Universidade de Brasília
Faculdade de Administração, Contabilidade, Economia e Gestão de Políticas Públicas
Departamento de Administração

ANDRIO DE ANDRADE ALVES

A GESTÃO DE RISCOS NO USO DA COMPUTAÇÃO EM NUVEM POR ÓRGÃOS DO GOVERNO FEDERAL

Brasília – DF
2019

ANDRIO DE ANDRADE ALVES

A GESTÃO DE RISCOS NO USO DA COMPUTAÇÃO EM NUVEM POR ÓRGÃOS DO GOVERNO FEDERAL

Monografia apresentada ao Departamento de Administração como requisito parcial à obtenção do título de Bacharel em Administração.

Professor Orientador:

Dr., Rafael Rabelo Nunes

Brasília – DF

2019

A GESTÃO DE RISCOS NO USO DA COMPUTAÇÃO EM NUVEM POR ÓRGÃOS DO GOVERNO FEDERAL

A Comissão Examinadora, abaixo identificada, aprova o Trabalho de Conclusão do Curso de Administração da Universidade de Brasília do aluno

Andrio de Andrade Alves

Dr., Rafael Rabelo Nunes
Professor-Orientador

Dr., Carlos André de Melo Alves
Professor-Examinador

Dr., Robson de Oliveira Albuquerque
Professor-Examinador

Brasília, 30 de abril de 2019

AGRADECIMENTOS

Meu sincero agradecimento ao Prof. Dr. Rafael Rabelo Nunes, orientador deste trabalho, pela oportuna sugestão do tema e pelas intervenções sempre precisas e didáticas ao longo do período em que este estudo se desenvolveu. Agradeço também aos meus incríveis amigos do trabalho e da faculdade, que me deram todo o apoio para possibilitar a execução deste estudo.

“In today’s world of exponential change, organizations that get too comfortable with the status quo are at major risk of disruption. If you’re not experimenting and not asking questions about how your organization is navigating and plugging into disruption, forming new ecosystems, and tapping into open markets, then your organization is at risk.” - Andrew Vaz.

RESUMO

Este estudo tem como o objetivo geral avaliar o posicionamento das instituições do Governo Federal em relação ao uso de serviços de computação em Nuvem e às práticas de gestão de riscos sendo executadas acerca da implantação desses serviços. Para atender a este objetivo e aos demais objetivos secundários definidos, o estudo foi conduzido nas seguintes fases: (1) revisão da literatura relativa à riscos, gestão de riscos e computação em nuvem, (2) escolha, estruturação do método de pesquisa e aplicação do referido método, (3) análise dos resultados e (4) elaboração das conclusões. A revisão da literatura compreendeu um levantamento bibliográfico sobre computação em nuvem, com ênfase na sua definição, benefícios e riscos inerentes ao seu uso, como também recomendações para a gestão de tais riscos. A escolha do método de pesquisa abrangeu a execução de entrevistas semiestruturadas com 10 instituições do Governo Federal, junto a servidores do nível tático. A análise dos resultados obtidos nas entrevistas evidenciou as práticas de gestão de riscos das instituições do Governo Federal entrevistadas quanto ao uso de nuvem. Por fim, as conclusões contemplam a visão geral dos temas abordados na pesquisa e recomendações para estudos futuros. Como contribuição, este estudo oferece uma visão acerca do posicionamento das instituições governamentais quanto ao uso de computação em nuvem e coloca à disposição daqueles que efetivamente por ela se interessam, por vontade própria ou dever de ofício, um rol de observações quanto ao cenário atual da evolução do uso dessa tecnologia nos órgãos federais.

Palavras-chave:

Gestão de riscos, Computação em nuvem, Governo, Entrevistas Semiestruturadas

SUMÁRIO

1. INTRODUÇÃO

No contexto da administração de empresas, especificamente na gestão de sistemas de informação, é pertinente o estudo das formas adotadas pelas organizações para viabilizar o processamento e o armazenamento de dados e de informações sob sua responsabilidade.

Na busca por serviços de Tecnologia da Informação, com melhores características de custo-benefício, grande parte das instituições e organizações atualmente podem optar por mesclar serviços de provimento próprio com os adquiridos de terceiros.

Este desenvolvimento e diversificação acabaram por proporcionar o nascimento de serviços contratáveis sob demanda e com a característica de permitir a opção por adquirir pacotes que englobam recursos de software, hardware e de comunicação de dados, que caracterizam a tecnologia conhecida como computação em nuvem, do inglês, *Cloud Computing*.

Atualmente, infraestruturas computacionais operadas isoladamente por organizações estão sendo substituídos por serviços providos via Internet, por instalações centralizadas de processamento de dados, gerenciadas pelos provedores de serviços em nuvem (GARTNER, 2018; DELOITTE, 2018; EUROSTAT, 2018). Visualizando as vantagens econômicas deste modelo de serviço, as instituições estão reavaliando o modo pelo qual se dispõem a adquirir e a utilizar recursos de tecnologia, em que em vez de alocar volumes expressivos de recursos para adquirir computadores e programas, elas estão considerando conectar a este novo ambiente.

A disponibilidade de tais recursos causou grandes mudanças em indústrias e governos nos últimos anos, e tal tendência está, inclusive, em pauta contemporaneamente no âmbito da administração pública federal brasileira. Com as mudanças ocorrendo no governo brasileiro nos últimos anos, ressalta-se um ponto de alta relevância que se trata do uso de Tecnologia da Informação para impulsionar a transformação digital da máquina pública.

Porém, apesar de oferecer grandes benefícios a adoção da computação em nuvem pelo governo federal abrange uma série de riscos e desafios para a sua implementação. Entre eles, está a complexa mudança da cultura das organizações e da legislação brasileira quanto ao tratamento de informações sensíveis.

Considerando este contexto de mudança de paradigma no campo de administração de sistemas de informação, este estudo visa trazer questões relevantes quanto ao posicionamento do Governo Federal do Brasil em relação à adoção da computação em nuvem, como também a sua abordagem quanto à gestão dos riscos inerentes à esta adoção.

1.1. Objetivo Geral

O objetivo geral desta pesquisa é avaliar o posicionamento das instituições do Governo Federal em relação ao uso de serviços de computação em Nuvem e às práticas de gestão de riscos sendo executadas acerca desses serviços.

