Riscos da computação em nuvem: estudo na ótica dos gestores de órgãos públicos federais no Brasil

Risks of cloud computing: a study from the perspective of managers of federal public agencies in Brazil

Andrio de Andrade Alves Bacharel em Administração. Universidade de Brasília (UnB) - Brasil. andrio.aa@gmail.com
http://orcid.org/0000-0003-0396-5345
Carlos André de Melo Alves Doutor em Administração pela Universidade de São Paulo. Professor da Universidade de Brasília (UnB) – Brasil. carlosandre@unb.br
http://orcid.org/0000-0001-9566-2514

Fábio Galvão Ferreira Tabosa Especialista em Governança de TI, Centro de Desenvolvimento do Serviço Nacional Aprendizagem Comercial (Senac) – Brasil. fabio.tabosa@gmail.com
http://orcid.org/0000-0002-1028-6781
Rafael Rabelo Nunes Doutor em Engenharia Elétrica. Universidade de Brasília (UnB) – Brasil. rafaelrabelo@unb.br
http://orcid.org/0000-0002-1538-4276

RESUMO

Este trabalho teve como objetivo avaliar os riscos ao se implantar serviços de Computação em Nuvem na ótica dos gestores de órgãos públicos federais no Brasil. Para alcançar o objetivo proposto, foram realizadas entrevistas semiestruturadas com servidores de nível tático, envolvidos com a gestão de tecnologia da informação de dez órgãos da Administração Pública Federal. Os dados foram analisados com base nas recomendações de entidades internacionais para enfrentamento de riscos dessa natureza, com base em nove dimensões: governança; legislação e regulamentações; conformidade e auditoria; continuidade dos negócios; segurança; isolamento; gestão de identidade e de acessos; proteção de dados; e resposta a incidentes. Os resultados demonstraram que ainda há um caminho a ser percorrido para a implementação desses serviços na Administração Pública, principalmente quando se refere a questionamentos acerca dos riscos que estão atrelados ao seu uso, com atenção ao tratamento de dados sensíveis. Em complemento, para se implementar o serviço de computação em nuvem como proposto pela Estratégia de Transformação Digital, os achados sugerem a necessidade de enfrentar riscos de transposição complexa, fato que funciona como incentivo para postergar a implementação dessa tecnologia por entidades governamentais brasileiras.
Palavras-chave: Computação em Nuvem. Riscos. Setor Público. Governo Eletrônico.

ABSTRACT

This work aimed to evaluate the risks when deploying Cloud Computing services from the perspective of managers of federal public agencies in Brazil. To achieve the proposed objective, semi-structured interviews were conducted with tactical level servers, involved with the management of information technology of ten Federal Public Administration agencies. The data were analyzed based on the recommendations of international entities to face risks of this nature, based on nine dimensions: governance; legislation and regulations; compliance and auditing; business continuity; security; isolation; identity and access management; data protection; and incident response. The results showed that there is still a way to go to implement these services in Public Administration, especially when it comes to questions about the risks that are linked to their use, with attention to the treatment of sensitive data. In addition, to implement the cloud computing service as proposed by the Digital Transformation Strategy, the findings suggest the need to face risks of complex transposition, a fact that works as an incentive to delay the implementation of this technology by Brazilian government entities.
Keywords: Cloud Computing. Risks. Public Sector. e-Government.

Recebido em 22/01/2021. Aprovado em 22/05/2021. Avaliado pelo sistema *double blind peer review*. Publicado conforme normas da ABNT.
https://doi.org/10.22279/navus.2021.v11.p01-18.1513

1 INTRODUÇÃO

A computação em nuvem é um modelo criado para permitir acesso onipresente, de forma conveniente e sob demanda a um conjunto compartilhado de recursos de computação configuráveis, os quais podem ser rapidamente provisionados e liberados com esforço mínimo de gerenciamento (MELL; GRANCE, 2011).

Em todo o mundo, as organizações governamentais têm modificado a infraestrutura computacional de serviços localmente mantidos para serviços ofertados por meio da computação em nuvem, de forma a reduzir o custo total com os investimentos em infraestrutura de TI e aproveitar os benefícios desse novo paradigma de computação (JONES *et al*., 2019).

Além da redução de custos, (MARSTON *et al*., 2011) descrevem outras vantagens gerais no uso da computação em nuvem: a redução de barreiras; a inovação; e a facilidade para escalar a aquisição de novos serviços. Essa última também é considerada uma característica do modelo de Veras (VERAS, 2012; MELL; GRANCE, 2011). Ademais, esses autores também elencam a possibilidade de autoatendimento sob demanda, do amplo acesso a serviços de rede, do *pool* de recursos, e de os serviços serem mensuráveis.

Em 2018, o Governo Federal publicou sua Estratégia Brasileira para a Transformação Digital (E-Digital), cujo objetivo é "aproveitar todo o potencial das tecnologias digitais para alcançar o aumento da produtividade, da competitividade e dos níveis de renda e emprego por todo o País, visando a construção de uma sociedade livre, justa e próspera para todos" (BRASIL, 2018c, p. 6).

A computação em nuvem é uma tecnologia que oferece uma infraestrutura para armazenar e processar dados. Nesse sentido, uma das ações estratégicas da E-Digital é "desenvolver política que estimule a adoção de nuvem como parte da estrutura tecnológica dos diversos serviços e setores da Administração Pública" (BRASIL, 2018c, p. 66).

Considerando o exposto, este trabalho apresenta o seguinte problema: quais são os riscos no uso dos serviços de computação em nuvem na ótica dos gestores de órgãos públicos federais do Brasil? Dessa forma, o objetivo é avaliar os riscos ao se implantar serviços de Computação em Nuvem, tomando como base a experiência na utilização dos serviços de nuvem a partir do ponto de vista dos gestores de órgãos públicos federais do Brasil.

O trabalho está organizado da seguinte forma: além desta introdução, a seção 2 apresenta o referencial teórico onde serão discorridos os modelos da computação em nuvem, os seus riscos, e as recomendações para a gestão desses riscos; em seguida, tem-se uma seção 3 com detalhamento da metodologia utilizada no trabalho; a seção 4 apresenta os resultados e sua análise; por fim, apresenta-se a conclusão.

