dois provedores de nuvem distintos, garantindo redundância e possibilidade de migração de serviços entre os provedores mitigando o risco de *vendor lock-in*. O MP, em itens do edital, tenta mitigar o risco de *vendor lock-in* apenas com a restrição de utilização de funções ou serviços exclusivos. Neste estudo entende-se que a solução de dois provedores dada pelo TCU é a mais adequada e abrangente.

8.2.2 Serviços de computação em nuvem

A definição dos serviços em computação em nuvem necessários para cada órgão da APF e como encontrar uma forma de comparar o valor dos serviços em cada um dos provedores de nuvem é um dos grandes desafios da contratação de serviços em nuvem. Cada provedor de serviço tem uma forma diferente de comercialização e serviços distintos.

Tanto o TCU quanto o MP utilizaram uma métrica de Unidade de Serviços em Nuvem (USN) cuja função é explicada pelo MP como:

> 5.1.5.1. A USN visa estabelecer-se como método previsível, linear e flexível para obtenção de uma quantidade objetivamente definida a ser cobrada pelos serviços de computação em nuvem. A métrica de USN consiste no estabelecimento de valor de referência específico para cada tipo de serviço de nuvem, conforme métrica individual associada ao consumo dos recursos.
>
> (MP, 2018b, p. 6, item 5.1.5.1)

Tanto o TCU quanto o MP elaboraram uma lista mínima de serviços que deveriam ser atendidos pelos provedores e criaram uma forma de cálculo do valor em USN de cada um dos serviços. A fórmula de cálculo do TCU para qualquer serviço do catálogo do provedor está claramente expressa no item 4.8 do anexo I do edital. Já o MP, não

estabelece uma fórmula para tal, e apresenta em uma tabela os valores em USN para cada um dos serviços exigidos.

Dado que a quantidade de serviços disponíveis em nuvem cresce em um ritmo alucinante, ficar preso a um catálogo de serviços fixo impede que a APF possa usufruir da inovação constante dessa tecnologia. Por esse motivo, a solução do TCU que contempla a possibilidade de adequação da tabela pública de preços para um valor em USN parece ser a melhor opção. Na subseção 8.3.2, será discutida a forma de alteração do catálogo.

Para a utilização dos serviços em nuvem é essencial a utilização da ferramenta de orquestração, que na avaliação dos editais do TCU e do MP pudemos perceber que pode ser fator decisivo para o sucesso da contratação. Por isso é necessário que a ferramenta atenda no mínimo às seguintes funcionalidades:

a) cadastrar dois ou mais provedores de nuvem, definir centros de custos (unidades virtuais às quais podem ser atribuídos projetos, e às quais podem ser associadas despesas) e o orçamento para o projeto, e provisionar todos os recursos a serem utilizados, respeitando o orçamento atribuído;

b) permitir a criação, modificação e exclusão de usuários e grupos de usuários, aos quais poderão ser atribuídas permissões de acesso;

c) atribuir usuários e permissões de acesso, monitoramento e alertas de custos e de níveis de uso;

d) isolar financeira e logicamente os recursos computacionais dos provedores de nuvem utilizados em diferentes projetos, de modo a não haver nenhum tipo de interferência entre os projetos;

e) permitir a visualização de todos os projetos e recursos;

f) configurar a governança do projeto, com possibilidade de restrição ou orientação de uso de recursos em regiões e /ou países pré-determinados;

g) possibilidade de movimentar os serviços de uma nuvem para outra, de forma automática. A movimentação inclui recursos, códigos fonte, serviços, dados, metadados, configurações e quaisquer outras informações necessárias à execução de qualquer serviço de uma nuvem para a outra, mediante acionamento manual por parte de operador humano. Uma vez dado o comando pelo operador humano, a ferramenta deverá ser capaz de realizar a migração sem intervenção humana;

h) armazenar *logs* de acesso para fins de auditoria. Os *logs* deverão ser mantidos durante toda a vigência do contrato, devendo ser entregues quando solicitados e no encerramento do contrato. O prazo de retenção desses *logs* poderão a qualquer tempo ser alterado de acordo com determinação do Senado Federal;

i) permitir que, a partir de uma interface personalizada, o usuário com as devidas permissões tenha acesso aos recursos disponíveis no provedor e consiga executar ao menos tarefas básicas (criar/alterar/excluir servidores virtuais, volumes de armazenamento, configurações de rede, etc.) relacionadas aos serviços de computação em nuvem contratados;

j) permitir monitorar as informações sobre a quantidade e o status das instâncias, bem como, o uso de seus recursos computacionais (CPU e RAM) e de outros serviços (tráfego de saída de rede, armazenamento, banco de dados, etc.), isoladamente por projeto;

k) permitir o monitoramento dos custos dos serviços;

l) permitir a emissão de alertas de gastos para cada projeto. Os alertas deverão ser apresentados na ferramenta e enviados por *e-mail* para os usuários responsáveis, previamente cadastrados;

m) emitir relatório com todos os custos de recursos relacionados a determinado projeto, ainda que esteja em execução em mais de um provedor de nuvem;

n) emitir relatório gerencial por centro de custos, com informações referentes ao orçamento por projeto, valores utilizados e saldo restante;

o) ser customizável para atender às necessidades do Senado Federal.

8.2.3 Serviços técnicos especializados

Os serviços técnicos especializados são prestados diretamente pelo *broker*. Em ambos os contratos são listados os serviços mínimos que devem ser atendidos. Esses serviços são quantificados em UST e tem seu valor definido na lista, devendo ser prestados por profissionais certificados pelos provedores. Para garantir que o *broker* tenha a capacidade de atender ao contrato são exigidos certificados de capacidade técnica.

Para os critérios de seleção do fornecedor será acrescentada a necessidade de apresentação de atestado de capacidade técnica. Quanto à lista de serviços, a mesma deverá ser levantada quando da elaboração de Estudo Técnico Preliminar e/ou Termo de Referência onde também deverá ser previsto o mecanismo de sua atualização.

8.2.4 Treinamento

Ambos os editais contemplam treinamento, contudo o TCU exige que o programa de formação do provedor seja aberto ao mercado, o que já constava nos critérios de avaliação utilizados. O programa de formação aberto ao mercado proporciona a contratação de mais treinamentos se necessário e contratação de profissionais qualificados sem ficar preso aos profissionais do provedor.

8.2.5 Prova de conceito

Tanto o TCU como o MP exigem em seus editais que o *broker* contratado comprove sua capacidade técnica e a aderência da solução ao requisitos do edital por meio da demonstração da solução em uma prova de conceito. Durante a elaboração do Estudo Técnico Preliminar e do Termo de Referência deverão ser elaboradas as requisições de serviço que deverão fazer parte de uma prova de conceito, que irá garantir que a solução proposta atende ao edital.

8.2.6 Critérios propostos para seleção do fornecedor

Levando em conta os pontos destacados nas subseções acima, os critérios propostos para seleção do fornecedor são os que estão no Quadro 18.

Quadro 18 – Critérios propostos para seleção do fornecedor

Nº	**Critério**
SF1	O *broker* deve ser representante de pelos menos dois provedores de nuvem
SF2	O *broker* deve possuir pessoal qualificado para trabalhar com o(s) provedor(es) de nuvem da solução
SF3	O provedor deve trabalhar com multirregiões e poder transferir carga de uma região para outra
SF4	O provedor deve implementar políticas e procedimentos para o uso de criptografia, incluindo gerenciamento de chaves criptográficas
SF5	O provedor deve possibilitar o armazenamento das chaves criptográficas fora do ambiente de nuvem
SF6	O provedor deve garantir e demonstrar isolamento de recursos e de dados de seus clientes
SF7	O provedor deve garantir controles eficazes e compatíveis com as políticas e procedimentos do cliente para gerenciamento de identidades de usuários e controle de acessos
SF8	O modelo de segurança das interfaces do provedor deve ser desenvolvido com base em padrões de mercado, incluindo mecanismos de autenticação forte de usuários e controle de acesso para restringir o acesso aos dados do cliente
SF9	Políticas, procedimentos e mecanismos devem ser estabelecidos e implementados pelo provedor para gerenciamento de vulnerabilidades conhecidas e atualizações de software, garantindo que aplicações, sistemas e vulnerabilidades de dispositivos de rede sejam avaliadas, e que atualizações de segurança fornecidas sejam aplicadas em tempo hábil, priorizando os *patches* mais críticos

Continua na próxima página

Quadro 18 – Continuação

Nº	Critério
SF10	O processo de gestão de vulnerabilidades do provedor deve ser transparente ao cliente
SF11	Os provedores devem utilizar pacotes modulares, usar formatos abertos ou populares para dados e serviços, e serem transparentes em regulações e taxas aplicadas à transferência de dados
SF12	Processos, procedimentos e recursos devem ser estabelecidos e testados, de maneira a viabilizar a transferência de operações de um provedor de computação em nuvem para outro provedor alternativo
SF13	O provedor deverá possuir programa de formação de profissionais aberto para o mercado
SF14	O provedor deve implementar controles para isolamento e segurança de sistema operacional
SF15	O provedor deve utilizar soluções de virtualização que sejam padrões ou referências de mercado
SF16	O provedor deve implementar política de atualização de versão de software e aplicação de correções
SF17	O provedor deve possuir certificação ISO 27001 e 27017
SF18	O provedor deve possuir certificação ISO 27018
SF19	Deverá ser definida uma métrica de USN de tal forma que por meio do valor do serviço no catálogo de serviços público do provedor possa ser definido o valor em USN do serviço
SF20	Deverá ser fornecida uma ferramenta de orquestração que atenda aos requisitos mínimos levantados
SF21	O *broker* deve comprovar sua capacidade técnica através da apresentação de certificados de capacidade técnica de prestação de serviços de computação em nuvem
SF22	O *broker* deverá demonstrar a solução em Prova de conceito definida no edital

Fonte: elaboração própria

8.3 Critérios para a execução contratual e gestão dos serviços

Os critérios propostos para a execução contratual e gestão dos serviços têm seu alicerce nos critérios que estão definidos no Quadro 11 da página 94, contudo por meio da análise das contratações do TCU e do MP, que se encontra na seção 7.4, em especial na subseção 7.4.2 da página 124, percebemos que existem ainda algumas deficiências, como

por exemplo a forma de atualização do catálogo de serviços e o provisionamento de saída, que trataremos nas subseções seguintes.