1.2. Objetivos Específicos

a) Evidenciar os conceitos e princípios de riscos e suas práticas de gestão;

b) Evidenciar o conceito de computação em Nuvem, identificando os seus benefícios, riscos potenciais e recomendações para gestão destes riscos;

c) Com base no conteúdo levantado nos objetivos “a” e “b” identificar e avaliar os posicionamentos dos entrevistados com relação à adoção da computação em Nuvem em cada instituição do Governo Federal;

d) Verificar a maturidade das instituições quanto à adoção da computação em nuvem, na ótica dos entrevistados;

e) Identificar as tendências de gestão de riscos em nuvem e práticas relacionadas nas instituições do Governo Federal relativas à computação em nuvem, como também os pontos que podem ser endereçados em seu planejamento para o futuro;

2. REFERENCIAL TEÓRICO

2.1. Riscos

O risco faz parte da vida de todos. Como sociedade, é necessário correr riscos para crescer e se desenvolver. Da energia à infraestrutura, das cadeias de suprimento à segurança

nos aeroportos, dos hospitais à segurança da informação: os riscos geridos de forma eficaz ajudam as sociedades a alcançar mais e melhores resultados. Na realidade atual, à medida que surgem novas tecnologias, os riscos relacionados a elas também evoluem rapidamente (GREGORIO, 2015, p. 212)

No caso de uma organização, os riscos são altamente relevantes quando se consideram o sucesso de um planejamento estratégico. De forma a buscar o atingimento dos objetivos de uma companhia, é preciso garantir que o gerenciamento de riscos seja o mais eficaz possível, de forma a minimizar os riscos que representam ameaças, e da mesma forma maximizar o potencial dos que representam oportunidades (BERG, 2010, p. 79).

A medida que a demanda por inovações tecnológicas aumenta, entender quais são os seus riscos, como mensurá-los e classificar suas consequências se tornou uma das demandas mais urgentes para instituições que pretendem usar a gestão de risco na tomada de decisão (CIENFUEGOS, 2013) e, a partir de tais estudos e percepções, conduzir questões estratégicas, buscando aumentar a eficiência da organização ao implementar novas tecnologias.

a) O Conceito de Risco

O conceito de risco é amplamente definido em termos de incerteza, probabilidade, eventos e consequências. As definições de risco foram desenvolvidas consideravelmente desde que a gestão de riscos passou a ser considerada como uma ferramenta essencial para um gerenciamento efetivo em organizações.

Segundo Berg (2010), “risco refere-se à incerteza que envolve eventos e resultados futuros. É a expressão da probabilidade e impacto de um evento com o potencial de influenciar a realização dos objetivos de uma organização”.

A definição abrange diferentes aspectos do conceito de risco, não considerando apenas como consequências negativas, mas definindo o risco como um resultado neutro. Já Gregorio (2005, p.210) aponta que “o risco se torna uma oportunidade de lucrar com a incerteza”. Com essas evidências, pode-se dizer que conceito de risco atualmente possui uma abordagem ainda mais ampla.

Há uma distinção entre o conceito de risco e o conceito de incerteza. Enquanto “a incerteza seria imensurável, o risco seria mensurável” (CIENFUEGOS, 2013, p.23). O risco

pode ser medido com base em probabilidade e seus efeitos. Quão arriscado é o evento depende de quanto o resultado provavelmente difere dos objetivos da organização.

Na pesquisa de Gregorio (2005), definindo duas fontes de incerteza, a pesquisa explorou os riscos enfrentados pelas instituições, afirmando que o contexto da incerteza que cada empresa enfrenta é composto de dimensões endógenas e exógenas. Fontes endógenas são as que tem origem dentro das organizações, enquanto as exógenas surgem no ambiente externo, seja ele composto de variáveis ambientais, políticas, sociais, macroeconômicas, financeira etc.

2.2. A Gestão de Riscos

A gestão de risco tem sua história iniciada após a Segunda Guerra Mundial. O conceito concentrou-se significativamente em assuntos relacionados ao mercado financeiro. No entanto, o desenvolvimento da pesquisa em gestão de risco mostra que "vários aspectos contribuíram para mudar essa aplicação restrita da disciplina de gestão de risco" (CIENFUEGOS, 2013). De acordo com Cienfuegos (2013), a gestão de risco mudou para uma abordagem mais ampla de "uma função técnica restrita para um gerenciamento amplo e integrado de todos os riscos de uma organização".

O gerenciamento de riscos é considerado um elemento crucial no sucesso da organização, especialmente em um ambiente de negócios incerto e em rápida mudança. Os gerentes precisam entender as fontes de risco, sua natureza e como elas podem ser gerenciadas de maneira eficaz. Anderson e Terp (2006) definiram o gerenciamento de riscos como o processo de compreender e gerenciar efetivamente as incertezas internas e externas, eliminando, reduzindo e controlando os riscos puros, aumentando os benefícios e evitando os detrimentos das exposições especulativas. Os autores também se referem a vários objetivos da gestão de risco para a organização, incluindo a criação de transparência, aumentando a consciência de risco, minimizando a probabilidade de perdas futuras e maximizando a probabilidade de sucesso.

A Gestão de Riscos é entendida, também, como uma abordagem científica para o problema de lidar com riscos, considerando que segue uma aplicação geral de técnicas, procedimentos e processos estruturados em uma sequência de passos lógicos (CIENFUEGOS, 2013). O conceito enfatiza a definição e desenvolvimento do programa de Gerenciamento de Riscos, que permite que as organizações alcancem suas estratégias e objetivos.

Em geral, a gestão de risco no mundo moderno não se limita a identificar e controlar os impactos negativos das incertezas que ocorrem, mas também a potencializar as oportunidades. Também é importante aumentar a conscientização sobre os riscos dentro das organizações, envolvendo pessoas em todos os níveis, a fim de obter uma visão melhor sobre a probabilidade de riscos e seus impactos. O desenvolvimento de uma cultura de gerenciamento de riscos ajuda a implementar o gerenciamento de riscos de maneira eficaz, conforme instruído pelas normas da série ABNT NBR 31000.

O processo de gerenciamento de riscos refere-se a etapas lógicas que compõem esta prática, abrange pontos cruciais no desenvolvimento de um plano eficaz de gerenciamento de riscos. Tratando-se de obras acadêmicas sobre o assunto, certos autores fornecem diferentes abordagens para o processo de gerenciamento de risco. Anderson e Terp (2006) descrevem o processo de gerenciamento de riscos como uma "progressão de cinco etapas", fornecendo uma maneira simples e lógica de analisar o gerenciamento de riscos, o que está de acordo com seus objetivos:

1. Identificação de risco,
2. Avaliação de risco,
3. Controle de risco,
4. Financiamento de risco e
5. Monitoramento e relatório de risco.