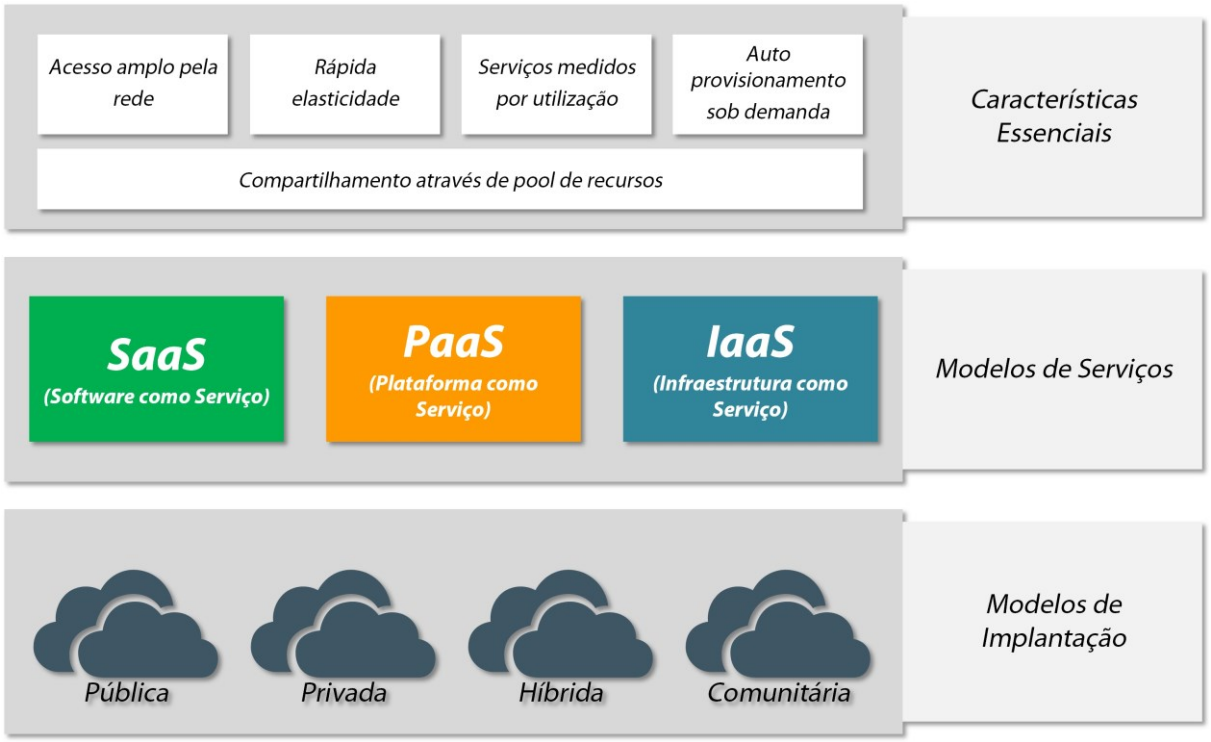
2 REFERENCIAL TEÓRICO

O *National Institute of Standards and Technology* - NIST, responsável pelo desenvolvimento de normas e orientações de segurança da informação, incluindo requisitos mínimos para os sistemas de informação federais do Governo dos Estados Unidos, apresenta definição de conceitos de nuvem considerada pelo Tribunal de Contas da União - TCU (BRASIL, 2015).

2.1 Computação em nuvem: aspectos conceituais e modelos de serviços

Esses conceitos de nuvem abrangem cinco características essenciais, três modelos de serviço e quatro modelos de implantação, ilustrados na Figura 1.

Figura 1 – Forma visual dos conceitos de nuvem



Fonte: Adaptado da NIST (MELL; GRANCE, 2011) e CSA (CLOUD SECURITY ALLIANCE, 2017, p. 10).

O NIST (MELL; GRANCE, 2011) descreve, de maneira abrangente, as cinco características essenciais de computação em nuvem, citadas na Figura 1, da seguinte forma:

- **Acesso amplo pela rede:** os recursos da nuvem estão disponíveis para acesso pela rede por diferentes dispositivos (estações de trabalho, *tablets*, *smartphones* etc.) através de mecanismos padrões.
- **Rápida elasticidade:** os recursos computacionais podem ser elasticamente provisionados e liberados e, em alguns casos, de maneira automática, adaptando-se à demanda.
- **Serviços medidos por utilização:** os serviços de computação em nuvem automaticamente controlam e otimizam a utilização de recursos através de mecanismos de medição utilizados em nível de abstração associado ao tipo de serviço utilizado, como armazenamento, processamento, largura de banda e contas de usuário ativas.
- **Auto provisionamento sob demanda:** o consumidor pode ter a iniciativa de provisionar recursos na nuvem e ajustá-los de acordo com as suas necessidades ao decorrer do tempo, de maneira automática, sem a necessidade de interação com cada provedor de serviços.
- **Compartilhamento através de *pool* de recursos**: os recursos computacionais do provedor são agrupados para servir a múltiplos consumidores (modelo *multi-tenant*) com recursos físicos e virtuais, sendo alocados e realocados dinamicamente de acordo com a demanda dos seus consumidores.

Quanto aos três principais modelos de serviços de nuvem ilustrados na Figura 1, eles são baseados numa arquitetura em camadas hierárquicas, na qual os serviços da camada superior são provisionados pela camada inferior subsequente (BRASIL, 2015; MELL; GRANCE, 2011; VERAS, 2012), a saber:

- **Infraestrutura como um serviço** (*Infrastructure as a Service - IaaS*): é a capacidade oferecida ao consumidor de fornecer processamento, armazenamento, redes e outros recursos fundamentais de computação, nos quais se pode implementar e executar softwares arbitrários, podendo incluir sistemas operacionais e aplicativos. Exemplos de segmento e produtos: Armazenamento e *Backup* (EMC, Symantec, RainStor, Amazon S3) e Computação (Amazon EC2, JitScale, Rackspace, Uniserver, Microsoft Azure, Google Compute Engine).

- **Plataforma como um serviço** (*Platform as a Service - PaaS*): é a capacidade oferecida ao consumidor de implementar os aplicativos criados ou adquiridos na infraestrutura em nuvem. Exemplos de segmento e produtos: Desenvolvimento de Aplicações Genéricas (Google App Engine, Microsoft Azure) e Desenvolvimento de Aplicações Especificas (Salesforce Force.com, SaaSPlaza, SAP Business ByDesign).
- ***Software* como um serviço** (*Software as a Service - SaaS*): possibilidade de usar os aplicativos do provedor em execução em uma infraestrutura de nuvem. Os aplicativos são acessíveis a partir de vários dispositivos, como um navegador da Web (por exemplo, *e-mail* baseado na Web) ou uma interface de programa. Exemplo de segmento e produtos: *Supply Chain Management* - SCM (Descartes, Ariba, Ketera, JDA Software), Sistema integrado de gestão empresarial - ERP (NetSuite, Exact Online, Twinfield, SAP Business ByDesing, Infor), Gestão de Relacionamento com o Cliente - CRM (Salesforce.com, PerfectView CRM Online, AccountView CRM Online), Produtividade de escritório (Google Apps, Microsoft Office 365 e Comunicação e colaboração - Cisco Webex, Microsoft Lync, IBM Lotusphere).

Independentemente do modelo de serviço, é necessário considerar também os modelos de implantação da nuvem (BRASIL, 2015; MELL; GRANCE, 2011). A implantação representa como a computação em nuvem será estruturada no que tange ao compartilhamento e controle de recursos físicos e virtuais (ABNT, 2016; MELL; GRANCE, 2011; TAURION, 2009; VERAS, 2012). Os modelos de implantação citados na Figura 1 podem ser assim descritos:

- **Nuvem Privada:** a infraestrutura de nuvem privada está disponível para uso exclusivo de uma única organização.
- **Nuvem Comunitária:** a infraestrutura de nuvem comunitária está disponível para uso exclusivo de uma comunidade específica, formada por organizações que possuem interesses e preocupações em comum.
- **Nuvem Pública:** a infraestrutura de nuvem pública está disponível para uso aberto do público em geral e fica nas instalações do provedor.
- **Nuvem Híbrida:** a infraestrutura de nuvem é uma composição de duas ou mais infraestruturas de nuvem (privada, comunitária ou pública).

2.2 Riscos da computação em nuvem e recomendações para a gestão desses riscos em organizações

Os riscos da computação em nuvem trazem relação com o modelo de serviço e o modelo de sua implantação citados na Seção 2.1 deste estudo. A norma ABNT NBR 27017:2016, titulada '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', fornece diretrizes que apoiam a implementação de controles de segurança para clientes e provedores de serviços de nuvem (ABNT, 2016).

Os principais riscos elencados pela ABNT encontram-se evidenciados em variados artigos e relatórios, entre eles: *Guidelines on Security and Privacy in Public Cloud Computing* (JANSEN; GRANCE, 2011) e *Cloud Computing: benefits, risks and recommendations for information security* (CATTEDDU; HOGBEN, 2009). Esse último consolida as classes de riscos em três dimensões, descritas no Quadro 1, a saber: riscos organizacionais e de políticas; riscos técnicos; e riscos legais e regulatórios.