8.3.1 Modelo de execução

Em relação ao modelo de execução do objeto, ambos os contratos apresentam um fluxo de solicitação de serviços semelhante, pelo qual o *broker* apresenta um plano de arquitetura de solução que é aprovado pelo órgão, e então é testado e homologado, antes de entrar em produção e bilhetagem. Quanto ao fluxo de solicitação desses serviços não há problemas detectados, mas quanto à qualidade do serviço e prazo de execução, o TCU que foi o único órgão que já vivenciou um ciclo completo, chamou a atenção quanto à necessidade de melhorias.

Dois pontos merecem uma atenção especial, a apresentação do relatório de faturamento e os prazos do fluxo de implantação de serviços. No caso da apresentação do relatório de faturamento, onde são detalhadas as USNs e USTs utilizadas, a não entrega, no caso do TCU, gerou um baixo uso do contrato em virtude de uma precaução para que não houvesse a utilização acima do contratado. Podemos perceber então que a informação da utilização do contrato no prazo adequado é fator crítico de sucesso do projeto. Outro problema recorrente foi a demora em corrigir o plano de arquitetura no momento de sua homologação, ocasionando atraso na efetiva utilização dos serviços em produção. Em virtude disso, foram incluídos os seguintes critérios:

a) o contrato deve prever SLA para a entrega do relatório de uso mensal de USNs e USTs e penalidades no caso de descumprimento reiterado;

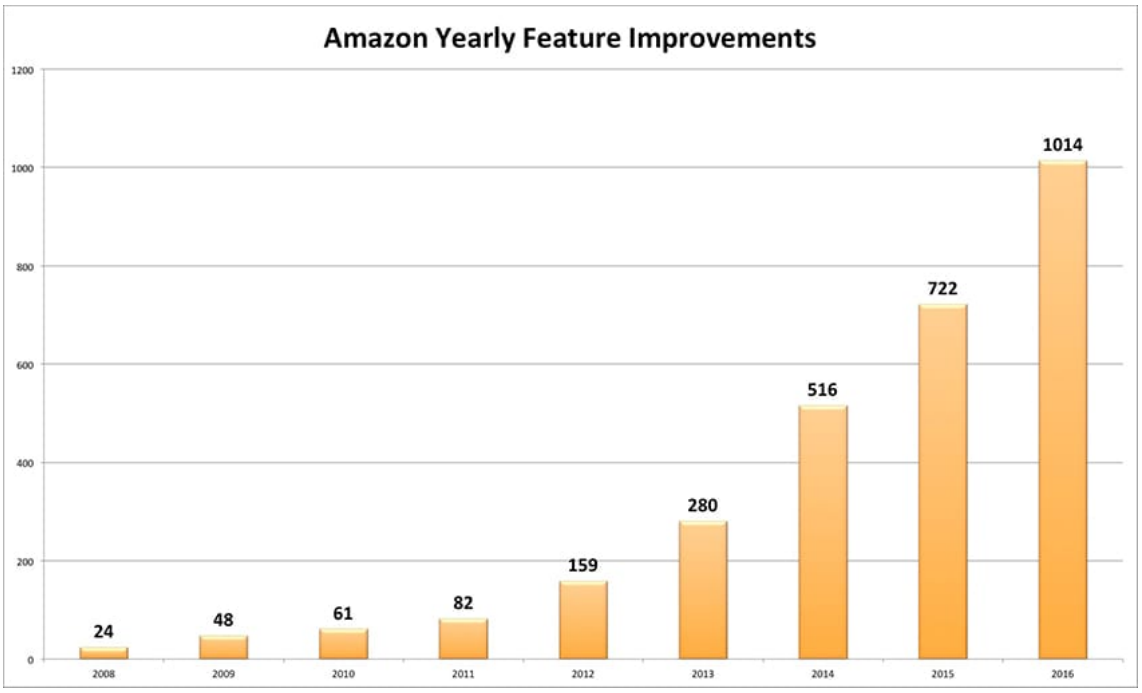
b) o contrato deve prever SLA para cada uma das fases da implantação de um serviço e penalidades no caso de descumprimento reiterado.

8.3.2 Atualização do catálogo de serviços

O crescimento de serviço de computação em nuvem está em ritmo acelerado e crescendo dia-a-dia, como podemos ver no gráfico de melhorias das características da *Amazon Web Services* (AWS) anualmente da Figura 7 abaixo. Cabe destacar que, utilizou-se a AWS como exemplo desta evolução, por ser ela o principal provedor de nuvem mundial da atualidade.

Com esse ritmo acelerado de desenvolvimento e melhorias dos serviços de computação em nuvem, ter um catálogo de serviços rígido, ou com baixa possibilidade de atualização, não permitirá à APF aproveitar todo o potencial de inovação da tecnologia de computação em nuvem. Por esse motivo, percebe-se que a estrutura de atualização de catálogo de serviços presente no edital do MP é muito restritiva, e o ideal é adotar uma solução próxima ao implementado pelo TCU.

Figura 7 – Melhorias das Características da AWS anualmente



Fonte: Golden (2018)

Portanto, surge a necessidade do seguinte critério: o contrato deve definir forma de cálculo do valor em USN de um serviço através do uso do catálogo público do provedor para inclusão de novos serviços no contrato. Cabe ressaltar que, esse critério não altera o objeto da contratação, que é serviços de computação em nuvem, nem expõe o Senado Federal à possibilidade de sobrepreços, já que, o catálogo de serviço dos provedores de nuvem é público e utilizado para prover os serviços a uma ampla gama de consumidores.

8.3.3 Provisionamento de saída

Um dos pontos que se avaliou serem ambos os contratos deficitários é em relação a como provisionar os recursos para a saída dos serviços da nuvem. Apesar de ambos procurarem avaliar o custo da saída ou da migração entre provedores ao final do contrato, não existe um provisionamento para garantir que os recursos financeiros e orçamentários necessários para a migração estejam disponíveis no encerramento do contrato.

É imprescindível que na OS de demanda do serviço seja especificado se será necessário ao final do contrato que o serviço seja migrado, ou bastará sua desativação. Caso seja necessária a migração, entende-se que mensalmente deverá ser informado no relatório de execução deste serviço, o valor em USN e UST necessário para a migração, de tal forma que o fiscal e o gestor do contrato possam reservar para cada um dos serviços o quantitativo necessário para o encerramento do contrato. Propõe-se então o seguinte critério: o relatório mensal de utilização do contrato deverá conter para cada uma das OSs

o quantitativo de USNs e USTs necessário a migração do serviço. No caso de OSs que alterem o serviço implantado em outras anteriores, o relatório deverá contemplar o custo de saída da solução em execução.

8.3.4 Critérios propostos para a execução contratual e gestão do serviço

Quadro 19 – Critérios propostos para a execução contratual e gestão do serviço

Ref.	**Critério**
CG1	OS SLAs com o provedor de nuvem devem ser cuidadosamente definidos e exequíveis, o que inclui penalidades em caso de não cumprimento
CG2	Os dados devem ser submetidos à classificação prévia da informação, antes de serem transmitidos para a nuvem
CG3	Implementar controle de acesso lógico apropriado ao grau de confidencialidade dos dados armazenados na nuvem
CG4	Implementar controles para transferência de dados, como criptografia e uso de VPN adequada
CG5	As chaves criptográficas não devem ser armazenadas na nuvem
CG6	Estabelecer limites do acesso do provedor aos dados do cliente
CG7	Os dados armazenados devem estar criptografados, sendo que o esquema criptográfico deve ser adequado à classificação das informações
CG8	O provedor deve assegurar que dados sujeitos a limites geográficos não sejam migrados para além de fronteiras definidas em contrato
CG9	Estabelecer responsabilidade do provedor em garantir o isolamento de recursos e dados contra acesso indevido por outros clientes
CG10	A política para gestão de mudanças deve ser acordada entre provedor e cliente, e este último deve ser comunicado com antecedência sobre mudanças (por exemplo, utilizando processos do ITIL)
CG11	*Logs* de auditoria do provedor que registram atividades de acesso de usuários privilegiados, tentativas de acesso autorizados e não autorizados, exceções do sistema, e eventos de segurança da informação devem ser mantidos em conformidade com as políticas e regulamentos aplicáveis, e devem estar de acordo com as políticas do cliente
CG12	Definir políticas e procedimentos que devem ser estabelecidos para triagem dos eventos relacionados à segurança e garantir o gerenciamento de incidentes completo e ágil
CG13	Quaisquer eventos de segurança de informação devem ser comunicados através de canais predefinidos de comunicação, de maneira rápida e eficiente, e de acordo com os requisitos legais, regulatórios e contratuais