Já COSO (2004) desenvolve o conceito de Gestão de Riscos Corporativos (*Enterprise Risk Management* - ERM), que consiste em oito componentes inter-relacionados. Ao integrar o gerenciamento de riscos e o gerenciamento corporativo, os componentes do ERM influenciam uns aos outros:

1. Ambiente interno,
2. Estabelecimento de objetivos,
3. Identificação de eventos,
4. Avaliação de risco,
5. Resposta ao risco,
6. Atividades de controle,
7. Informação e comunicação e
8. Monitoramento.

No Brasil, a série de normas ABNT NBR 31000, baseadas no padrão internacional ISO 31000, estabelecem a relação entre os princípios de gerenciamento de risco, estrutura e processos de gerenciamento de risco, definindo elementos para gerenciar riscos que podem ser aplicados em toda ou em parte de uma organização.

O processo de gerenciamento de riscos expande-se dos cinco principais passos tradicionais para oito etapas de sequência. Os elementos adicionais significativos do processo de gerenciamento de risco pela norma ABNT NBR 31000, em comparação com o processo tradicional, são “estabelecimento do contexto” e “comunicação e consulta”.

Figura 1 – Princípios e Estrutura da Gestão de Riscos - Adaptado de ABNT NBR 31000 (2018)

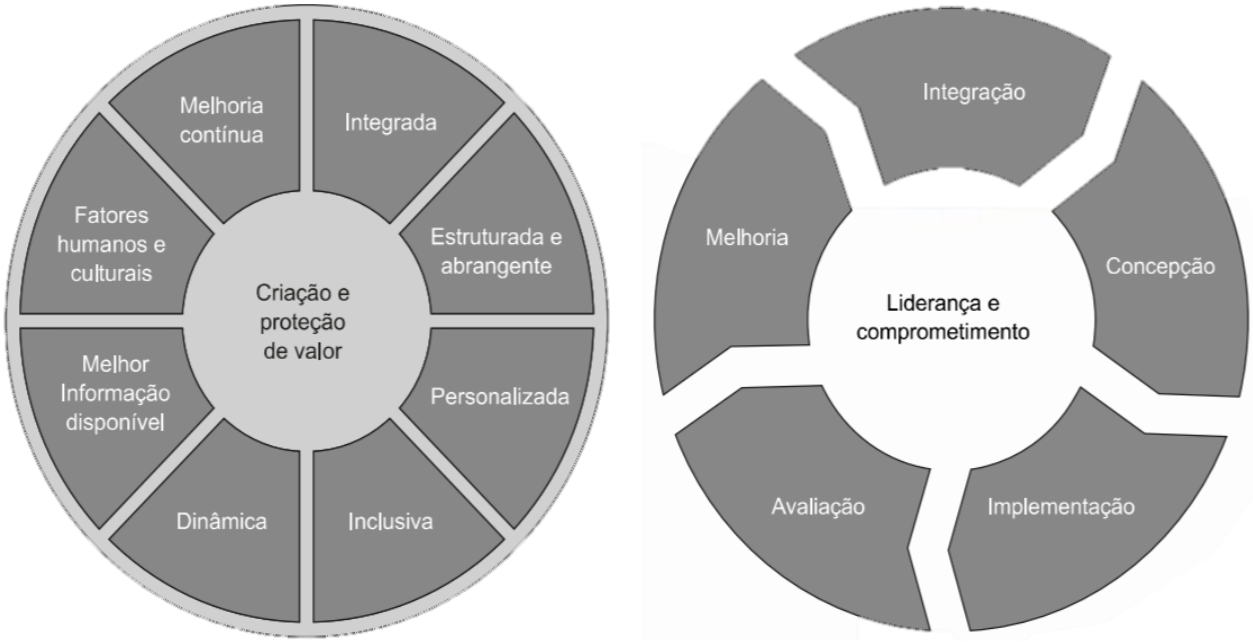
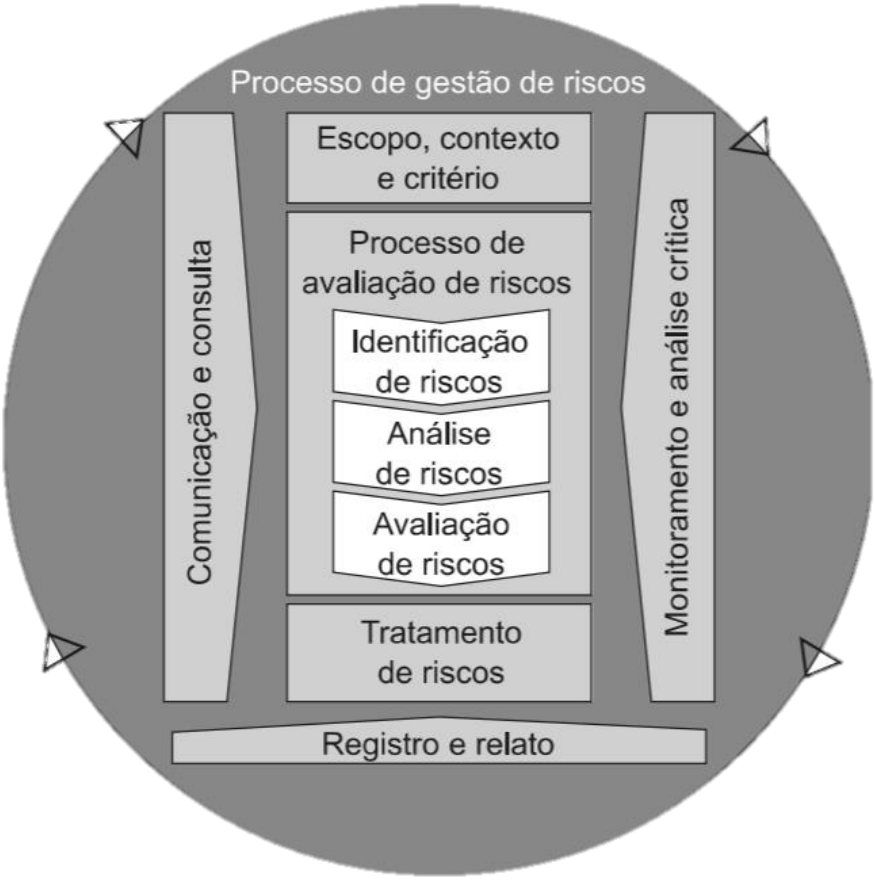


Figura 2 – Processo de Gestão de Riscos - Adaptado de ABNT NBR 31000 (2018)



- **Estabelecimento do contexto**

Como as características e necessidades da organização são diferentes, estabelecer o contexto é importante para buscar a abordagem apropriada para a organização. Esta etapa, descrita na figura 2, inclui as atividades para definir o ambiente interno e externo, buscando definir objetivos e escopo do processo de gerenciamento de riscos. Ao estabelecer o contexto, também é importante desenvolver critérios de risco. Segundo Berg (2010, p.83), “os critérios devem refletir o contexto definido, muitas vezes dependendo de políticas internas, metas e objetivos da organização e dos stakeholders”. Berg também sugere que os métodos para avaliar o ambiente organizacional incluam a metodologia SWOT (identificação dos pontos fortes, pontos fracos, oportunidades e ameaças) e estruturas PEST (influências políticas, econômicas, sociais e tecnológicas).