Quadro 1 – Riscos de computação em nuvem

Dimensão do Risco	Risco
Riscos organizacionais e de políticas	Perda de governança e controle Dependência do provedor de serviços de nuvem Serviços compostos e cadeia de disponibilidade
Riscos técnicos	Falha de isolamento Falha de interface de gerenciamento Exclusão dos dados incompleta ou insegura Gestão de identidade e acessos Invasores e ataques
Riscos legais e regulatórios	Conformidade Proteção de dados Residência de dados Auditoria e gestão de metadados

Fonte: Adaptado de (CATTEDDU; HOGBEN, 2009).

De forma a enfrentar esses riscos, algumas recomendações sobre gerenciamento de riscos podem ser propostas. O gerenciamento de riscos da computação em nuvem deve ser flexível o suficiente para lidar com um cenário em constante evolução e mudança, principalmente no que se trata de tecnologias (JANSEN; GRANCE, 2011). O NIST, a Agência da União Europeia para a Segurança Cibernética (ENISA) e a *Cloud Security Alliance* (CSA), instituições que contribuem para o fortalecimento de políticas de defesa cibernéticas, elencam pontos de relevância no que tange o uso de nuvem pelas organizações, incluindo recomendações para a gestão de tais riscos. Essas recomendações foram utilizadas como base para a construção da norma ABNT NBR ISO/IEC 27017 (ABNT, 2016) e estão estruturadas em nove dimensões, resumidas no Quadro 2.

Quadro 2 – Dimensões de recomendação para gestão de riscos em nuvem

Dimensão de Recomendação para Gestão de Riscos	Descrição
Governança	Conjunto de práticas, políticas e padrões, com a finalidade de garantir controles efetivos, ampliar os processos de segurança, minimizar os riscos e otimizar o desempenho das atividades de TI.
Legislação e regulamentações	Leis e regulamentos que impõem obrigações de segurança e privacidade à organização e, potencialmente, impactam as iniciativas de computação em nuvem.
Conformidade e auditoria	Mecanismos e ferramentas de auditoria para determinar como os dados são armazenados, protegidos e usados para validar os serviços e para verificar a aplicação das políticas, garantindo que as práticas organizacionais sejam seguidas durante todo o ciclo de vida dos sistemas.
Continuidade dos negócios	Assegurar que, durante uma interrupção intermediária ou prolongada ou um desastre grave, as operações críticas possam ser imediatamente retomadas e que todas as operações possam ser eventualmente reinstituídas de maneira oportuna e organizada.
Segurança	Medidas para garantir a disponibilidade, integridade, confidencialidade e a autenticidade da informação. Inclui avaliações de vulnerabilidade e testes de penetração, revisando regularmente certificações e atestados de conformidade específicos do setor, de forma a obter garantia de que o provedor está seguindo as práticas recomendadas e os regulamentos da infraestrutura em nuvem.

Isolamento	Entender a virtualização e outras técnicas de isolamento lógico que o provedor de nuvem emprega em sua arquitetura de *software* e avaliar os riscos envolvidos à organização, como também configurar adequadamente os serviços de virtualização de acordo com as orientações do provedor e outras práticas recomendadas em padrões e certificações do setor.
Gestão de Identidades e Acessos	Proteger as funções de autenticação, autorização, auditoria e outras funções de gerenciamento de identidade e acesso que sejam adequadas à organização.
Proteção de Dados	Utilizar a opção de criptografia apropriada com base nos modelos de gestão de riscos para os dados, negócios e requerimentos técnicos, e, sempre que possível, utilizar chaves gerenciadas pela organização. Não confiar e depender completamente dos controles de acesso e criptografia fornecidas pelo provedor.
Resposta a Incidentes	Certificar-se de que a organização possa responder aos incidentes de maneira coordenada com o provedor de nuvem, de acordo com suas respectivas funções e responsabilidades para o ambiente de computação.

Fonte: Adaptado da NIST (MELL; GRANCE, 2011) e CSA (CLOUD SECURITY ALLIANCE, 2017, p. 10).

No tocante à legislação e à regulamentação citadas no Quadro 2 e buscando minimizar riscos, é útil mencionar que a contratação dos serviços de nuvem pode ser normatizada em diferentes setores. Como exemplo, no setor financeiro brasileiro, a contratação desses serviços é regulamentada para instituições financeiras, com base na Resolução do Conselho Monetário Nacional nº 4.658, de 26 de abril de 2018 (BRASIL, 2018b), e para as instituições de pagamento, tal regulamentação baseia-se na Circular nº 3.909, de 16 de agosto de 2018 do Banco Central do Brasil (BRASIL, 2018a). Acrescenta-se que a referida resolução é aplicável, inclusive a bancos com controle público federal.

Por fim, ainda no contexto da legislação e da regulamentação elencadas no Quadro 2, podem ser lembradas recomendações direcionadas às organizações da Administração Pública Federal brasileira a respeito dos riscos na computação em nuvem, citando-se os seguintes exemplos: as orientações do Acórdão nº 1.739/2015-TCU, pelo Tribunal de Contas da União, a respeito dos riscos mais relevantes na contratação de serviços de nuvem (BRASIL, 2015); os pontos apresentados pela Portaria do Gabinete de Segurança Institucional - GSI nº 9/2018 (BRASIL, 2018d), que orienta as entidades governamentais a apenas trafegarem informações não sigilosas por meio da nuvem; e a Instrução Normativa nº 01/2019 divulgada pela Secretaria de Governo Digital do Ministério da Economia (BRASIL, 2019), que fomenta o uso de serviços de nuvem entre organizações públicas.

Em complemento, relativa às dimensões citadas no Quadro 2 'Legislação e regulamentações' e também 'Proteção de Dados', pode ser lembrada a Lei nº 13.709, de 14 de agosto de 2018, também chamada de Lei Geral Proteção de Dados Pessoais - LGPD (BRASIL, 2018e). Essa lei, embora não esteja relacionada diretamente a serviços de nuvem, traz obrigações quanto ao tratamento de dados pessoais sensíveis, a serem consideradas por organizações públicas que usem tais serviços.

2.3 Trabalhos correlatos

No decorrer da pesquisa bibliográfica, utilizando repositórios internacionais de pesquisa acadêmica, foram identificados trabalhos de pesquisa, os quais abrangem pesquisas semelhantes de avaliação na adoção de serviços de computação em nuvem por organizações governamentais. A seguir, serão descritos os trabalhos relacionados a objetivos semelhantes a este.

Em seu trabalho, (JONES *et al*., 2019) demonstram como as implantações de computação em nuvem podem complementar e melhorar as abordagens existentes à implementação de TI. Nesse estudo de pesquisa,

destacaram-se as experiências de implantação de uma solução de computação em nuvem implementadas para três organizações do setor público no Reino Unido. A descoberta empírica salientou classificações de vantagens (estratégicas, táticas e operacionais) e evidenciou riscos a que se sujeitam a organização adotante da solução.

Em (ALI *et al*., 2020), os autores apresentam a aplicação de um modelo de requisitos de segurança de computação em nuvem conceitual com quatro componentes - segurança de dados; avaliação de risco; requisitos legais e de conformidade; e requisitos técnicos e de negócios - de forma a promover uma visão equilibrada sobre segurança em nuvem para governos. O trabalho foi conduzido com 480 funcionários de TI do governo Australiano.

3 METODOLOGIA

A presente pesquisa trata-se de um estudo descritivo e exploratório com abordagem qualitativa. Ao estudar campos como risco e segurança, os pesquisadores tendem a confiar em métodos subjetivos que exigem a entrada de respondentes bem qualificados para obter dados (TANG *et al*., 2008).