Continua na próxima página

Quadro 19 – Continuação

Ref.	Critério
CG14	O cliente deve prever cópia dos *logs* fornecidos pelo provedor, de acordo com sua própria política de retenção; deve haver, da parte do provedor, um mecanismo para filtragem e cópia dos *logs* gerados pelo fornecedor para a área do cliente
CG15	Estabelecer direitos claros e exclusivos de propriedade e acesso aos dados, inclusive referentes a *logs*
CG16	Definir as obrigações do provedor quanto a requisitos mínimos de autorização e transparência de acesso do provedor aos ativos físicos e virtuais do cliente, bem como a respeito da necessidade de divulgação ao cliente de suas políticas e orientações específicas
CG17	Definir as obrigações do provedor quanto a requisitos mínimos de contratação de pessoal e de monitoramento de suas atividades, bem como a respeito da necessidade de divulgação ao cliente de suas políticas e orientações específicas
CG18	Definir a necessidade de realização de avaliações periódicas independentes, com a finalidade de verificar a adequação dos controles do provedor a um conjunto de critérios pré-definidos
CG19	Especificar mecanismos de segurança e proteção de propriedade intelectual, e quaisquer requisitos legais ou regulatórios
CG20	Especificar nível esperado dos serviços (SLA) e mecanismos clássicos de gestão contratual de serviços terceirizados (comunicações formais, multas, rescisão etc)
CG21	Estabelecer processos ágeis de migração para provedores alternativos, em caso de falhas do provedor principal
CG22	Deve assegurar a conformidade dos dados e aplicações hospedadas na nuvem com os requisitos de padrões, legais e regulatórios, aos quais o negócio está sujeito, de maneira contínua e atualizada
CG23	Avaliar quais informações serão hospedadas na nuvem, considerando o processo de classificação da informação, o valor do ativo de informação, os controles de acesso físicos e lógicos, o modelo de serviço e de implementação de computação em nuvem e a localização geográfica onde as informações serão armazenadas
CG24	Deve prever soluções de contingência independentes de provedor específico (portabilidade do serviço para outro provedor)
CG25	Assegurar os níveis de serviço no caso de interrupções de serviço planejadas ou não planejadas
CG26	Prever modelo de remuneração vinculada aos níveis de serviço estabelecidos, prevendo glosas no caso de descumprimento de parâmetros mínimos

Continua na próxima página

Quadro 19 – Continuação

Ref.	Critério
CG27	Definir sanções no caso de descumprimento reiterado de parâmetros mínimos de níveis de serviço estabelecidos
CG28	Assegurar que todas as vulnerabilidades sejam priorizadas e corrigidas dentro de SLAs acordados contratualmente entre cliente e provedor
CG29	Definir divisão clara de papéis de cliente e provedor
CG30	Estabelecer indicadores claros e precisos tanto de ambiente como de segurança, com responsáveis pelo seu monitoramento e disponibilização
CG31	O contrato deverá prever verificações intermediárias do nível de uso da capacidade contratada, alertas quando atingidos patamares de recursos e tetos de recursos máximos utilizáveis em função do orçamento disponível
CG32	Prever condições e limites claros de custos para saída do provedor
CG33	Especificar que os direitos de propriedade sobre os dados armazenados na nuvem pela organização são exclusivos da organização
CG34	Definir em quais países os dados do cliente podem ser armazenados
CG35	Definir que o provedor deve atender à política de exclusão de dados do cliente
CG36	Utilizar criptografia para proteger os dados de acesso indevido
CG37	O contrato deve detalhar definições específicas de incidentes, eventos, ações a serem tomadas e responsabilidades do provedor e do cliente
CG38	O contrato deve definir requisitos de interoperabilidade entre as ferramentas de gestão de incidentes do provedor e do cliente
CG39	O contrato deve prever SLA para a entrega do relatório de uso mensal de USNs e USTs e penalidades no caso de descumprimento reiterado
CG40	O contrato deve prever SLA para cada uma das fases da implantação de um serviço e penalidades no caso de descumprimento reiterado
CG41	O contrato deve definir forma de cálculo do valor em USN de um serviço através do uso do catálogo público do provedor para inclusão de novos serviços no contrato
CG42	O relatório mensal de utilização do contrato deverá conter para cada uma das OSs o quantitativo de USNs e USTs necessário a migração do serviço

Fonte: elaboração própria

8.4 Conclusão do capítulo

Neste capítulo foram apresentados os critérios propostos para um modelo de contratação de serviços em nuvem para o Senado Federal. Na seção 8.1 foram apresentados 25 (vinte e cinco) critérios a serem adotados na fase de planejamento da contratação.

Na seção 8.2 apresentou-se 22 (vinte e dois) critérios a serem utilizados na seleção do fornecedor, e na seção 8.3 42 (quarenta e dois) critérios para a fase de execução contratual e gestão do serviço.

9 Conclusão

9.1 Conclusões

Este trabalho de pesquisa teve como objetivo propor critérios para a contratação de serviços em nuvem para o Senado Federal servindo de norteador do processo de adoção dos serviços de computação em nuvem no âmbito desta casa legislativa.

Uma das justificativas para a realização desta pesquisa foi a oportunidade de redução de custo por meio da adoção da tecnologia de computação em nuvem, com a migração de recursos de investimento para custeio (CAPEX para OPEX), o que proporciona uma melhor utilização dos recursos, já que não há o desperdício com contratação de um parque computacional que fica ocioso na maior parte do tempo, devido à contratação dos recursos para atender a demanda crescente antes da sua efetiva necessidade. Outra justificativa foi a Emenda constitucional nº. 95 do teto dos gastos (BRASIL, 2016b), que congelou os gastos públicos, fazendo com que fosse cada vez mais necessária a boa utilização dos recursos. A EC nº 95 irá reduzir a contratação no serviço público, fazendo com que cada vez mais o servidor público tenha que se voltar para a atividade fim, e na área de Tecnologia da Informação, o ideal é se dedicar ao desenvolvimento de soluções específicas para o Senado Federal e menos para a contratação, manutenção e gerenciamento de infraestrutura, o que ao longo do tempo irá se tornar uma *commoditie* como energia elétrica, água e telefonia. Porém, ainda não existe um modelo de contratação maduro na APF e este trabalho buscou dar mais um passo na construção deste objetivo.

Dessa forma, foi realizado um levantamento dos conceitos de computação em nuvem, suas características essenciais, seus modelos de serviço e implantação e a arquitetura de referência da computação em nuvem, além de identificar a legislação e as normas vigentes para a contratação de serviços em nuvem na Administração Pública Federal e as especificidades das contratações no Senado Federal.

Tendo sido levantado todo esse referencial teórico, sentiu-se a necessidade de antes de avaliar as contratações do TCU e do MP, buscar os critérios a serem utilizados, e para isso foram analisados trabalhos acadêmicos anteriores que pudessem balizar a formulação dessa avaliação. De posse desses critérios e da legislação e normas vigentes identificadas, foram analisadas as contratações do TCU e do MP.

Após a análise, todos os objetivos específicos da pesquisa haviam sido atendidos, e por meio dela foi possível "propor os critérios para a contratação de serviços em nuvem para o Senado Federal" alcançando o objetivo geral. A aplicação do modelo em uma contratação do Senado Federal ainda não é uma realidade, mas os critérios propostos com

certeza são um ponto de partida importante.

9.2 Limitações

Apesar das contratações do TCU e do MP já contemplarem as características de um uso mais intenso e amplo dos serviços de computação em nuvem, o uso dos contratos ainda é incipiente e não podem ser tratados como uma solução definitiva para a utilização dos serviços de computação em nuvem no setor público.

Não havia dados disponíveis com relação ao faturamento dos contratos, pois apesar de o contrato do TCU já estar com mais de 1 (um) ano de execução, devido às dificuldades encontradas com o software de orquestração, nenhuma fatura dos serviços de nuvem havia sido paga. Já com relação aos contratos da ata de registro do MP a situação é ainda mais incipiente, já que a única OS de serviços de nuvem que havia sido aprovada ainda não se encontrava em execução até o final do mês de junho de 2019.

Quanto à validade dos critérios, os mesmos devem ser avaliados durante contratações do Senado Federal, o que ainda não ocorreu.

Também, em virtude do tempo reduzido para a elaboração deste trabalho, não foram levantadas as necessidades do Senado Federal e possíveis serviços que seriam necessários na contratação. Sem o levantamento dessas necessidades, não existe a possibilidade de elaborar um estudo técnico preliminar ou um termo de referência.

9.3 Trabalhos Futuros

Este trabalho pode servir como embrião de uma contratação de serviços em nuvem pelo Senado Federal, assim como ser utilizado por outros órgãos públicos para avaliação da validade dos critérios em outros entes da APF.