- **Avaliação de risco**

Esta etapa, citada na figura 2, existe para fornecer uma avaliação global para identificação, análise e avaliação de risco. Após cada etapa em que os riscos são identificados, analisados e avaliados, é crucial gerar uma revisão abrangente, que ajude os gestores a avaliar totalmente seu processo de gerenciamento de riscos. Esta etapa visa levar em consideração fatores críticos e apoiar o processo de tomada de decisão. Cada uma das etapas será detalhada a seguir.

a) Identificação de riscos

A identificação de riscos é uma das principais etapas do processo de gerenciamento de riscos. Ela concentra em revelar e identificar os riscos potenciais que podem ocorrer. Com base nas informações fornecidas no primeiro estágio "estabelecer o contexto", os gerentes são capazes de determinar os riscos que provavelmente afetarão os objetivos da organização, de um processo ou de um projeto. Nesta fase, os riscos são identificados e classificados em diferentes categorias, observando os fatores que os influenciam por meio de todos os aspectos. De acordo com Berg (2010, p.82), "ferramentas criativas suportam este processo de grupo", das quais podem ser citadas: *brainstorming*, entrevistas, método Delphi, *checklists*, dentre outras.

b) Análise de riscos

"A análise de risco envolve a identificação da fonte de risco, a consequência e a probabilidade de se estimar o risco inerente ou desprotegido sem controles em vigor" (BERG, 2010, p.84). Em outras palavras, é a etapa em que os gerentes usam técnicas diferentes para avaliar os impactos potenciais dos riscos e a probabilidade de eles ocorrerem. É necessário entender os riscos e suas consequências. Em atividades do dia-a-dia, a análise de risco pode ser considerada como um processo complexo quando os principais riscos podem exigir uma metodologia mais sofisticada.

c) Avaliação de risco

Conhecendo certos impactos e probabilidades de risco, os gestores podem decidir quais riscos requerem mais atenção do que outros. A etapa de avaliação de riscos ajuda a tomar decisões sobre riscos aceitáveis e inaceitáveis.

d) Tratamento de risco

Quando os riscos são inaceitáveis, o tratamento é necessário. O objetivo desta etapa mencionada na figura 2 não é eliminar riscos, mas minimizar os impactos negativos com opções econômicas. As opções oferecidas nesta fase incluem: evitar riscos, reduzir riscos, transferir riscos, diversificar soluções (GREGORIO, 2005, p.217).

e) Comunicação e consulta

É importante entender que o processo de gestão de riscos requer comunicação e consulta em todas as etapas para atingir seus objetivos. Os riscos precisam ser comunicados por meio de consultas internas e / ou externas para obter *insights* mais profundos sobre o processo de gerenciamento de riscos.

f) Monitoramento e revisão

É essencial ter os riscos monitorados e revisados periodicamente e formalmente, medindo os resultados do tratamento e assegurando que o ambiente em mudança não afete a avaliação de risco. Novos riscos também podem ser levados em consideração durante a revisão. Essa etapa é crucial para determinar um gerenciamento de risco bem-sucedido.

2.3. Riscos no Setor Público

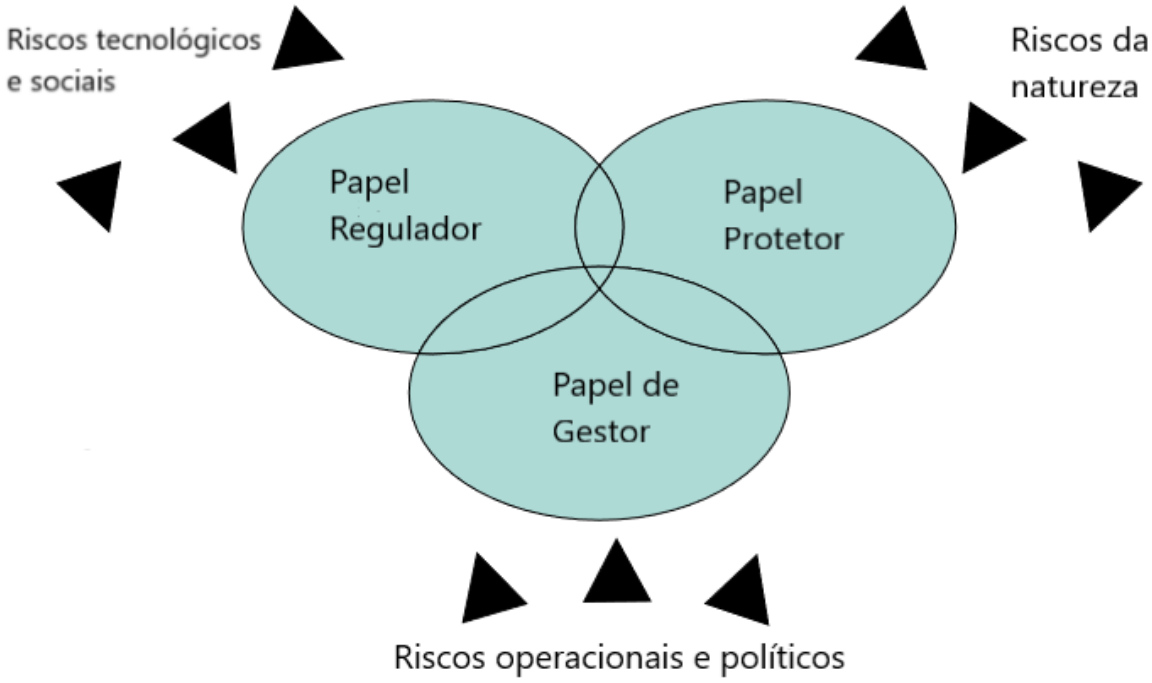
Segundo Barreto (2009, p.11), a Administração Pública possui diversas características próprias que tornam necessária a adoção de práticas de gestão diferenciadas, justificando inclusive a existência de um ramo específico de estudos de administração voltados ao setor público. A gestão de riscos faz parte integrante das operações de instituições públicas, lidando com a probabilidade de imprevistos que acarretam ineficiências, irregularidades financeiras e desperdício de recursos no setor público, buscando manter tais riscos sob controle (BARAFORT et al. 2017).