Para coletar os dados da pesquisa, foram utilizadas entrevistas semiestruturadas - às vezes chamadas de entrevistas informais - tratando de conversar com pessoas, mas de maneira que sejam autoconscientes, organizadas e parcialmente estruturadas (LONGHURST, 2010). Entrevistas são tipicamente usadas quando os objetivos do estudo são complexos e difíceis de explicar concisamente em um formulário de pesquisa e quando informações detalhadas são necessárias (BURLESON; LEVINE; SAMTER, 1984).

A seleção de participantes para entrevistas semiestruturadas é de grande importância. Tradicionalmente as pessoas são escolhidas com base em sua experiência relacionada ao tema da pesquisa (CAMERON; KNEALE; SEE, 2002). Nesse trabalho, os entrevistados foram dez servidores de diferentes organizações do Governo Federal, incluindo o Poder Judiciário, Executivo, o setor financeiro e as agências reguladoras, citadas no Quadro 3. O período das entrevistas ocorreu em abril de 2019.

Quadro 3 – Organizações públicas em que os gestores públicos entrevistados atuam.

Poderes da esfera federal	Organização
Judiciário	Conselho da Justiça Federal – CJF
Executivo	Advocacia Geral da União - AGU; Agência de Promoção de Exportações e Investimentos - APEX; Agência Nacional de Energia Elétrica - ANEEL; Agência Nacional de Vigilância Sanitária - ANVISA; Banco do Brasil Tecnologia e Serviços – BBTS; Caixa Econômica Federal - CEF; Ministério da Economia - ME; Ministério do Desenvolvimento Regional - MDR; e Secretaria do Tesouro Nacional - STN.

Fonte: Elaborado pelos autores, a partir de dados da pesquisa

O critério para selecionar o gestor público entrevistado de cada organização citada no Quadro 3 foi a necessidade de que esse fizesse parte de departamentos relacionados a Tecnologia da Informação, Infraestrutura, Segurança ou equivalentes e estivesse incluído em um ou mais dos seguintes grupos:

- Posições de tomadores de decisões a respeito de Tecnologia da Informação ou equivalentes (Diretor, Chefe de divisão, *Chief Information Officer*, entre outros).
- Posições de influência em coordenações de Segurança da Informação das instituições (analistas, gerentes, coordenadores, entre outros).

- Posições de influência na coordenação de infraestrutura relacionada à Tecnologia da Informação das instituições (analistas, gerentes, coordenadores, entre outros).

As entrevistas foram iniciadas abordando questões relativas ao uso de tecnologias baseadas em nuvem, a fim de avaliar a ótica dos participantes quanto à gestão dos riscos no contexto de cada organização. Para isso, os entrevistados foram perguntados a respeito das circunstâncias presentes, passadas e futuras quanto à utilização de recursos em nuvem pelas suas organizações.

Ao conduzir as entrevistas semiestruturadas, é possível fazer anotações ou gravar áudio da discussão, permitindo concentrar-se totalmente na interação (VALENTINE, 2005). Logo após a entrevista, documentam-se os principais temas que surgiram e qualquer assunto que possa ter valor para agregar à pesquisa, qualificando esse procedimento como análise de dados qualitativos (KITCHIN; TATE; NICHOLAS, 2000; MILES; HUBERMAN, 1994).

Os dados levantados com a execução das entrevistas foram utilizados para compor a descrição e as análises dos resultados relativos à ótica dos entrevistados, com relação à gestão de riscos no uso da computação em nuvem nos órgãos públicos em que atuam. Na segmentação dessa análise, foram consideradas, inclusive, as dimensões descritas no Quadro 2.

Para atingir os objetivos propostos neste estudo, não se fez necessário identificar os entrevistados, optando-se por segmentar as respostas de maneira anônima, utilizando-se uma numeração de 1 a 10 para fazer remissão a cada entrevistado, incluindo siglas como, por exemplo, E01, E02 em diante. As perguntas aplicadas aos entrevistados estão citadas nos Quadro 4 e no Quadro 5.

Quadro 4 – Relação de perguntas aplicadas nas entrevistas – Maturidade.

Critério Maturidade	Perguntas
Maturidade no uso de Nuvem	1. Hoje a sua instituição utiliza serviços ou soluções baseadas em computação em nuvem? Quais?
	2. Há quanto tempo esse tipo de tecnologia está sendo utilizado pela instituição?
	3. Há serviços ou soluções em nuvem que a sua organização deixou de utilizar? Quais os motivos para que eles fossem descontinuados?
	4. Há serviços ou soluções que a organização deseja adquirir no futuro ou planos para migrar mais recursos para a nuvem? Quais e por quais motivos?

Fonte: Elaborado pelos autores, a partir de dados da pesquisa

Quadro 5 – Relação de perguntas aplicadas nas entrevistas – Dimensões de Riscos.

Dimensão de Recomendação para Gestão de Riscos	Perguntas
I. Governança	1. A sua organização estabeleceu uma política ou procedimento para decidir em quais casos é apropriado usar os serviços de computação em nuvem?
	2. Existe um planejamento de gestão de riscos sobre o uso da nuvem?
II. Legislação e Regulamentações	1. Você enxerga riscos a sua organização implicados pela legislação brasileira quanto ao uso de nuvem? Quais?
	2. Quais as medidas que a sua organização tem tomado para se adequar à legislação atual quanto ao uso de nuvem?
	3. Em quais aspectos você acredita que a legislação pode prejudicar ou promover o avanço tecnológico do Governo quanto ao uso de nuvem?
III. Conformidade e Auditoria	1. Você enxerga riscos a sua organização referentes à conformidade e auditoria relacionados ao uso de sistemas em nuvem?
	2. Existe um planejamento para lidar com tais riscos?

IV. Continuidade dos Negócios	1. Quais são as maiores preocupações quanto aos riscos do uso de nuvem que possam impedir as atividades da instituição?
	2. Existe um planejamento para lidar com tais riscos?
V. Segurança	1. Quais são as maiores preocupações da organização quanto à segurança dos serviços em nuvem?
	2. Quais são as estratégias sendo executadas para a gestão dos riscos de segurança?
VI. Isolamento	1. Quais são as maiores preocupações da organização quanto ao isolamento das redes, aplicações, contas com privilégios e ambientes virtuais corporativos?
	2. Quais são as estratégias sendo executadas para garantir o isolamento dos ambientes virtuais da organização?
VII. Gestão de Identidade e Acessos	1. Quais as maiores preocupações e riscos considerados quanto a gestão de identidade e acessos a serviços em nuvem?
	2. Quais as estratégias sendo implementadas para gerenciar esses riscos?
VIII. Proteção de Dados	1. Quais são as maiores preocupações da organização quanto à proteção de dados e riscos relacionados?
	2. Se informações sensíveis estiverem envolvidas, são necessárias medidas diferenciadas?
	3. Quais são as medidas que estão sendo executadas quanto a esse assunto?
IX. Resposta a Incidentes	1. Quais as maiores preocupações da instituição quanto aos riscos relacionados a incidentes e sua remediação?
	2. Quais medidas estão sendo implementadas para uma resposta eficiente a incidentes?
Critério Risco	Perguntas
Riscos de uso de Nuvem	1. Quais são as maiores preocupações da organização quanto ao uso de nuvem e seus riscos?

Fonte: Elaborado pelos autores, a partir de dados da pesquisa

4 RESULTADOS

Nesta seção serão apresentados os resultados da pesquisa em seções: a primeira mostra resultados sobre o uso da computação em nuvem nos órgãos públicos, na ótica dos entrevistados (Subseção 4.1); em seguida, serão mostrados resultados sobre o nível de maturidade no uso de nuvem de cada um dos órgãos, de acordo com a ótica dos entrevistados (Subseção 4.2); por fim, apresentam-se os principais pontos relatados pelos entrevistados, no que tange às recomendações para enfrentamento de riscos em nuvem, de acordo com os pontos elencados pelo NIST, ENISA e a CSA (Subseção 4.3).