Nos próximos anos a cultura de contratação em nuvem na APF estará mais desenvolvida e será possível validar se os critérios que foram propostos são realmente necessários, se foram citados critérios que não precisam ser utilizados, e se existem critérios a serem considerados que não foram elencados no presente estudo.

Os critérios propostos podem ainda ser avaliados quando à sua real necessidade, quando da contratação de serviços em nuvem no âmbito do Senado Federal. Para tanto, seria interessante realizar um estudo de caso fazendo essa avaliação no decorrer de uma contratação do próprio Senado Federal.

Referências

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27001:2013*: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro, 2013. 30 p. Citado 3 vezes nas páginas 68, 70 e 174.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27002:2013*: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro, 2013. 99 p. Citado 3 vezes nas páginas 70, 73 e 175.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27017:2016*: Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem. Rio de Janeiro, 2016. 49 p. Citado 2 vezes nas páginas 70 e 175.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27018:2018*: Tecnologia da informação - Técnicas de segurança - Código de prática para proteção de informações de identificação pessoal (PII) em nuvens públicas que atuam como processadores de PII. Rio de Janeiro, 2018. 28 p. Citado 2 vezes nas páginas 71 e 175.

BRASIL. Lei nº 8.666, de 21 de junho de 1993. Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências. *Diário Oficial da União*, Brasília, DF, jun. 1993. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8666compilado.htm>. Acesso em: 07/05/2019. Citado 3 vezes nas páginas 29, 47 e 171.

BRASIL. Lei nº 10.520, de 17 de julho de 2002. Institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências. *Diário Oficial da União*, Brasília, DF, jul. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10520.htm>. Acesso em: 16/05/2019. Citado 2 vezes nas páginas 47 e 171.

BRASIL. Decreto nº 5.450, de 31 de maio de 2005. Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências. *Diário Oficial da União*, Brasília, DF, jun. 2005. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/decreto/d5450.htm>. Acesso em: 16/05/2019. Citado 2 vezes nas páginas 49 e 172.

BRASIL. Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008. Disciplina a gestão de segurança da informação e comunicações na administração pública federal, direta e indireta, e dá outras providências. *Diário Oficial da União*, Brasília, DF, jun. 2008. Disponível em: <http://dsic.planalto.gov.br/legislacao/in_01_gsidsic.pdf>. Acesso em: 18/05/2019. Citado na página 173.

BRASIL. Norma Complementar nº 06/IN01/DSIC/GSIPR. Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. *Diário Oficial da União*, nov. 2009. Disponível em: <http://dsic.planalto.gov.br/legislacao/nc_6_gcn.pdf>. Acesso em: 19/05/2019. Citado 2 vezes nas páginas 57 e 173.

BRASIL. Decreto nº 7.174, de 12 de maio de 2010. Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União. *Diário Oficial da União*, Brasília, DF, maio 2010. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Decreto/D7174.htm>. Acesso em: 21/05/2019. Citado 2 vezes nas páginas 49 e 172.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. *Diário Oficial da União*, Brasília, DF, nov. 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 06/05/2019. Citado 3 vezes nas páginas 48, 73 e 171.

BRASIL. Decreto nº 7.724, de 16 de maio de 2012. Regulamenta a Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição. *Diário Oficial da União*, Brasília, DF, maio 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm>. Acesso em: 16/05/2019. Citado 3 vezes nas páginas 49, 50 e 172.

BRASIL. Decreto nº 7.845, de 14 de novembro de 2012. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. *Diário Oficial da União*, Brasília, DF, nov. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Decreto/D7845.htm>. Acesso em: 16/05/2019. Citado 4 vezes nas páginas 50, 51, 73 e 172.

BRASIL. Decreto nº 7.892, de 23 de janeiro de 2013. Regulamenta o Sistema de Registro de Preços previsto no art.15 da Lei nº 8.666, de 21 de junho de 1993. *Diário Oficial da União*, Brasília, DF, jun. 2013. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7892.htm>. Acesso em: 21/05/2019. Citado 2 vezes nas páginas 49 e 172.

BRASIL. Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013. Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal. *Diário Oficial da União*, Brasília, DF, fev. 2013. Disponível em: <http://dsic.planalto.gov.br/legislacao/instrucao_normativa_nr2.pdf>. Acesso em: 18/05/2019. Citado 4 vezes nas páginas 53, 54, 73 e 173.

BRASIL. Instrução Normativa GSI/PR nº 3, de 6 de março de 2013. Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em

algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal. *Diário Oficial da União*, Brasília, DF, mar. 2013. Disponível em: <http://dsic.planalto.gov.br/legislacao/instrucao_normativa_nr3.pdf>. Acesso em: 18/05/2019. Citado 4 vezes nas páginas 54, 55, 73 e 173.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*, Brasília, DF, abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 16/05/2019. Citado 3 vezes nas páginas 48, 49 e 171.

BRASIL. Norma Complementar nº 07/IN01/DSIC/GSIPR. Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. *Diário Oficial da União*, Brasília, DF, jul. 2014. Disponível em: <http://dsic.planalto.gov.br/legislacao/nc_07_revisao_01.pdf>. Acesso em: 19/05/2019. Citado 3 vezes nas páginas 58, 73 e 173.

BRASIL. Norma Complementar nº 19/IN01/DSIC/GSIPR. Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta. *Diário Oficial da União*, Brasília, DF, jul. 2014. Disponível em: <http://dsic.planalto.gov.br/legislacao/nc_19_SISTEMAS_ESTRUTURANTES.pdf>. Acesso em: 19/05/2019 19/05/2019 19/05/2019. Citado 2 vezes nas páginas 60 e 173.

BRASIL. Norma Complementar nº 21/IN01/DSIC/GSIPR. Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta. *Diário Oficial da União*, Brasília, DF, out. 2014. Disponível em: <http://dsic.planalto.gov.br/legislacao/nc_21_preservacao_de_evidencias.pdf>. Acesso em: 19/05/2019. Citado 3 vezes nas páginas 61, 73 e 174.

BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. *Diário Oficial da União*, Brasília, DF, maio 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 16/05/2019. Citado 2 vezes nas páginas 51 e 172.

BRASIL. Emenda Constitucional nº 95, de 15 de dezembro de 2016. *Diário Oficial da União*, Brasília, DF, dez. 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc95.htm>. Acesso em: 13/05/2019. Citado 2 vezes nas páginas 31 e 151.

BRASIL. *Constituição (1988). Constituição da República Federativa do Brasil. Texto constitucional promulgado em 5 de outubro de 1988, com as alterações determinadas pelas Emendas Constitucionais de Revisão nºs 1 a 6/94, pelas Emendas Constitucionais nºs 1/92 a 99/2017 e pelo Decreto Legislativo nº 186/2008.* Brasília, DF: Senado Federal, Coordenação de Edições Técnicas, 2018. 522p. ISBN 978-85-7018-909-7. Citado na página 79.

BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. *Diário Oficial da União*, Brasília, DF, dez. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm>. Acesso em: 16/05/2019. Citado 3 vezes nas páginas 51, 52 e 172.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*, Brasília, DF, ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm>. Acesso em: 19/05/2019. Citado 3 vezes nas páginas 49, 72 e 171.

BRASIL. Norma Complementar nº 14/IN01/DSIC/GSIPR. Estabelece princípios, diretrizes e responsabilidades relacionados à segurança da informação para o tratamento da informação em ambiente de computação em nuvem, nos órgãos e entidades da Administração Pública Federal, direta e indireta. *Diário Oficial da União*, Brasília, DF, mar. 2018. Disponível em: <http://dsic.planalto.gov.br/arquivos/documentos-pdf/NC_14_R01.pdf>. Acesso em: 19/05/2019. Citado 5 vezes nas páginas 59, 60, 73, 135 e 173.

BRASIL. Instrução Normativa nº 1, de 4 de abril de 2019. Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal. *Diário Oficial da União*, Brasília, DF, abr. 2019. Disponível em: <https://www.governodigital.gov.br/documentos-e-arquivos/INSTRUCAO%20NORMATIVA%20No%201-%20DE%204%20DE%20ABRIL%20DE%202019.pdf/at_download/file>. Acesso em: 18/05/2019. Citado 4 vezes nas páginas 56, 57, 81 e 173.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Portaria MP/STI nº 20 , de 14 de junho de 2016. Dispõe sobre orientações para contratação de soluções de Tecnologia da Informação no âmbito da Administração Pública Federal direta, autárquica e fundacional e dá outras providências. *Diário Oficial da União*, Brasília, DF, jun. 2016. Disponível em: <https://www.governodigital.gov.br/documentos-e-arquivos/legislacao/Portaria%20MP-STI%20no%2020%20de%2014%20de%20junho%20de%202016.pdf>. Acesso em: 21/05/2019. Citado na página 174.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Boas Práticas, Orientações e Vedações para Contratação de Serviços de Computação em Nuvem. *Ministério do Planejamento, Orçamento e Gestão*, Brasília, DF, jun. 2016. Disponível em: <https://www.governoeletronico.gov.br/documentos-e-arquivos/Orientacao%20servicos%20em%20nuvem.pdf>. Acesso em: 05/05/2019. Citado 3 vezes nas páginas 31, 68 e 174.