Como o processo de gestão de riscos é exigente e dispendioso, uma organização compromete significativos recursos na gestão de riscos, e o resultado de tais investimentos deve gerar valor para o setor público em vez de contribuir para o desperdício de recursos (ZINS; WEILL, 2017). Esse conceito é essencial no setor público porque, sem uma gestão adequada do risco, pode haver uma crise na realização de objetivos de longo prazo e até mesmo na confiança dos cidadãos nas instituições estatais (AGYEI-MENSAH; KWAME, 2016).

Segundo Knechel e Salterio (2016, p.13), “controles insatisfatórios levam a perdas, escândalos, fracassos e danos à reputação das organizações de qualquer setor. Onde os riscos são permitidos e novos empreendimentos são realizados sem um meio de controle de risco, é provável que haja problemas”.

Trazendo-se um posicionamento de outros países, a Unidade Estratégica do governo do Reino Unido (*Security Unit*), em seu artigo sobre a evolução da capacidade do governo de lidar com riscos e incerteza, é trazida uma visão sobre a certas responsabilidades dos governos e como elas podem ser afetadas por variados tipos de risco. Segundo a *Security Unit* (2002), Os governos têm três papéis: (1) papel regulador no fornecimento da estrutura legal onde as atividades de empresas e indivíduos geram riscos para outras pessoas; (2) papel de protetor, para proteger indivíduos, empresas e o meio ambiente contra os riscos que lhes são impostos de fora - por exemplo, grandes inundações ou outros desastres naturais, riscos à saúde ou segurança pública, ameaças externas à segurança ou riscos à estabilidade econômica; (3) papel de gestão em relação ao seu próprio negócio, incluindo a prestação de serviços públicos e o desempenho das funções reguladoras e de administração (figura 3).

Figura 3 – Funções Reguladoras - Adaptado de Risk: Improving government’s capability to handle risk and uncertainty (STRATEGY UNIT, 2002).



Já McPhee (2005), em estudo conduzido pelo Escritório Nacional de Auditoria da Austrália (ANAO), identifica três grandes grupos de riscos que afetam a Administração Pública: (1) riscos estratégicos, gerados a partir do planejamento mal estruturado, dadas as circunstâncias internas e externas à organização; (2) riscos ambientais, que cobrem os fatores macro ambientais, fatores competitivos e fatores de mercado; e (3) riscos operacionais, cobrindo riscos de processo e aqueles relacionados às entregas próprias do governo (MCPHEE, 2005).

Segundo Barreto (2009, p.11) "riscos que cercam os projetos governamentais derivam de uma multiplicidade de questões de complexidade altamente variável, sendo que tais questões nem sempre são de responsabilidade de uma única pessoa ou entidade". Em quase todos os casos, a gestão de riscos exige que os gestores públicos ponderem e avaliem entre os interesses conflitantes até identificarem uma solução ótima e aceitável, sendo que essas soluções quase sempre envolvem opções políticas e não técnicas (ÁVILA, 2013, p.7).

Tratando-se do governo brasileiro, em maio de 2016, a Controladoria-Geral da União (CGU) e o Ministério do Planejamento, Orçamento e Gestão publicaram a Instrução Normativa Conjunta MP/CGU nº 01, que dispõe sobre a sistematização de práticas relacionadas à governança, à gestão de riscos e aos controles internos no âmbito de órgãos e entidades do Poder Executivo Federal. Quanto à gestão de riscos, o normativo diz que os órgãos devem observar os seguintes princípios:

- Gestão de riscos de forma sistemática, estruturada e oportuna, subordinada ao interesse público;
- Estabelecimento de níveis de exposição a riscos adequados;
- Estabelecimento de procedimentos de controle interno proporcionais ao risco, observada a relação custo-benefício, e destinados a agregar valor à organização;
- Utilização do mapeamento de riscos para apoio à tomada de decisão e à elaboração do planejamento estratégico;
- Utilização da gestão de riscos para apoio à melhoria contínua dos processos organizacionais;

2.4. Gestão de riscos de TI e Segurança da Informação

- **Princípios Segurança da informação**

Segundo a Norma ABNT NBR ISO/IEC 27002 (2007), "a Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio".

Fontes (2010) indica que a partir dos objetivos do negócio é que se planejam os objetivos da segurança da informação, com o intuito de possibilitar a realização do negócio no que depende do uso dos recursos da informação.

Sobre o assunto, Whitman e Mattord (2012) definem que a segurança da informação se fundamenta em proteger a confidencialidade, integridade e disponibilidade dos ativos de informação, seja no armazenamento, processamento ou transmissão. É alcançada através da aplicação de políticas, educação, treinamento e conscientização e tecnologia (WHITMAN; MATTORD, 2012).

a) Integridade

Segundo Sommerville (2007) integridade é a garantia de que os programas e os dados dos sistemas não serão danificados, ou seja, diz respeito à garantia de que a informação realmente é o que deveria ser. Integridade significa garantir a existência dos dados, não corrompidos, encontrando-se íntegros, concluindo que aos dados originais nada foi acrescentado, retirado ou modificado.

Whitman e Mattord (2012) definem que a informação tem integridade quando é completa, inteira e incorrupta. A integridade da informação é ameaçada quando a informação é exposta a corrupção, danos, destruição ou outras perturbações do seu estado autêntico. Também indicam que a integridade é a base dos sistemas de TI, pois a informação não tem valor ou não é utilizada se os usuários não puderem verificar sua integridade.

b) Disponibilidade

A disponibilidade permite que usuários autorizados (pessoas ou sistemas de computador) acessar informações sem interferência ou obstrução e recebê-las no formato requerido (WHITMAN; MATTORD, 2012).

Segundo a Associação Brasileira de Normas Técnicas (2006), disponibilidade é propriedade que a informação apresenta, de estar disponível e utilizável numa eventual requisição de uma entidade autorizada. Beal (2008) define a disponibilidade como a garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna.

c) Confidencialidade

Confidencialidade é a propriedade que a informação apresenta, de estar disponível apenas para aqueles que estão autorizados a obtê-la (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2006). Segundo Whitman e Mattord (2012), a informação tem confidencialidade quando está protegida contra divulgação ou exposição a indivíduos ou sistemas não autorizados. A confidencialidade garante que apenas aqueles com os direitos e privilégios para acessar informações possam fazê-lo. Quando indivíduos ou sistemas não autorizados podem visualizar informações, a confidencialidade é violada. Para proteger a confidencialidade das informações, pode-se utilizar algumas medidas, incluindo as seguintes:

1. Classificação da informação
2. Armazenamento seguro de documentos
3. Aplicação de políticas gerais de segurança
4. Educação de guardiões da informação e usuários finais

A confidencialidade, como a maioria das características da informação, é interdependente com outras características e está mais intimamente relacionada à característica conhecida como privacidade (WHITMAN; MATTORD, 2012).