4.1 Gestão de riscos em nuvem na ótica dos entrevistados

Após serem entrevistados quanto ao uso da nuvem, a abordagem aos entrevistados contemplou os pontos elencados no Quadro 2, com relação à gestão de riscos em nuvem, levando em conta as dimensões citadas no referido quadro. Nessa etapa da entrevista, o objetivo foi que os entrevistados elencassem os riscos a serem endereçados pelas organizações e avaliar quais são os planos delas para mitigar os riscos relacionados. Buscou-se categorizar, na ótica de cada entrevistado e com base no seu relato, a situação atual do planejamento estratégico de cada organização, observando se estão sendo executadas ações à gestão dos referidos riscos ou não, como também se existiriam planos à implementação de práticas ou políticas a respeito dos citados riscos.

4.1.1 Governança

Segundo todos os entrevistados, no período em que os dados foram coletados os planejamentos quanto à governança específica para o uso de nuvem estavam em andamento e em fase inicial. Portanto, ainda não houve implementação de políticas e diretrizes sendo executadas, mas vinham sendo desenvolvidas à medida que a maturidade dos órgãos também evoluía quanto ao uso dessa tecnologia.

Tratando-se das maiores tendências de governança entre os entrevistados, destacam-se as questões relativas à Portaria GSI nº 9/2018 (BRASIL, 2018d), que orienta as instituições governamentais a apenas trafegarem informações não sigilosas por meio da nuvem, o que tem sido discutido e incentivado internamente por todas as organizações entrevistadas. Porém, no período em que os dados foram coletados não existiam controles implementados nas instituições para identificar se essa orientação vem sendo executada propriamente pelos usuários.

Em seguida, ressalta-se a atenção à criação de políticas que governem o uso dos recursos em nuvem de forma a controlar os gastos, para que se mantenham no orçamento planejado pela instituição no momento de sua contratação. Sem políticas efetivas, podem ocorrer situações em que o uso indevido dos recursos implique em gastos não previstos, os quais, se estiverem fora do orçamento, podem gerar um impacto no funcionamento de sistemas críticos da organização.

Com base nos dados coletados, 30% das instituições ainda não iniciaram o seu planejamento para estruturar uma governança específica de nuvem, enquanto 70% delas estão iniciando processos para estruturar comitês de arquitetura e segurança, que deverão elaborar as especificações a serem seguidas pelas entidades, incluindo as definições de quais sistemas e informações deverão ser trafegadas em nuvem, com base em análises dos riscos elencados pelo Acórdão nº 1.739/2015 do TCU (BRASIL, 2015), previamente citada no referencial teórico deste estudo.

4.1.2 Legislação e regulamentações

Quanto à legislação e regulamentações, 60% das instituições demonstraram maior relevância quando se trata da possibilidade de não estarem em conformidade com as normas que limitam o tráfego de informações sigilosas, visto que os servidores possuem maior trabalho para categorizar e decidir o que pode ser trafegado no ambiente, correndo-se o risco de serem armazenadas informações em lugares considerados indevidos por sua classificação.

Destaca-se, inclusive, que a regulação atual implica em consequências negativas quanto à praticidade do uso da nuvem, afirmando que as legislações impostas podem prejudicar o avanço tecnológico do governo no caso dos provedores não se adequarem a tais exigências, limitando certas formas de utilização da nuvem que podem inviabilizar o seu uso pelas instituições.

Já os demais 40% dos entrevistados se posicionaram de maneira oposta ao relato do parágrafo anterior, afirmando que a legislação estabelece diretrizes mais seguras quando se trata da utilização da nuvem pelo governo, sendo benéficas, pois ajudam a evitar vazamentos de dados.

Apesar dos pontos adversos, os entrevistados concordam que, após a divulgação da IN nº 01/2019 pela Secretaria de Governo Digital do Ministério da Economia (BRASIL, 2019), a qual fomenta o uso de nuvem por todas as instituições da Administração Pública e foi citada no referencial teórico, os normativos estão evoluindo gradativamente para que o governo tenha mais abertura para se desenvolver tecnologicamente.

As estratégias de gerenciamento de riscos que estavam sendo implementadas pelas organizações em que os entrevistados atuavam abrangem a contratação de serviços de consultoria para avaliar a conformidade das instituições perante a lei geral de proteção de dados e demais; a análise de riscos de acordo com o acórdão do TCU nº 1.739/2015 para a implantação de quaisquer soluções em nuvem (BRASIL, 2015); e a promoção de treinamentos para os diferentes departamentos quanto às questões de conformidade com a legislação.

4.1.3 Conformidade e auditoria

Tratando-se dos temas relacionados à conformidade e auditoria, 70% dos entrevistados acreditam que a utilização de soluções em nuvem é mais adequada quando se refere às práticas de conformidade, pois os provedores disponibilizam maiores recursos de rastreabilidade e verificação de conformidade e complementam que o risco é menos significante ao se utilizar a nuvem no caso de ser necessário atender a alguma demanda de *e-discovery* ou auditoria.

Os demais 30% dos entrevistados demonstraram receio com questões relativas à efetividade das funcionalidades ofertadas pelo provedor no caso de se avaliar a conformidade das instituições com a Lei Geral de Proteção de Dados (LGPD) ou demais regulamentações referentes ao uso de nuvem.

Todos os respondentes concluíram que não havia um processo de verificação de conformidade com maturidade suficiente em suas instituições na maioria dos casos, pois o ambiente ainda estava em fase de testes com um número limitado de usuários, à época em que as entrevistas foram realizadas.

Apesar de estar em momento de adaptação, na ótica dos entrevistados estavam sendo implementadas estratégias para que fossem desenvolvidos processos mais estruturados. Entre as ações que estão sendo executadas, destacam-se as exigências contratuais das instituições para que o provedor de nuvem forneça as funcionalidades necessárias, além da implementação de soluções de classificação automática de arquivos por meio da identificação de palavras-chave.

4.1.4 Continuidade dos negócios

Sobre os riscos relacionadas à continuidade dos negócios, os entrevistados evidenciaram, entre outros, a finalização do contrato com o provedor. Tal fato pode ocorrer após uma série de fatores inerentes à gestão no setor público, incluindo possíveis cortes de orçamento em períodos de renovação contratual. Em casos mais críticos, pode ser necessário optar pela portabilidade dos serviços para outro provedor, sendo, nesse caso, considerados riscos de dependência do provedor de serviços de nuvem, conhecido também como *Lock-in* ou Aprisionamento.

Dos entrevistados, 30% apontam que, em casos de falhas de conexão, indisponibilidade dos sistemas, degradação de desempenho, perda de dados e limitação de orçamento contratual para prover escalabilidade da capacidade computacional são riscos relevantes com potencial para causar a interrupção de suas atividades.

Entre os entrevistados, metade declarou que as organizações em que atuam já possuíam planos de contingência em execução, abrangendo: a formação de comitês de segurança e arquitetura com o objetivo de construir e executar procedimentos que assegurem a continuidade dos negócios em caso de incidentes; adoção de modelo de contratação de múltiplos provedores de nuvem para possibilitar a portabilidade quando necessário; provisionamento de canais secundários de conectividade com a internet e planos de contingência já estruturados no caso da interrupção de serviços essenciais para as entidades governamentais.