BRASIL. Tribunal de Contas da União. Acórdão nº 2.569/2018. Plenário. Relator: Ministro Aroldo Cedraz. Sessão de 07/11/2018. *Diário Oficial da União*, Brasília/DF, nov. 2018. Disponível em: <https://contas.tcu.gov.br/sagas/SvlVisualizarRelVotoAcRtf?codFiltro=SAGAS-SESSAO-ENCERRADA&seOcultaPagina=S&item0=648516>. Acesso em: 08/06/2019. Citado 5 vezes nas páginas 29, 30, 66, 67 e 174.

BRASIL. Tribunal de Contas da União. Acórdão nº 1.739/2015. Plenário. Relator: Ministro Benjamin Zymler. Sessão de 15/07/2015. *Diário Oficial da União*, Brasília, DF, jul. 2015. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20150720/AC_1739_24_15_P.doc>. Acesso em: 05/05/2019. Citado 10 vezes nas páginas 31, 39, 47, 59, 61, 63, 64, 65, 91 e 174.

CARISSIMI, A. Desmistificando a computação em nuvem. 2015. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/erad-rs/2015/002.pdf>. Acesso em: 10/05/2019. Citado na página 39.

COSTA, B. et al. *Desmistificando a Adoção de Serviços em Nuvem Governamental*. 1. ed. Brasília/DF: IBGP - Instituto Brasileiro de Governança Pública, 2019. ISBN 978-65-80621-00-2. Citado 2 vezes nas páginas 107 e 134.

COSTA, B. G. S. da. *Uma proposta de migração de sistemas legados do governo para a nuvem*. Dissertação (Mestrado) — Universidade de Brasília, Brasília/DF, 2018. Disponível em: <http://repositorio.unb.br/handle/10482/34321>. Acesso em: 11/06/2019. Citado na página 179.

COSTA, L. D. S.; MEDEIROS, M. F. M. de. Políticas públicas brasileiras de computação em nuvem: análise documental dos relatórios do Global Cloud Computing Scorecard. *Revista Brasileira de Políticas Públicas*, Centro de Ensino Unificado de Brasilia, Brasília/DF, v. 7, n. 3, 2017. ISSN 2236-1677. Disponível em: <https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4945>. Acesso em: 11/06/2019. Citado na página 179.

DINIZ, I. V. de L.; COSTA, L. dos S.; MEDEIROS, M. F. M. Utilização da computação em nuvem no poder legislativo: percepções dos gestores e entraves ao uso. *Revista Brasileira de Políticas Públicas*, v. 7, n. 1, 2017. ISSN 2236-1677. Disponível em: <https://www.publicacoes.uniceub.br/RBPP/article/view/4586>. Acesso em: 06/05/2019. Citado na página 178.

EVANGELISTA, W. G. *Critérios para avaliação de viabilidade da adoção de computação em nuvem por parte de organizações da Administração Pública Federal*. Dissertação (Mestrado) — Universidade Católica de Brasília, 2014. Disponível em: <https://bdtd.ucb.br:8443/jspui/bitstream/123456789/1424/1/Wellington%20Galdino%20Evangelista.pdf>. Acesso em: 06/05/2019. Citado na página 177.

EVANGELISTA, W. G.; SOUZA NETO, J. Modelo de avaliação da capacidade das organizações da administração pública federal para a adoção de software as a service (saas) público. *Revista Servidor Público*, v. 67, n. 2, p. 173–202, abr. 2016. ISSN 2357-8017. Disponível em: <http://repositorio.enap.gov.br/handle/1/2926>. Acesso em: 06/05/2019. Citado 7 vezes nas páginas 75, 76, 77, 78, 133, 134 e 178.

FEDOSEENKO, V. *What is XaaS? IaaS vs SaaS vs PaaS: what's the difference. Examples*. Cyprus, 2018. Disponível em: <https://www.ispsystem.com/news/xaas>. Acesso em: 11/05/2019. Citado na página 40.

FERREIRA, M. A.; ANDRADE, C. A. B. Cloud computing - normas, leis e orientações do governo brasileiro. *Intr@ciência Revista Científica*, n. 12, dez. 2016. Disponível em: <http://uniesp.edu.br/sites/_biblioteca/revistas/20170531133522.pdf>. Acesso em: 08/05/2019. Citado 2 vezes nas páginas 47 e 178.

FREITAS, P. H. C. *Critérios de migração do processamento e armazenamento de dados da administração pública para a nuvem*. Dissertação (Mestrado) — Universidade Católica de Brasília, Brasília/DF, dez. 2018. Disponível em: <https://bdtd.ucb.br:8443/jspui/bitstream/tede/2549/2/PedroHenriqueChagasFreitasDissertacao2018.pdf>. Acesso em: 11/06/2019. Citado na página 179.

GIL, A. C. *Como Elaborar Projetos de Pesquisa*. 6. ed. São Paulo: Atlas, 2017. ISBN 9788597012613. Citado na página 35.

GOLDEN Bernard. Cloud Database Wars: Google Spanner vs. Microsoft CosmosDB. 2018. Disponível em: <https://www.simplilearn.com/google-spanner-vs-microsoft-cosmosdb-cloud-database-article/articles>. Acesso em: 06/07/2019. Citado na página 146.

LIU, F. et al. *NIST Cloud Computing Reference Architecture*. National Institute of Standards and Technology. Gaithersburg, MD, EUA, 2011. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf>. Acesso em: 05/05/2019. Citado 4 vezes nas páginas 41, 42, 43 e 44.

LOPES, T. F. *Requisitos para a Contratação de Serviços em Computação em Nuvem pela Administração Pública Federal*. Dissertação (Mestrado) — Universidade Católica de Brasília, 2015. Disponível em: <https://bdtd.ucb.br:8443/jspui/bitstream/tede/2065/2/ThiagoFerreiraLopesDissertacao2015.pdf>. Acesso em: 06/05/2019. Citado 5 vezes nas páginas 47, 73, 75, 91 e 177.

MEDEIROS, M. F. M. de; SOUSA NETO, M. V. Uso da computação em nuvem no setor público: um estudo de caso com gestores de ti do estado do rio grande do norte e do governo federal. *Revista Gestão & Tecnologia*, v. 16, n. 1, p. 135–156, abr. 2016. ISSN 2177-6652. Disponível em: <revistagt.fpl.edu.br/get/article/view/790>. Acesso em: 06/05/2019. Citado na página 177.

MELL, P.; GRANCE, T. *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology. Gaithersburg, MD, EUA, 2011. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. Acesso em: 05/05/2019. Citado 5 vezes nas páginas 29, 37, 38, 39 e 41.

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO. *Edital do Pregão Eletrônico nº 29/2018*. Ministério do Planejamento, Desenvolvimento e Gestão. Brasília, DF, 2018. Disponível em: <http://www.planejamento.gov.br/acesso-a-informacao/licitacoes-e-contratos/licitacoes/pregao/2018/18_lici_pregao29_reaberto_edital-pe-29-18-publicado.pdf>. Acesso em: 24/06/2019. Citado na página 108.

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO. *Termo de Referência do Pregão Eletrônico nº 29/2018*. Ministério do Planejamento, Desenvolvimento e Gestão. Brasília, DF, 2018. Disponível em: <http://www.planejamento.gov.br/acesso-a-informacao/licitacoes-e-contratos/licitacoes/pregao/2018/18_lici_pregao29_reaberto_anexo-i-termo-referencia.pdf>. Acesso em: 24/06/2019. Citado 5 vezes nas páginas 109, 110, 111, 112 e 140.

NOGUEIRA, G. S. *Um comparativo entre os modelos de Brasil, Estados Unidos da América e Reino Unido para a contratação de serviços em nuvem*. Dissertação (Mestrado) — Instituto Legislativo Brasileiro, Brasília/DF, 2016. Disponível em:

<https://www2.senado.leg.br/bdsf/bitstream/handle/id/535905/TCC_Gilberto%20Nogueira.pdf?sequence=1>. Acesso em: 06/05/2019. Citado na página 178.

SANTOS, E. F. dos. Melhores práticas para a adoção de backup em nuvem por órgãos do Poder Legislativo Federal. *Universidade do Sul de Santa Catarina*, 2019. Disponível em: <https://www.riuni.unisul.br/bitstream/handle/12345/7045/MelhoresPraticasBackupEmNuvem.pdf?sequence=1&isAllowed=y>. Acesso em: 08/05/2019. Citado 2 vezes nas páginas 47 e 179.

SENADO FEDERAL. Ato da Comissão Diretora nº 16, de 2008. Institui, no âmbito do Senado Federal e de suas Secretarias Especiais e Órgãos Supervisionados, as minutas-padrão constantes do Anexo deste Ato e dá outras providências. *Boletim Administrativo do Pessoal (BASF)*, Brasília, DF, set. 2008. Disponível em: <https://adm.senado.gov.br/normas/ui/pub/normaConsultada?idNorma=223036>. Acesso em: 21/05/2019. Citado 2 vezes nas páginas 81 e 181.

SENADO FEDERAL. Ato da Comissão Diretora nº 2, de 2008. Dispõe sobre a gestão de Contratos no Senado Federal e dá outras providências. *Boletim Administrativo do Pessoal (BASF)*, Brasília, DF, fev. 2008. Disponível em: <https://adm.senado.gov.br/normas/ui/pub/normaConsultada?idNorma=255733>. Acesso em: 21/05/2019. Citado 2 vezes nas páginas 81 e 181.