Para Caiçara (2007), confidencialidade consiste em assegurar que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por algum meio. Sua manutenção busca garantir que indivíduos não tenham acesso acidental ou intencional a informações quando não autorizados. O autor também afirma que confidencialidade significa proteger informações contra sua revelação para indivíduos não autorizados. No caso da rede, significa que os dados, enquanto transitam, não poderão ser vistos, alterados ou extraídos da rede por pessoas não autorizadas, bem como capturados por dispositivos ilícitos, de forma a garantir sigilo profissional, com acessos restritos e limitados a cada perfil de usuário, de acordo com a sua função no processo assistencial (CAIÇARA, 2007).

- **Gestão de Riscos em TI**

Com o advento da internet e a modernização dos sistemas de informação, configura-se um cenário de alta complexidade e custo de proteção dos ativos de informação em todas as esferas organizacionais. Portanto, buscando proteger a informação em seu ciclo de existência, é altamente importante para o alcance dos objetivos de segurança adotar um enfoque de gestão baseado nos riscos específicos de cada organização (BEAL, 2005).

Para Augusto Paes de Barros (CAPRINO; CABRAL, 2015), a gestão de risco é o objetivo principal da segurança da informação, pois são aplicadas medidas de segurança para evitar perdas, sejam elas relacionadas à confidencialidade, integridade ou disponibilidade. Como são eventos incertos, é preciso compreender a probabilidade e a dimensão de tais perdas. Em outras palavras, o risco.

Segundo a Associação Brasileira de Normas Técnicas (2013), por meio da norma NBR ISO/IEC 27001, a segurança da informação é obtida através da implementação de um conjunto aplicável de controles, selecionados através do processo de gerenciamento de riscos escolhido e gerenciados usando um Sistema de Gestão de Segurança da Informação, incluindo políticas, processos, procedimentos, estruturas organizacionais, software e hardware para proteger os ativos de informações identificados. Esses controles precisam ser especificados, implementados, monitorados, revisados e aprimorados, quando necessário, para garantir que a segurança da informação específica e os objetivos de negócios da organização sejam atendidos. Dessa forma, espera-se que os controles de segurança da informação relevantes sejam integrados de forma transparente aos processos de negócios de uma organização (ASSOCIACAO BRASILEIRA DE NORMAS TECNICAS, 2013).

Quando uma corporação adota a ABNT NBR ISO/IEC 27001 como referência, ela passa a seguir uma abordagem orientada a processos, permitindo uma maior eficácia na gestão da segurança. Esta abordagem concentra-se nos processos que impactam diretamente os resultados do negócio e não apenas em soluções tecnológicas que aumentam o nível de segurança. A corporação passa a avaliar e gerenciar os riscos inerentes a cada processo de negócio, incorporando a segurança naturalmente na gestão de seus processos (ZAPATER; SUZUKI, 2005).

Côrte (2014) apresenta três aspectos que devem estar envolvidos na estratégia de segurança: Pessoas, Processos e Tecnologias. Segundo o autor, cada uma dessas partes deve ser

analisada buscando uma forma de gerenciar os riscos atrelados a essas variáveis. Entrando em detalhes em cada uma das variáveis, o autor afirma que: (1) Pessoas representam o elo mais fraco da corrente da segurança, pois são passíveis de cometer falhas de segurança, com ou sem intenção; (2) Processos devem ser flexíveis até o ponto que não afetem a segurança das informações, a partir daí devem ser tratados de forma rígida e metódica; (3) Tecnologias deverão ser aplicadas onde puderem suportar a Política de Segurança das Informações, as Normas e os Processos definidos para cumprimento da estratégia de segurança, e para reforçar o elo mais fraco da corrente, as pessoas (Côrte, 2014).

Segundo a norma ABNT NBR 27000, antes de considerar o tratamento de um risco, uma organização deve definir critérios para determinar se os riscos podem ou não ser aceitos. Os riscos podem ser aceitos se, por exemplo, for avaliado que o risco é baixo ou que o custo do tratamento não é viável para a organização. Para cada um dos riscos identificados após a avaliação, uma decisão de tratamento precisa ser tomada, a qual pode incluir os seguintes exemplos:

a) Aplicar controles apropriados para reduzir os riscos;
b) Aceitar riscos de maneira consciente e objetiva, desde que satisfaçam claramente a política e os critérios da organização para aceitação de risco;
c) Evitar riscos por não permitir ações que possam causá-los;
d) Compartilhar os riscos associados a outras partes, por exemplo, seguradoras ou fornecedores.

Entendendo que os processos de gestão de riscos no âmbito da Tecnologia da Informação muitas vezes acarretam significativos investimentos de recursos financeiros e operacionais para organizações, torna-se interessante para as mesmas que a gestão de uma parcela dos ricos seja terceirizada. Neste caso, uma das soluções para tais questões é a adoção de serviços de computação em Nuvem, em inglês, *Cloud Computing.*

2.5. Computação em Nuvem

2.5.1. Fundamentos da Computação em Nuvem

Segundo o Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST), 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 (por exemplo, redes, servidores, armazenamento, aplicativos e serviços) que podem ser rapidamente provisionados e liberados com esforço mínimo de gerenciamento ou interação com o provedor de serviços (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2011).

Já a Associação Brasileira de Normas e Técnicas traduziu o conceito de computação em nuvem criado pela *International Organization for Standardization* (ISO) como "um paradigma para habilitar o acesso, via rede, a um grupo escalável e elástico de recursos, físicos ou virtuais, com auto provisionamento e administração sob demanda" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2015).

Sobre a inovação que a computação em Nuvem trouxe para o mercado, Weiss (2007, p. 16) afirma que:

> O conceito de Nuvem lida com muitas tecnologias e arquiteturas já existentes. A centralização de recursos de computação não é uma novidade, mas um retorno às raízes, assim como não são novidades a computação utilitária, a computação distribuída e o software como serviço. Mas a Nuvem inova, ao integrar todos esses modelos de computação. E esta integração requer a mudança do centro de poder, dos processadores para a rede – dentro da Nuvem, os processadores tornam-se commodities e é a rede que mantém uma Nuvem una e conecta nuvens umas às outras, bem como o céu ao chão (WEISS, 2007)

Smith (2009) resume o conceito evidenciando que, essencialmente, computação em Nuvem é uma forma de alugar computadores, espaço para armazenagem e capacidade de rede, com preços baseados em tempo de utilização, de alguma organização que já dispõe desses recursos em sua própria infraestrutura e pode disponibilizá-los via Internet.