A outra metade dos entrevistados declarou que as organizações em que atuam ainda não possuíam planos de contingência estruturados, majoritariamente em consequência de ainda estarem desenvolvendo a sua maturidade com a utilização de serviços em nuvem, ou por ainda estarem em processo de aquisição. Porém, esses entrevistados declararam que os órgãos públicos em que atuavam estavam efetuando: testes por meio da implantação de pilotos de sistemas; análises de riscos; classificação de sistemas críticos que necessitam de maior prioridade quanto à sua disponibilidade; e elaboração de cláusulas contratuais específicas que prevejam essas situações de maneira a contorná-las se necessário, exigindo que os provedores estejam aptos a suprir as necessidades personalizadas de cada órgão.

4.1.5 Segurança

A respeito dos riscos relacionados à segurança, os participantes da pesquisa apontaram maior relevância quanto à possibilidade de vazamento de informações decorrente de acessos por invasores. 40% dos entrevistados reconhecem que, além dos controles e certificações de segurança fornecidos pelo provedor, também precisa ser considerada a segurança dos sistemas gerenciados pela entidade pública para garantir que eles não tenham vulnerabilidades.

Há uma preocupação quanto a situações em que os códigos dos sistemas elaborados pela instituição, mesmo quando hospedados em nuvem, não sejam suficientemente seguros, considerando também que o uso de software de fontes públicas (imagens de sistemas operacionais, trilhas de desenvolvimento, entre outras aplicações) pode conter *malware* e necessitam de uma maior atenção e controle.

Dos entrevistados, 60% afirmaram que ainda as organizações em que atuam estão desenvolvendo táticas para reforçar a segurança de seus ambientes em nuvem, visto que no momento estão em fase de testes ou no processo de aquisição. Nesses casos, os entrevistados evidenciaram que atualmente essas organizações estão efetuando análises de riscos com o objetivo de solicitar medidas de contorno aos fornecedores no momento da contratação, construindo exigências específicas por meio de cláusulas contratuais.

4.1.6 Isolamento

Quando a abordagem se tratou dos riscos relacionados ao isolamento dos ambientes hospedados em infraestrutura de nuvem pública, os entrevistados elencaram riscos relacionados ao isolamento lógico dos ambientes virtuais e o possível acesso por outros clientes do provedor que estejam compartilhando o uso do mesmo hardware, como também ao acesso não permitido de funcionários do provedor aos ambientes das instituições.

Apesar de tais afirmações, metade dos entrevistados afirmaram não possuir preocupações quanto ao isolamento de ambientes das organizações em que atuam, acreditando que os provedores de nuvem oferecem maior garantia de isolamento dos recursos por conta da natureza de sua estrutura compartilhada, envolvendo tecnologias e procedimentos que talvez não sejam implementados de maneira igualmente eficiente em servidores das referidas organizações.

Quanto às estratégias para mitigar os riscos, os entrevistados afirmaram que as organizações em que atuavam praticava determinadas medidas para evitá-los, incluindo: a segmentação de acessos para funcionalidades de administração dos recursos; o isolamento de ambientes de desenvolvimento, homologação e produção; e a construção de exigências em cláusulas contratuais para garantir que esse fator de segurança seja gerenciado pelo provedor.

4.1.7 Gestão de identidades e acessos

Ao serem abordados a respeito dos riscos inerentes à gestão de identidade e acessos, os entrevistados elencaram preocupações quanto à baixa maturidade das políticas de gestão nas organizações em que atuam. Como parte das estratégias para a remediação dos riscos relacionados ao tema, todos os entrevistados afirmaram que as organizações em que atuavam estavam planejando ou estiveram em processo de implementação de soluções como: múltiplo fator de autenticação, segmentação de privilégios, acesso condicional, biometria, dupla validação de alterações nas configurações do ambiente e liberação momentânea de privilégios.

Foi apontado por 30% dos entrevistados que ainda não foram implementadas soluções mais robustas de gestão de acessos nas organizações em que atuavam, porém estiveram executando um plano de controle de acessos e identidade, o qual estaria previsto para ser tratado em futuras contratações, considerando os riscos inerentes ao tema.

4.1.8 Proteção de dados

Tratando-se das questões relativas à proteção de dados, o risco de vazamento de informações sensíveis é o ponto de maior relevância, citado por todos os entrevistados enquanto evidenciavam as regras estabelecidas pela LGPD (BRASIL, 2018e) e pela Portaria GSI nº 9/2018 (BRASIL 2018d), afirmando que, por se tratarem de organizações governamentais, um vazamento de informações poderia acarretar em significativos problemas econômicos e políticos com impacto de nível nacional. Além do referido vazamento, também são considerados possíveis perdas de dados e o tratamento de tais dados por terceiros de maneira não autorizada conforme a legislação vigente.

Considerando a ótica dos entrevistados desta pesquisa, todas as instituições ainda encontravam-se desenvolvendo processos e práticas para garantir a proteção dos dados, conforme a legislação. Entre as táticas citadas, 20% dos entrevistados afirmaram que as organizações estiveram buscando apoio jurídico-legal para que se mantenham em conformidade por meio de serviços de consultoria para verificar a maturidade delas quanto à aderência aos requisitos das leis que tangem à proteção de dados.

Em meio às demais estratégias das organizações públicas, citadas pelos entrevistados, estão: evitar o tráfego de informações não públicas em ambientes de nuvem; executar o tratamento de metadados, buscando evitar o vazamento de informação pessoal identificável; implementação de processos de classificação das informações, definindo permissões para serem tratadas em ambientes de nuvem; e iniciativas de comitês para a análise de riscos, de forma a coordenar futuras contratações dos serviços de nuvem.

4.1.9 Resposta a incidentes

No âmbito dos temas relacionados com a resposta a incidentes, os entrevistados pontuaram riscos que causassem a ineficiência de tais processos, levando em consideração a falta de maturidade quanto à estruturação desse tipo de resposta. Situações nas quais não existe um histórico ou indicadores de eficiência de casos em que incidentes foram tratados implicam na impossibilidade de se identificar problemas crônicos.

A respeito das estratégias das organizações públicas, os entrevistados, em todos os casos, comunicaram que não existem planos completamente estruturados quando se trata de tecnologias em nuvem. Porém, conforme evidenciado por metade dos entrevistados, estão sendo estabelecidas equipes dedicadas nas referidas organizações para dar tratamento de incidentes com planos de comunicação e alertas definidos.

Nos demais casos, quando do início do processo de renovação contratual, os entrevistados afirmaram que as organizações em que atuavam estiveram avaliando os riscos elencados pelo acórdão do TCU e classificados quanto à sua criticidade, buscando-se elencar tais questões no momento da renovação da contratação, de forma a fazer requisições para que os provedores de nuvem disponibilizem recursos que auxiliem no tratamento de incidentes.

4.2 Análise dos resultados quanto a maturidade quanto ao uso de nuvem

Cumprindo-se os objetivos a que este estudo se propôs, são analisados os dados coletados, explorando os aspectos mais relevantes relacionados à maturidade quanto ao uso de nuvem nas óticas dos entrevistados, além de suas percepções quanto aos riscos inerentes ao uso da computação em nuvem pelo governo e as maiores tendências de práticas de gestão de riscos. No Quadro 6, é apresentada uma consolidação das respostas de acordo com a experiência no uso de computação em nuvem, tipo e a utilização pelo público interno da organização.