SENADO FEDERAL. Ato do Primeiro-Secretário nº 31/2009. Estabelece a possibilidade de realização das compras e contratações eletrônicas do Senado Federal por meio do Portal de Compras do Governo Federal – COMPRASNET. *Boletim Administrativo do Pessoal (BASF)*, Brasília, DF, jun. 2009. Disponível em: <https://adm.senado.gov.br/normas/ui/pub/normaConsultada?idNorma=261577>. Acesso em: 21/05/2019. Citado 2 vezes nas páginas 87 e 181.

SENADO FEDERAL. Ato da Comissão Diretora nº 9, de 2012. Regulamenta, no âmbito do Senado Federal, a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso aos dados, informações e documentos de interesse da sociedade e do Estado. *Boletim Administrativo do Pessoal (BASF)*, Brasília, DF, maio 2012. Disponível em: <https://adm.senado.gov.br/normas/ui/pub/normaConsultada?idNorma=203925>. Acesso em: 13/06/2019. Citado na página 82.

SENADO FEDERAL. Ato da Comissão Diretora nº 16, de 2013. Institui a Política de Gestão de Riscos Organizacionais do Senado Federal. *Boletim Administrativo do Pessoal (BASF)*, Brasília, DF, jun. 2013. Disponível em: <https://adm.senado.gov.br/normas/ui/pub/normaConsultada?idNorma=203076>. Acesso em: 13/06/2019. Citado 2 vezes nas páginas 83 e 181.

SENADO FEDERAL. Ato da Comissão Diretora nº 8/2015. Regulamenta a atuação dos servidores que atuam como fiscais de contratos no âmbito do Senado Federal. *Boletim Administrativo do Pessoal (BASF)*, Brasília, DF, jun. 2015. Disponível em: <https://adm.senado.gov.br/normas/ui/pub/normaConsultada?idNorma=13696053>. Acesso em: 21/05/2019. Citado 2 vezes nas páginas 84 e 181.

SENADO FEDERAL. Ato da Diretoria-Geral nº 20, de 2015 Dispõe sobre a fiscalização e a gestão dos contratos de prestação de serviços terceirizados de natureza continuada no âmbito do Senado Federal. *Boletim Administrativo do Pessoal (BASF)*, Brasília, DF, jun.

2015. Disponível em: <https://adm.senado.gov.br/normas/ui/pub/normaConsultada?idNorma=13686050>. Acesso em: 21/05/2019. Citado 2 vezes nas páginas 89 e 181.

SENADO FEDERAL. Ato da Diretoria-Geral nº 27, de 2015. Dispõe sobre procedimentos a serem adotados na gestão de contratos. *Boletim Administrativo do Pessoal (BASF)*, Brasília, DF, ago. 2015. Disponível em: <https://adm.senado.gov.br/normas/ui/pub/normaConsultada?idNorma=13726050>. Acesso em: 21/05/2019. Citado 2 vezes nas páginas 90 e 181.

SENADO FEDERAL. Ato da Diretoria-Geral nº 9, de 2015. Estabelece, no âmbito do Senado Federal, normas procedimentais para contratações. *Boletim Administrativo do Pessoal (BASF)*, Brasília, DF, mar. 2015. Disponível em: <https://adm.senado.gov.br/normas/ui/pub/normaConsultada?idNorma=13639050>. Acesso em: 21/05/2019. Citado 3 vezes nas páginas 87, 89 e 181.

SENADO FEDERAL. Ato da Comissão Diretora nº 9/2017. Institui a Política Corporativa de Segurança da Informação do Senado Federal - PCSI. *Boletim Administrativo do Pessoal (BASF)*, Brasília, DF, jun. 2017. Disponível em: <https://adm.senado.leg.br/normas/ui/pub/normaConsultada?idNorma=13901154>. Acesso em: 29/05/2019. Citado 3 vezes nas páginas 84, 86 e 181.

SENADO FEDERAL. Plano Diretor de Tecnologia da Informação 2017-2019. Senado Federal, Brasília/DF, 2017. Disponível em: <https://www12.senado.leg.br/transparencia/gestgov/pdf-planejamento-estrategico/PDTI.PDF>. Acesso em: 04/07/2019. Citado na página 134.

SENADO FEDERAL. Resolução nº 13, de 2018. Consolida as alterações promovidas na estrutura administrativa do Senado Federal. *Diário Oficial da União*, Brasília, DF, n. 121, jun. 2018. Disponível em: <https://adm.senado.gov.br/normas/ui/pub/normaConsultada?idNorma=14041416>. Acesso em: 21/05/2019. Citado 2 vezes nas páginas 79 e 181.

SMITH, E.; SHIRER, M. *Worldwide public cloud services spending forecast to reach $210 billion this year, according to IDC*. 2019. Disponível em: <https://www.idc.com/getdoc.jsp?containerId=prUS44891519>. Acesso em: 08/05/2019. Citado na página 31.

TRIBUNAL DE CONTAS DA UNIÃO. *Relatório de Fiscalização - Fiscalização: 650/2014 - TC 025.994/2014-0 - Relator: Benjamin Zymler*. Tribunal de Contas da União. Brasília, DF, 2015. Disponível em: <https://contas.tcu.gov.br/etcu/ObterDocumentoSisdoc?seAbrirDocNoBrowser=true&codArqCatalogado=8970143&codPapelTramitavel=52998950>. Acesso em: 26/05/2019. Citado 6 vezes nas páginas 62, 91, 94, 97, 133 e 135.

TRIBUNAL DE CONTAS DA UNIÃO. *Edital do Pregão Eletrônico nº 22/2017*. Tribunal de Contas da União. Brasília, DF, 2017. Disponível em: <https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A15CC7BCB8015CEA6BFBA152F8>. Acesso em: 29/05/2019. Citado 4 vezes nas páginas 98, 99, 100 e 107.

VAQUERO, L. M. et al. A break in the clouds: towards a cloud definition. *ACM SIGCOMM Computer Communication Review*, Association for Computing Machinery (ACM), New York, NY, v. 39, n. 1, p. 50–55, dec 2008. Disponível em: <https://dl.acm.org/ft_gateway.cfm?id=1496100&ftid=606313&dwn=1&CFID=130420820&CFTOKEN=bf1e5e1d6da4e8cc-B44165A9-98C6-AB39-CDA17E69E35E2270>. Acesso em: 17/05/2019. Citado na página 37.

VIROTE, A. P. P. *Em direção a uma proposta de utilização da computação em nuvem na Administração Pública Federal: um estudo de caso no Instituto Federal Goiano*. Dissertação (Mestrado) — Universidade Federal de Pernambuco, Recife, 2016. Disponível em: <https://repositorio.ufpe.br/bitstream/123456789/18622/1/MPROF-ALFREDO-PUPAK.pdf>. Acesso em: 08/05/2019. Citado na página 178.

YIN, R. K. *Estudo de Caso: Planejamento e Métodos*. 2. ed. Porto Alegre: Bookman, 2001. ISBN 85-7307-852-9. Citado na página 35.

Glossário

Autenticidade

Propriedade que garante que a informação provém da fonte anunciada e que não foi alterada no decorrer de um processo.

AWS

abreviatura de *Amazon Web Services*, divisão da Amazon que atua como provedor de serviços em nuvem.

CAPEX

CAPEX é a sigla da expressão inglesa *capital expenditure* e que designa o montante de dinheiro despendido na aquisição de bens de capital de uma determinada empresa.

Classificação de *data centers* em *Tiers* de acordo com a norma TIA 942

A classificação *Tier* adotada em *data centers* foi desenvolvida pelo *Uptime Institute*, nos EUA, é usada desde 1995 e tem reconhecimento mundial. Os níveis de disponibilidade associados às classificações Tier foram determinados por meio de resultados de análises de disponibilidade de *data centers* reais. Existem quatro tipos de *data centers*: Tier I, Tier II, Tier III e Tier IV.

***Tier* I** é o básico que possui componentes internos não redundantes e uma rota de alimentação externa (energia e conexão de dados) não redundante servindo ao ambiente crítico. A infraestrutura *Tier* I inclui um espaço dedicado para os sistemas de TI; um sistema *UPS* (*no-break*) para lidar com falhas momentâneas no fornecimento de energia; um equipamento dedicado de refrigeração e um sistema gerador para proteger as funções de TI de falhas prolongadas no fornecimento de energia. A disponibilidade para o *Tier* I é de 99,671%.

***Tier* II** possui componentes internos redundantes e uma rota de distribuição de alimentação externa (energia e conexão de dados) não redundante servindo ao ambiente crítico. Os componentes redundantes são: geradores, sistemas UPS (nobreak), sistemas de refrigeração e tanques de combustível. Esses componentes podem ter seu funcionamento interrompido, seguindo um plano de manutenção, por exemplo, sem a necessidade de desligar qualquer um dos equipamentos críticos de TI. A disponibilidade para o *Tier* II é de 99,741%.

***Tier* III** é um *data center* paralelamente sustentável que possui componentes de capacidade redundantes e múltiplas rotas independentes de distribuição (energia e conexão de dados) que servem o ambiente crítico. Apenas uma rota de distribuição é

necessária para servir o ambiente crítico em qualquer momento. Qualquer componente nas rotas de distribuição pode ser interrompido sem impactar qualquer equipamento do ambiente crítico. A disponibilidade para o *Tier* III é de 99,982%.