O modelo de Nuvem é composto de cinco características essenciais, três modelos de serviço e quatro modelos de implantação (VERAS, 2012; MELL, GRACE, 2011).

a) Características

Veras (2012) e Mell e Grance (2011) definem cinco características como essenciais na *Cloud Computing*:

- Autoatendimento sob demanda: Um consumidor pode provisionar unilateralmente recursos de computação, como tempo de servidor e armazenamento em rede, conforme necessário, automaticamente, sem exigir interação humana com cada provedor de serviços.

- Amplo acesso a serviços de rede: Os recursos estão disponíveis na rede e são acessados por meio de mecanismos padrão que promovem o uso por plataformas (por exemplo, telefones celulares, tablets, laptops e estações de trabalho).

- Pool de recursos: os recursos de computação do provedor são agrupados para atender a vários consumidores usando um modelo de multi-locação, com diferentes recursos físicos e virtuais atribuídos e reatribuídos dinamicamente de acordo com a demanda do consumidor. Há um senso de independência de localização em que o cliente geralmente não tem controle ou conhecimento sobre a localização exata dos recursos fornecidos, mas pode ser capaz de especificar a localização em um nível mais alto de abstração (por exemplo, país, estado ou datacenter). Exemplos de recursos incluem armazenamento, processamento, memória e largura de banda de rede.

- Elasticidade rápida: Os recursos podem ser provisionados e liberados de forma elástica, em alguns casos automaticamente, para escalar rapidamente para fora e para dentro de acordo com a demanda. Para o consumidor, os recursos disponíveis para provisionamento muitas vezes parecem ilimitados e podem ser apropriados em qualquer quantidade e a qualquer momento.

- Serviços mensuráveis: Os sistemas em nuvem controlam e otimizam automaticamente o uso de recursos aproveitando 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). O uso de recursos pode ser monitorado, controlado e relatado, proporcionando transparência tanto para o provedor quanto para o consumidor do serviço utilizado (VERAS, 2012; MELL; GRACE, 2011).

b) Modelos de Serviço

Segundo Veras (2012) e Mell e Grace (2011) existem três principais modelos de serviço:

- Infraestrutura como um serviço (*Infrastructure as a Service - IaaS*): é a capacidade oferecida ao consumidor é fornecer processamento, armazenamento, redes e outros recursos

fundamentais de computação, nos quais pode-se implementar e executar softwares arbitrários, podendo incluir sistemas operacionais e aplicativos.

- 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.

- 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.

Em todos os modelos, o consumidor não gerencia ou controla a infraestrutura de Nuvem subjacente, incluindo rede, servidores, sistemas operacionais, armazenamento ou até mesmo recursos de aplicativos individuais. (VERAS, 2012; MELL; GRACE, 2011)

c) Métodos de Implantação

Os modelos de implantação representam como a computação em Nuvem pode ser estruturada, com base no compartilhamento e controle de recursos físicos e virtuais. Segundo a Associação Brasileira de Normas Técnicas (2015), Taurion (2009), Mell e Grance (2011) e Veras (2012), estes modelos podem ser divididos em:

- Nuvem privada: 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 da instituição.

- Nuvem da comunidade: 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). Ela pode ser de propriedade, gerenciado e operado por uma ou mais das organizações da comunidade, um terceiro ou uma combinação deles, e pode existir dentro ou fora das instalações.

- Nuvem pública: A infraestrutura de Nuvem é provisionada para uso aberto pelo público em geral. Ele pode ser de propriedade, gerenciado e operado por uma organização comercial,

acadêmica ou governamental ou por alguma combinação deles. 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, estouro de Nuvem para balanceamento de carga entre nuvens).

2.5.2. Benefícios e Riscos no uso da Nuvem

a) Benefícios e vantagens quanto ao uso de Nuvem

O uso da computação em nuvem garante certos benefícios às organizações que não são viáveis com a utilização de infraestrutura local, como por exemplo, acesso remoto à gestão de recursos computacionais, escalabilidade, agilidade, eficiência e segurança flexível (GRIFFITH, 2015). Também deve-se considerar que a computação em nuvem oferece a oportunidade para que as organizações reduzam os seus custos com a manutenção de infraestrutura local, podendo ser usada como serviço com despesas proporcionais à demanda, em vez de serem feitos investimentos significativos com a compra de *hardware* (MILLER, 2008).

Para Bandyopadhyay et al. (2009), as vantagens gerais no uso da computação em nuvem giram em torno dos seguintes benefícios-chave:

- **Redução de custos**: Redução drástica do custo de entrada para empresas que tentam se beneficiar de análises de dados com uso intensivo de computação, até então disponíveis apenas para grandes corporações. Esses exercícios computacionais normalmente envolvem grandes quantidades de recursos, e a computação em nuvem possibilita o provisionamento dinâmico dos mesmos. A computação em nuvem também representa uma enorme oportunidade para muitos países do terceiro mundo que foram deixados para trás na revolução da TI.

- **Redução de investimento inicial**: Fornecimento de acesso quase imediato aos recursos de hardware, sem grandes investimentos iniciais para os usuários, levando a um tempo de comercialização mais rápido em muitos negócios. Tratar a TI como uma despesa de custeio

e não de investimento também ajuda a reduzir drasticamente os custos iniciais na computação corporativa.

- **Redução de barreiras**: Por conta de sua facilidade de provisionamento, a computação em nuvem pode reduzir as barreiras de TI à inovação, como podem ser observadas em várias startups promissoras, como Airbnb, Spotify, dentre outras.

- **Facilidade para escalar**: torna-se mais fácil para as empresas dimensionarem seus serviços, que dependem cada vez mais de informações precisas, de acordo com a demanda do cliente. Como os recursos de computação são gerenciados por meio de software, eles podem ser implantados muito rapidamente conforme surgem novos requisitos.

- **Inovação**: A computação em nuvem também possibilita novas classes de aplicativos e fornece serviços que não eram possíveis antes, entre eles os aplicativos móveis carregados de inteligência artificial.