Quadro 6 – Consolidação das respostas das entrevistas quanto à maturidade

Entrevistado	Utilização (anos)	Modelo de Serviços em Nuvem			Público Interno
		IaaS	PaaS	SaaS	
E01	01	Não	Não	Sim	Parcial
E02	02	Sim	Não	Sim	Integral
E03	05	Sim	Sim	Sim	Integral
E04	1,5	Não	Não	Sim	Integral
E05	3	Não	Não	Sim	Parcial
E06	6	Não	Não	Sim	Integral
E07	3	Não	Sim	Sim	Integral
E08	0,5	Não	Não	Não	Não
E09	1,5	Sim	Sim	Sim	Parcial
E10	0,7	Não	Não	Sim	Parcial
Comentário	80% com uso até 3 anos	30% Sim 70% Não	30% Sim 70% Não	90% Sim 10% Não	50% Integral, 40% Parcial e 10% Não

Fonte: Elaborado pelos autores a partir de dados da pesquisa.

Ao analisar as óticas dos entrevistados quanto à maturidade de uso de nuvem, verifica-se no Quadro 6 que é possível apontar que 80% das instituições que estão utilizando essa tecnologia por 3 anos ou menos e que ainda estariam desenvolvendo a sua experiência com a gestão desses ambientes. Complementado a questão, os entrevistados relataram que as instituições ainda enfrentariam dificuldades quanto à disponibilidade de mão de obra especializada para exercer as atividades de gestão dos ambientes de nuvem, sendo um dos fatores característicos da fase de transformação digital em que o governo se encontra.

De acordo com o Quadro 6 e dentro da perspectiva dos 40% dos órgãos que já possuem uma maturidade avançada nesse aspecto, os entrevistados relataram que estes estão hospedando diversos sistemas e utilizando ostensivamente as funcionalidades oferecidas pela nuvem na modalidade de *software* como um serviço (*Software as a Service* - SaaS), de forma a tornar a gestão de TI mais eficiente quando se trata de custos e performance. Também foi apontado que os usuários dessas instituições estão familiarizados com as plataformas, fazendo uso delas em seu dia a dia, como nos casos em que há a possiblidade do uso dessas plataformas para fins de teletrabalho.

Em complemento, verifica-se que os 60% dos órgãos públicos com adoção mais recente geralmente ainda se encontram executando testes e planejando as formas de alavancar a adoção dessas plataformas pelos seus usuários, majoritariamente com uma abordagem de lançamento limitado a certos departamentos como forma de piloto. Tratando-se de hospedagem de sistemas na nuvem, é predominante nessas instituições o receio quanto ao fato de suas equipes ainda não possuírem conhecimentos técnicos avançados e ainda se encontrarem testando tais serviços.

Considerando os depoimentos dos entrevistados, pode-se concluir que estes acreditam nos benefícios, na segurança e no valor agregado do uso de nuvem, porém, entre os maiores desafios à implementação, está a mudança da cultura das organizações para adotar todas as soluções em nuvem que, a princípio, poucos possuem conhecimentos aprofundados.

4.3. Análise no que tange à ótica a respeito dos riscos da nuvem e sua gestão

Analisando os resultados da pesquisa, nota-se que os entrevistados majoritariamente acreditam nas vantagens dos aspectos de segurança oferecidos pelos ambientes de nuvem para as organizações em que atuavam, como a maior eficiência quando comparados aos riscos de se gerenciar uma infraestrutura local, também com relação à disponibilidade, integridade e a confidencialidade dos dados. Porém, apesar de reconhecer a superioridade da computação em nuvem, ainda existem preocupações que exercem relevância

nas considerações e planejamentos em torno da contratação de serviços de nuvem e da migração dos dados e sistemas governamentais para esses serviços terceirizados.

Entre as maiores tendências levantadas pelos entrevistados, destacam-se as preocupações quanto às imposições que a legislação atual define acerca dos ambientes em questão, incluindo contextos em volta do tratamento de dados sensíveis e às imposições quanto à residência de dados em território nacional.

São enfatizadas inclusive questões relativas às características intrínsecas do modelo de aquisição e contratação por instituições governamentais, considerando riscos atrelados a términos de contrato e aos cortes orçamentários que podem impedir uma escalabilidade ou renovação contratual, levando em consideração também os riscos quanto à portabilidade dos ambientes de um provedor para outro, no caso de uma mudança decorrente de tais casos.

Após avaliar os posicionamentos dos entrevistados a respeito das organizações governamentais em que atuavam, é possível atestar que eles, em sua maioria, indicaram que as organizações estavam em fase de planejamento e estruturação dos seus processos voltados para mitigar os riscos levantados na presente pesquisa. As que se encontravam no momento de avaliação eram compostas por órgãos que utilizavam a tecnologia em nuvem por um menor volume de tempo e que, inclusive, ainda estavam testando tais soluções, não chegando ao ponto de efetivamente implementar estratégias robustas de gestão de riscos na ocasião da coleta dos dados.

Apesar da baixa maturidade dessas instituições quanto ao uso de nuvem baseada na ótica dos entrevistados, existem iniciativas em todas as organizações para elaborar planos estruturados que tratam da gestão dos riscos, abordando principalmente questões em torno da contratação desses serviços. Para tais demandas, foi informado pela maioria dos entrevistados que as organizações em que atuavam estavam instituindo comitês para executar a avaliação de riscos e os planejamentos de segurança, resposta a incidentes e demais atividades relacionadas.

Nesse sentido, eles esperaram que, com os resultados dos estudos e definições trazidas pelos comitês de análise de riscos, seria elaborado pelas organizações em que atuavam cláusulas contratuais que exigiriam dos provedores a prestação de funcionalidades quanto aos temas em pauta, como exemplo, a gestão de acessos, isolamento de recursos críticos e portabilidade para outros provedores. Também foi apontada a tendência de se adotar modelos de aquisição de dois ou mais provedores de serviços de nuvem em que há possibilidade de o órgão migrar os seus serviços entre os provedores de acordo com a sua necessidade em um eventual incidente.

Com relação aos riscos no contexto das imposições regulatórias e legislativas, os entrevistados afirmam que os órgãos em que atuavam buscou apoio jurídico-legal por meio de consultorias, para garantir a sua conformidade com a legislação e exigir recursos específicos dos provedores no momento das contratações e renovações.

A partir de tais posicionamentos, embora estejam em fase inicial de sua transformação digital, na ótica dos entrevistados, as instituições que participaram desta pesquisa possuem planos promissores de se modernizar de maneira eficaz, levando em conta os aspectos relacionados aos riscos e à sua gestão eficiente.

5 CONCLUSÃO

Este trabalho teve como objetivo avaliar os riscos ao se implantar serviços de Computação em Nuvem na ótica dos gestores de órgãos públicos federais no Brasil. Para alcançar o objetivo proposto, foram realizadas entrevistas semiestruturadas com servidores de nível tático, envolvidos com a gestão de tecnologia da informação de dez órgãos da Administração Pública Federal. O estudo explorou questões relativas a um tema atual e em ascensão no campo de administração de empresas no âmbito de Tecnologia da Informação: a computação em nuvem e a gestão de riscos relacionados ao seu uso.

Com base nos resultados da pesquisa, foi possível colher impressões dos respondentes sobre a situação das organizações que participaram do estudo, trazendo questões sobre a permeabilidade da computação em nuvem na Administração Pública Federal, sobre a maturidade no uso de tais soluções e a identificação de tendências de gestão de riscos praticadas por essas organizações.

Constatou-se que a adoção de computação em nuvem pode representar uma economia de recursos públicos, porém traz desafios principalmente quando gestores se deparam com questionamentos acerca dos riscos que estão atrelados ao seu uso, com atenção ao tratamento de dados sensíveis. Em adição, para adotar a computação em nuvem, na linha de ação proposta pela Estratégia de Transformação Digital, pode ser necessário enfrentar riscos de transposição complexa, os quais acabam por postergar a implementação dessa tecnologia pelas entidades governamentais.