***Tier* IV** é um *data center* tolerante a falhas composto por vários sistemas fisicamente independentes e isolados, componentes redundantes e múltiplas rotas independentes de alimentação (energia e conexão de dados) ativas simultaneamente, servindo ao ambiente crítico. Sistemas complementares e rotas de distribuição devem estar fisicamente isolados um do outro (compartimentalizados) para prevenir qualquer tipo de incidente de impactar simultaneamente os sistemas ou as demais rotas de distribuição/alimentação. A disponibilidade para o *Tier* IV é de 99,99%.

Cloud bursting

Em computação em nuvem, *cloud bursting* é uma configuração definida entre uma nuvem privada e uma nuvem pública para lidar com picos na demanda de TI. Se uma organização que usa uma nuvem privada alcançar 100% de sua capacidade de recursos, o tráfego excedente será direcionado a uma nuvem pública para que não haja interrupção de serviços.

Colocation

O *Colocation* é um serviço de aluguel apenas da infraestrutura de data center para a instalação do servidor do cliente. Ele se diferencia do servidor dedicado pela ausência de contratação do equipamento de processamento, já que esse pertence ao cliente. O serviço de *data center* entra como suporte, fornecendo serviço, espaço no *rack*, energia elétrica, conectividade com a internet, climatização, etc.

Confidencialidade

Propriedade que limita o acesso à informação somente às entidades autorizadas pelo proprietário da informação.

Criptografia

conjunto de princípios e técnicas empregados para cifrar a escrita, torná-la ininteligível para os que não tenham acesso às convenções combinadas.

Data center

Data center, Datacenter, ou Centro de Processamento de Dados, é um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como *switches*, roteadores, e outros.

DICA

Sigla para disponibilidade, integridade, confidencialidade e autenticidade.

Disponibilidade

Propriedade que garante que a informação esteja sempre disponível para o uso dos usuários autorizados pelo proprietário da informação.

Ferramenta de orquestração

Software utilizado para realizar a orquestração de serviços, como explicado na subseção 3.1.4.2.2.

Hosting

Hosting é hospedagem tradicional. Hospeda aplicações, soluções de tecnologia da informação ou ativos, além de gerenciar tarefas de manutenção para garantir o pleno e bom funcionamento do ambiente. Ele se apresenta em duas categorias: hospedagem dedicada e hospedagem compartilhada.

IDC

A *International Data Corporation* é uma fornecedora chinesa de inteligência de mercado, serviços de consultoria e eventos para os mercados de tecnologia da informação, telecomunicações e tecnologia de consumo.

Integridade

Propriedade que assegura que a informação manipulada mantém todas as características originais estabelecidas pelo proprietário da informação.

Multi-tenant

O termo *multi-tenant* refere-se a uma arquitetura onde uma única instância lógica é compartilhada por centenas ou milhares de usuários. Em outras palavras, a típica arquitetura que permite a otimização do uso de recursos de infraestrutura e software através de compartilhamento, mantendo os inquilinos, usuários, logicamente separados. Normalmente os usuários compartilharem os mesmos recursos computacionais: processador , armazenamento, espaço, memória, etc.

NIST

O *National Institute of Standards and Technology* (NIST) (em português: Instituto Nacional de Padrões e Tecnologia), anteriormente conhecido como *The National Bureau of Standards*, é uma agência governamental não regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos. A missão do instituto é promover a inovação e a competitividade industrial dos Estados Unidos, promovendo a metrologia, os padrões e a tecnologia de forma que ampliem a segurança econômica e melhorem a qualidade de vida.

On-premises

O sistema *on-premises* é o uso de servidores, equipamentos e recursos de TI dentro da empresa sob sua responsabilidade. Ou seja, é utilizada infraestrutura local interna própria ou de terceiros em vez de serviço externo para processar suas aplicações de *hardware* e *software*. A própria empresa é responsável pelas configurações, implementações e atualizações. .

OPEX

OPEX é uma sigla derivada da expressão *Operational Expenditure*, que significa o capital utilizado para manter ou melhorar os bens físicos de uma empresa, tais como equipamentos, propriedades e imóveis. As despesas operacionais são os preços contínuos para dirigir um produto, o negócio, ou o sistema.

Política de Segurança da Informação e Comunicações (POSIC)

Documento aprovado pela autoridade responsável do órgão ou entidade da APF, como o objetivo de estabelecer ações que visam a garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações produzidas ou custodiadas por estes, independentemente da forma e do meio físico em que estejam registradas.

Recursos criptográficos

sistemas, programas, processos, equipamentos isolados ou em rede que utilizam algoritmo simétrico ou assimétrico para realizar cifração ou decifração.

Sala segura

Possui todas as características de uma sala-cofre, exceto a certificação ABNT NBR 15247. No entanto, uma sala segura deve estar em conformidade com outras certificações internacionais equivalentes, como por exemplo, a EN 1363-1.

Sala-cofre

A Sala Cofre é um sistema modular composto por painéis remontáveis, para proteção física de equipamentos de *hardware*, formando uma Sala dentro de Sala. Pode ser montada com o data center em funcionamento, sendo possível ampliá-la ou mudá-la para outro local, conforme a necessidade do cliente, o que preserva o investimento realizado. Para ser classificado como sala-cofre, o ambiente deve estar em conformidade com as normas ABNT NBR 15247 (teste de fogo, calor e umidade; teste de resistência a desmoronamentos).

Servidores físicos

Em informática, um servidor é um *software* ou computador, com sistema de computação centralizada que fornece serviços a uma rede de computadores, chamada de cliente. O servidor físico é aquele computador que ficará na empresa, numa sala específica de TI e será utilizado como ponto de acesso e armazenagem de informações, onde serão guardados documentos importantes, implantados softwares, banco de dados, dados de acesso, entre outros.

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.

Apêndices

APÊNDICE A – Leis, decretos, normativos e documentos vigentes aplicáveis à contratação de serviços em nuvem

Neste apêndice encontram-se as leis, decretos, instruções normativas e documentos vigentes aplicáveis à contratação de serviços em nuvem identificados quando do levantamento de referências para a realização deste trabalho. No Quadro 20, encontram-se as leis, no Quadro 21, os decretos, no Quadro 22 as instruções normativas, no Quadro 23 as normas complementares e no Quadro 24 os demais documentos.

Quadro 20 – Leis vigentes aplicáveis à contratação de serviços em nuvem

Lei	**Descrição**
Lei nº 8.666, de 21 de junho de 1993 (BRASIL, 1993)	Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências
Lei nº 10.520, de 17 de julho de 2002 (BRASIL, 2002)	Institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências.
Lei nº 12.527, de 18 de novembro de 2011 (BRASIL, 2011)	Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.
Lei nº 12.965, de 23 de abril de 2014 (BRASIL, 2014a)	Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. (Marco Civil da Internet)
Lei nº 13.709, de 14 de agosto de 2018 (BRASIL, 2018c)	Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

Fonte: Elaboração própria.

Quadro 21 – Decretos vigentes aplicáveis à contratação de serviços em nuvem

Decreto	**Descrição**
Decreto nº 5.450, de 31 de maio de 2005 (BRASIL, 2005)	Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências
Decreto nº 7.174, de 12 de maio de 2010 (BRASIL, 2010)	Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União.
Decreto nº 7.724, de 16 de maio de 2012 (BRASIL, 2012a)	Regulamenta a Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.
Decreto nº 7.845, de 14 de novembro de 2012 (BRASIL, 2012b)	Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.
Decreto nº 7.892, de 23 de janeiro de 2013 (BRASIL, 2013a)	Regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666, de 21 de junho de 1993.
Decreto nº 8.771, de 11 de maio de 2016 (BRASIL, 2016a)	Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.
Decreto nº 9.637, de 26 de dezembro de 2018 (BRASIL, 2018b)	Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional

Fonte: Elaboração própria.

Quadro 22 – Instruções Normativas vigentes aplicáveis à contratação de serviços em nuvem

Instrução Normativa	**Descrição**
Instrução Normativa GSI /PR nº 1, de 13 de junho de 2008. (BRASIL, 2008);	Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
Instrução Normativa GSI /PR nº 2, de 5 de fevereiro de 2013. (BRASIL, 2013b)	Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.
Instrução Normativa GSI /PR nº 3, de 06 de março de 2013. (BRASIL, 2013c)	Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.
Instrução Normativa nº 1, de 4 de abril de 2019. (BRASIL, 2019)	Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

Fonte: Elaboração própria.

Quadro 23 – Normas Complementares vigentes aplicáveis à contratação de serviços em nuvem

Norma Complementar	**Descrição**
NC nº 06/IN01/DSIC/ GSIPR (BRASIL, 2009)	Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
NC nº 07/IN01/DSIC/ GSIPR (BRASIL, 2014b)	Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.
NC nº 14/IN01/DSIC/ GSIPR (BRASIL, 2018d)	Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.
NC nº 19/IN01/DSIC/ GSIPR (BRASIL, 2014c)	Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta.

Continua na próxima página

Quadro 23 – Continuação

Norma Complementar	Descrição
NC Nº 21/IN01/DSIC/GSIPR (BRASIL, 2014d)	Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

Fonte: Elaboração própria.