Embora estejam, em geral, em uma fase inicial de sua transformação digital, na ótica dos entrevistados, as organizações em que atuavam revelavam planos de se modernizar, levando em conta os aspectos relacionados aos riscos e à sua gestão eficiente. Quanto aos riscos no contexto das imposições regulatórias e legislativas, os entrevistados afirmaram que os órgãos em que atuavam buscaram apoio jurídico-legal por meio de consultorias, para garantir a sua conformidade com a legislação e exigir recursos específicos dos provedores no momento das contratações e renovações.

Este estudo oferece uma visão acerca do posicionamento quanto à adoção da computação em nuvem em uma amostra de organizações no Governo Federal e coloca à disposição de interessados um rol de observações sobre a situação contemporânea no cenário de gestão de riscos a que órgãos públicos federais no Brasil estão sujeitos. Os resultados apresentados nesta pesquisa referem-se aos dados que foram coletados num determinado momento do tempo e a partir das entrevistas dos gestores atuantes nas referidas organizações.

Por fim, este estudo deixa uma abertura para a realização de pesquisas e trabalhos acadêmicos futuros sobre o tema, com vistas a validar os resultados posteriores de mudanças nas organizações públicas estudadas ou em futuros estudos que tratem sobre a maturidade das organizações públicas no Brasil nas diversas esferas (federal, estadual e municipal) quanto ao uso de serviços de nuvem, considerando ainda os impactos pós pandemia da COVID-19. É possível, ainda, elaborar mecanismos para avaliação de risco de produtos e serviços em nuvem ofertados no país por provedores.

AGRADECIMENTOS

Os autores agradecem o apoio das Agências brasileiras de pesquisa, desenvolvimento e inovação CNPq (Projeto INCT SegCiber 465741/2014-2, PQ-2 312180/2019-5 e LargEWiN BRICS2017-591), CAPES (Projetos FORTE 23038.007604/2014-69 e PROBRAL 88887.144009/2017-00) e FAP-DF (Projetos UIoT 0193.001366/2016 e SSDDC 0193. 001365/2016), bem como o suporte do Laboratório LATITUDE/UnB (Projeto SDN 23106. 099441/2016-43) e projetos de cooperação com o Conselho Administrativo de Defesa Econômica (grant CADE 08700.000047/2019-14).

REFERÊNCIAS

ALI, Omar *et al*. Assessing information security risks in the cloud: A case study of Australian local government authorities. **Government Information Quarterly**, [*s. l.*], v. 37, n. 1, p. 101419, 2020. Disponível em: https://doi.org/10.1016/j.giq.2019.101419. Acesso em: 28 out. 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27017 - 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, BR: [*s. n.*], 2016.

BRASIL. Banco Central do Brasil. **Circular nº 3.909, de 16 de agosto de 2018.** Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil. Brasília: Banco Central do Brasil, 2018a. Disponível em: https: //www.bcb. gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=3909. Acesso em: 20 maio 2020.

BRASIL. Conselho Monetário Nacional. **Resolução nº 4.658, de 26 de abril de 2018.** Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Brasília: Conselho Monetário Nacional, 2018b. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%25C3%25 A7%25C3%25A3o&numero=4658. Acesso em: 20 maio 2020.

BRASIL. Ministério da Ciência Tecnologia Inovações e Comunicações. **Estratégia Brasileira de Transformação Digital: E-digital**. Brasília: Ministério da Ciência Tecnologia Inovações e Comunicações, 2018c. Disponível em: http://www.mctic.gov.br/mctic/export/sites/institucional/estrategiadigital.pdf. Acesso em: 20 maio 2020.

BRASIL. Ministério da Economia. **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. Brasília: Ministério da Economia, 2019. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/70267659/do1-2019-04-05-instrucao-normativa-n-1-de-4-de-abril-de-2019-70267535. Acesso em: 20 maio 2020.

BRASIL. Presidência da República. **Portaria GSI nº 9 de 15 de março de 2018**. Brasília: Presidência da República, 2018d. Disponível em: https://www.in.gov.br/inicio. Acesso em: 20 maio 2020.

BRASIL. Tribunal de Contas da união. **Acórdão nº 1.739/2015**. Brasília: Tribunal de Contas da União, 2015. Disponível em: http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20150720/AC_1739_24_15_P.doc. Acesso em: 20 maio 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados (LGPD). Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Brasília, DF: Presidência da República, 2018e. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 maio 2020.

BURLESON, Brant R.; LEVINE, Barbara J.; SAMTER, Wendy. Decision-Making Procedure and Decision Quality. **Human Communication Research**, Oxford, v. 10, n. 4, p. 557–574, 1984.

CAMERON, David; KNEALE, Pauline; SEE, Linda. An evaluation of a traditional and a neural net modelling approach to flood forecasting for an upland catchment. **Hydrological Processes**, Londres, v. 16, n. 5, p. 1033–1046, 2002.

CATTEDDU, Daniele; HOGBEN, Giles. **Cloud Computing Security Risk Assessment**. Heraklion: ENISA, 2009.

CLOUD SECURITY ALLIANCE. **CSA Security Guidance** v. 4., p. 152, 2017. Disponível em: https://cloudsecurityalliance.org/download/security-. Acesso em: 17 abr. 2020.

JANSEN, Wayne; GRANCE, Timothy. **Guidelines on security and privacy in public cloud computing**. Gaithersburg, MD: [*s. n.*], 2011. Disponível em: https://doi.org/10.6028/NIST.SP.800-144. Acesso em: 15 abr. 2020.

JONES, Steve *et al.* Risks and rewards of cloud computing in the UK public sector: A reflection on three Organisational case studies. **Information Systems Frontiers**, [*s. l.*], v. 21, n. 2, p. 359–382, 2019. Disponível em: https://doi.org/10.1007/s10796-017-9756-0. Acesso em: 22 out. 2020.

KITCHIN, Rob; TATE, Nick; NICHOLAS, J. Tate. **Conducting Research in Human Geography: Theory, Methodology and Practice**. 1. ed. Ann Arbor: Prentice Hall, 2000.

LONGHURST, Robyn. Semi-structured interviews and focus groups. **Key methods in geography**, Londres,

UK, p. 103, 2010.

MARSTON, Sean *et al.* Cloud computing - The business perspective. **Decision Support Systems**, Miami, US, v. 51, n. 1, p. 176–189, 2011. Disponível em: https://doi.org/10.1016/j.dss.2010.12.006

MELL, P M; GRANCE, T. **The NIST definition of cloud computingLecture Notes in Electrical Engineering**. Gaithersburg, MD: [*s. n.*], 2011. Disponível em: https://doi.org/10.6028/NIST.SP.800-145. Acesso em: 15 abr. 2020.

MILES, Matthew B; HUBERMAN, A Michael. **Qualitative data analysis:** An expanded sourcebook. Londres: SAGE, 1994.

TANG, Wenzhe *et al.* Incentives in the Chinese Construction Industry. **Journal of Construction Engineering and Management**, Beijing, CH, v. 134, n. 7, p. 457-467, 2008. Disponível em: https://doi.org/10.1061/(ASCE)0733-9364(2008)134:7(457). Acesso em: 10 abr. 2020.

TAURION, Cezar. **Cloud Computing: computação em nuvem: t**ransformando o mundo da tecnologia da informação. Rio de Janeiro: Brasport, 2009. E-book.

VALENTINE, Gill. Tell me about... Using interviews as a research methodology apud Flowerdew, R. and Martin, D.(eds.). **Methods in human geography:** A guide for students doing a research project, Harlow, v. 2, p. 110-127, 2005. Disponível em: https://ucl.rl.talis.com/items/8DCA1D60-D21E-0B81-1790-4E27EC52DDCA.html. Acesso em: 10 abr. 2020.

VERAS, Manoel. **Cloud Computing - Nova Arquitetura da TI**. Rio de Janeiro: Brasport, 2012.