Quadro 24 – Outros normativos e documentos aplicáveis à contratação de serviços em nuvem

Documento	Descrição
Acórdão (TCU) 1.739 /2015 (BRASIL. TCU, 2015)	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.
Acórdão (TCU) 2.659 /2018 (BRASIL. TCU, 2018)	Avaliar as práticas comerciais adotadas por grandes fabricantes de tecnologia da informação (TI) na relação com a Administração Pública, quando da contratação de licenciamento de software e seus serviços agregados.
Portaria MP/STI nº 20 , de 14 de junho de 2016 (BRASIL. MP, 2016a)	Dispõe sobre orientações para contratação de soluções de Tecnologia da Informação no âmbito da Administração Pública Federal direta, autárquica e fundacional e dá outras providências.
Boas Práticas, Orientações e Vedações para Contratação de Serviços de Computação em Nuvem (BRASIL. MP, 2016b)	Este documento de Boas práticas, Orientações e Vedações tem força normativa legal, estando vinculado à Portaria MP/STI nº 20, de 14 de junho de 2016, na forma de anexo, tendo sido assinado, em sua última versão, pelo Secretário de Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão em 13/05/2016 e publicado na mesma data.
ABNT NBR ISO/IEC 27001:2013 (ABNT, 2013a)	Especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização.

Continua na próxima página

Quadro 24 – Continuação

Documento	Descrição
ABNT NBR ISO/IEC 27002:2013 (ABNT, 2013b)	Fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.
ABNT NBR ISO/IEC 27017:2016 (ABNT, 2016)	Fornece diretrizes para os controles de segurança da informação aplicáveis à prestação e utilização de serviços em nuvem, fornecendo o seguinte: diretrizes adicionais para implementação de controles relevantes especificados na ABNT NBR ISO/IEC 27002; controles adicionais com diretrizes de implementação que são relacionadas especificamente a serviços em nuvem.
ABNT NBR ISO/IEC 27018:2018 (ABNT, 2018)	Estabelece objetivos de controle, controles e diretrizes comumente aceitos para implementação de medidas para proteger as Informações de Identificação Pessoal (PII) de acordo com os princípios de privacidade descritos na ISO/IEC 29100, para o ambiente de computação em nuvem pública.

Fonte: Elaboração própria.

APÊNDICE B – Trabalhos Acadêmicos Relacionados

Neste apêndice, no Quadro 25, encontram-se os trabalhos acadêmicos relacionados à contratação de nuvem no setor público brasileiro.

Quadro 25 – Trabalhos acadêmicos relacionados à contratação de nuvem no setor público brasileiro

Título	**Autor**	**Ano**	**Objetivo geral**
Critérios para avaliação de viabilidade da adoção de computação em nuvem por parte de organizações da Administração Pública Federal (EVANGELISTA, 2014)	Wellington Galdino Evangelista	2014	Propor critérios para a avaliação de viabilidade de uma organização da Administração Pública Federal em adotar a modalidade de serviço da computação em nuvem conhecida como *Software* como serviço ou simplesmente SaaS, de um provedor de mercado
Requisitos para a contratação de serviços em computação em nuvem pela Administração Pública Federal (LOPES, 2015)	Thiago Ferreira Lopes	2015	Identificar os requisitos que devem constar num acordo de nível de serviço ou contrato entre empresas e/ou órgãos vinculados à APF com um provedor de serviço de computação em nuvem externo, considerando a legislação atual e as diretrizes governamentais.
Uso da Computação em Nuvem no Setor Público: um estudo de caso com gestores de TI do Estado do Rio Grande do Norte e do Governo Federal (MEDEIROS; SOUSA NETO, 2016)	Marcos Fernando Machado de Medeiros e Manoel Veras Sousa Neto	2016	Identificar os fatores qeu influenciam a utilização da computação em nuvem na esfera pública, no Brasil

Continua na próxima página

Quadro 25 – Continuação

Título	Autor	Ano	Objetivo geral
Cloud Computing - Normas, Leis e Orientações do Governo Brasileiro (FERREIRA; ANDRADE, 2016)	Marina A. Ferreira e César A. B. Andrade	2016	Explicitar da maneira mais simples e concisa possível as principais leis, normas e orientações no Brasil que envolvam computação em nuvem
Um comparativo entre os modelos de Brasil, Estados Unidos da América e Reino Unido para a contratação de serviços em nuvem (NOGUEIRA, 2016)	Gilberto Souza Nogueira	2016	Comparar o modelo de contratação a fim de extrair desse estudo o modo pelo qual os países usados na análise adquirem os serviços de computação em nuvem e lidam com a questão da segurança digital.
Modelo de avaliação da capacidade das organizações da administração pública federal para a adoção de software as a service (SaaS) público (EVANGELISTA; SOUZA NETO, 2016)	Wellington Galdino Evangelista e João Souza Neto	2016	Identificar quais são os critérios que devem ser considerados no momento em que uma entidade da administração pública federal (APF) decidir adotar a computação em nuvem
Em direção a uma proposta de utilização da computação em nuvem na Administração Pública Federal: um estudo de caso no Instituto Federal Goiano (VIROTE, 2016)	Alfredo Pupak Pereira Virote	2016	Elaborar um catálogo de boas práticas para contratações de serviços de Computação em Nuvem contendo o passo a passo das diretrizes a serem seguidas nos diversos órgãos da APF.
Utilização da computação em nuvem no poder legislativo: percepções dos gestores e entraves ao uso (DINIZ; COSTA; MEDEIROS, 2017)	Igor Vinicius de Lucena Diniz, Lucas dos Santos Costa e Marcos Fernando M. Medeiros	2017	Avaliar a aderência da computação em nuvem ao Poder Legislativo de um estado brasileiro, no que se refere à sua forma de utilização, como na efetivação da computação em nuvem como uma política pública de tecnologia da informação.

Continua na próxima página

Quadro 25 – Continuação

Título	Autor	Ano	Objetivo geral
Políticas públicas brasileiras de computação em nuvem: análise documental dos relatórios do global cloud computing scorecard (COSTA; MEDEIROS, 2017)	Lucas dos Santos Costa e Marcos Fernando Machado de Medeiros	2017	Apresentar as iniciativas de políticas públicas de computação em nuvem desenvolvidas no Brasil
Critérios de migração do processamento e armazenamento de dados da administração pública para a nuvem (FREITAS, 2018)	Pedro Henrique Chagas Freitas	2018	Investigar os critérios que devem respaldar a migração dos recursos computacionais de processamento e armazenamento de dados para nuvem no contexto da administração pública federal.
Uma proposta de migração de sistemas legados do governo para a nuvem (COSTA, 2018)	Breno Gustavo Soares da Costa	2018	Propor um modelo de referência de migração de sistemas legados para a nuvem
Melhores práticas para a adoção de backup em nuvem por órgãos do Poder Legislativo Federal (SANTOS, 2019)	Eduardo Ferraz dos Santos	2019	Identificar as melhores práticas que devem ser seguidas pelos órgãos do Poder Legislativo Federal para a adoção de backup em nuvem, considerando tanto a particularidade de suas atribuições quanto o alinhamento com a legislação e jurisprudência vigentes

Fonte: Elaboração própria.

APÊNDICE C – Normativos do Senado Federal

Neste apêndice, no Quadro 26, encontram-se as resoluções, normas e atos próprios do SF relacionados às contratações do Senado Federal e a sua área de Tecnologia da Informação.

Quadro 26 – Normativos do Senado Federal aplicáveis à contratação de serviços em nuvem

Nº.	**Descrição**
Resolução nº 13/ 2018 (SF, 2018)	Consolida as alterações promovidas na estrutura administrativa do Senado Federal
ATC nº 2/2008 (SF, 2008b)	Dispõe sobre a gestão de Contratos no Senado Federal e dá outras providências
ATC nº 16/2008 (SF, 2008a)	Institui, no âmbito do Senado Federal e de suas Secretarias Especiais e Órgãos Supervisionados, as minutas-padrão constantes do Anexo deste Ato e dá outras providências.
ATC nº 9/2012 (SF, 2013)	Regulamenta, no âmbito do Senado Federal, a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso aos dados, informações e documentos de interesse da sociedade e do Estado.
ATC nº 16/2013 (SF, 2013)	Institui a Política de Gestão de Riscos Organizacionais do Senado Federal.
ATC nº 8/2015 (SF, 2015a)	Regulamenta a atuação dos servidores que atuam como fiscais de contratos no âmbito do Senado Federal.
ATC nº 9/2017 (SF, 2017a)	Institui a Política Corporativa de Segurança da Informação do Senado Federal - PCSI.
APS nº 31/2009 (SF, 2009)	Estabelece a possibilidade de realização das compras e contratações eletrônicas do Senado Federal por meio do Portal de Compras do Governo Federal – COMPRASNET.
ADG nº 9/2015 (SF, 2015d)	Estabelece, no âmbito do Senado Federal, normas procedimentais para contratações.
ADG nº 20/2015 (SF, 2015b)	Dispõe sobre a fiscalização e a gestão dos contratos de prestação de serviços terceirizados de natureza continuada no âmbito do Senado Federal.
ADG nº 27/2015 (SF, 2015c)	Dispõe sobre procedimentos a serem adotados na gestão de contratos.

Fonte: Elaboração própria.

Encontra-se em estudo um novo ato normativo interno sobre contratações, porém, como o mesmo não está ainda em vigor não foi considerado neste estudo.