Interligando os benefícios no uso de computação em nuvem ao âmbito da gestão de riscos e à segurança da informação, a *European Network and Information Security Agency* (ENISA) aponta uma série de benefícios de segurança oferecidos pelo modelo de computação em nuvem, dentre eles a escalabilidade rápida e inteligente de recursos, considerando a ampla capacidade do provedor de nuvem de realocar dinamicamente recursos para gerenciamento de tráfego, autenticação, criptografia, medidas defensivas contra ataques cibernéticos, dentre outras vantagens relacionadas à gestão da segurança.

b) Riscos no uso da Nuvem

A norma ABNT NBR 27017:2016, nomeada "*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 em nuvem. Seu objetivo é fornecer controles específicos para serviços em nuvem, visando mitigar riscos inerentes a esse tipo de serviço.

Para obter uma solução completa de segurança em cenários de computação em nuvem, a ISO 27017:2016 deve ser adotada de forma complementar aos controles da norma ISO/IEC 27002:2013, pois esta apresenta requisitos de segurança primordiais e fundamentais para um

ambiente computacional independente da forma em que os recursos de Tecnologia da Informação são administrados.

Desta forma, as sugestões de controles explicitados na norma ABNT NBR ISO/IEC 27017:2016 foram construídos com base na reunião dos variados riscos atrelados ao uso de serviços em Nuvem, elencados por de instituições multinacionais e/ou governamentais, como pela ENISA (*European Network and Information Security Agency*) e NIST (*National Institute of Standards and Technology*, EUA), dentre outras.

Os principais riscos elencados pela norma ABNT NBR ISO/IEC 27017:2016, encontram-se evidenciados em variados artigos e relatórios, entre eles: *Guidelines on Security and Privacy in Public Cloud Computing* (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2011) e *Cloud Computing: benefits, risks and recommendations for information security* (ENISA, 2009), que serão usados como base para esta pesquisa, além de uma série de publicações acadêmicas a respeito do assunto.

De forma a estruturar determinados conjuntos de riscos pertinentes a computação em nuvem, para os fins desta pesquisa utilizou-se o modelo de agrupamento evidenciado no relatório publicado pela ENISA citado cima. A instituição separou os riscos de acordo com a sua natureza em diferentes grupos e, dentre eles, serão considerados para este trabalho:

I. Riscos Organizacionais e de Políticas
II. Riscos Técnicos
III. Riscos Legais e Regulatórios

I. Riscos Organizacionais e de Políticas

Nesta seção, são evidenciados alguns dos principais riscos que estão atrelados às esferas organizacionais relacionadas ao âmbito estratégico, incluindo a estruturação de governança, implementação de políticas, cláusulas contratuais, dentre outros assuntos relacionados. Para os fins deste estudo, foram evidenciados os seguintes riscos:

- **Perda de Governança e Controle**

Segundo o NIST (2011), com a ampla disponibilidade de serviços de computação em nuvem, a falta de controles organizacionais sobre os funcionários que envolvem esses serviços

arbitrariamente pode ser uma fonte de problemas. Em casos de perda de governança, por exemplo, sistemas vulneráveis poderiam ser implantados, regulamentações legais poderiam ser ignoradas, taxas poderiam se acumular rapidamente a níveis inaceitáveis, recursos poderiam ser usados para propósitos não sancionados ou outros efeitos adversos poderiam ocorrer (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2011).

A perda de governança e controle pode ter um impacto potencialmente severo na estratégia da organização e, portanto, na capacidade de cumprir sua missão e objetivos. Tais perdas podem levar à impossibilidade de cumprir os requisitos de segurança, a falta de confidencialidade, integridade e disponibilidade de dados e a deterioração do desempenho e da qualidade do serviço, sem mencionar a introdução de desafios de conformidade (ENISA, 2009).

- **Dependência do provedor (Lock-In ou Aprisionamento)**

Segundo Kim (2009), o aprisionamento e a baixa interoperabilidade entre provedores são problemas que os consumidores já conhecem ao adquirirem serviços, mesmo que não sejam os de computação em nuvem. Qian et al. (2009) ressalta a possibilidade de não haver uma padronização das interfaces externas dos diversos provedores de serviços em nuvem, o que significa que, uma vez um consumidor vinculando-se a um determinado provedor, ele pode estar limitado a esse provedor, sem a viabilidade tangível de migrar seus serviços para outro. Além disso, os provedores de nuvem podem ter um incentivo para impedir (direta ou indiretamente) a portabilidade dos serviços e dados de seus clientes. (ENISA, 2009)

- **Serviços Compostos e Cadeia de Disponibilidade**

Os consumidores preocupam-se se os serviços contratados terão disponibilidade satisfatória, pois este é um dos pontos críticos da computação em nuvem (ARMBRUST, 2009), porém não é possível saber ou prever quem serão as demais partes a compartilhar os recursos envolvidos e concorrer para uma eventual degradação do desempenho (SMITH, 2009).

Kim (2009) acrescenta que mesmo os provedores mais qualificados não estão livres de enfrentarem problemas e verem seus serviços ficar indisponíveis para os consumidores por algum período de tempo, também levando em consideração a possibilidade do provedor interromper a prestação dos serviços de forma definitiva ou deixar de dispor de condições para continuar prestando os serviços da maneira pactuada.

Segundo a ANISA (2009), um provedor de computação em nuvem pode terceirizar determinadas tarefas especializadas de sua cadeia de produção para terceiros. Em tal situação, o nível de segurança do provedor de nuvem pode depender do nível de segurança de cada um dos links e do nível de dependência do provedor de nuvem no terceiro. Qualquer interrupção ou corrupção na cadeia ou falta de coordenação de responsabilidades entre todas as partes envolvidas pode levar a: indisponibilidade de serviços, perda de confidencialidade de dados, integridade e disponibilidade, perdas econômicas e de reputação devido a falha em atender a demanda do cliente, violação de SLA, falha de serviço em cascata, dentre outros (ANISA, 2009).

II. Riscos Técnicos

Dentro da seção de riscos técnicos, levou-se em consideração aqueles riscos que estivessem atrelados às particularidades específicas das tecnologias de computação em nuvem, que podem ter impacto significativo em organizações caso venham a se concretizar. Para os fins desta pesquisa, foram evidenciados os seguintes riscos técnicos:

- **Falha de Isolamento**

Smith (2009) relata que muitas empresas hesitam em transferir seus dados para um computador externo que potencialmente possa permitir que esses dados sejam acessados por outras empresas que venham a compartilhar esse computador.

A multi-locação e recursos compartilhados são características que definem a computação em nuvem. Essa categoria de risco abrange a falha de mecanismos que separam armazenamento, memória, roteamento e reputação entre diferentes locatários (por exemplo, os chamados ataques de salto de clientes) (ENISA, 2009). O NIST (2011) ressalta que uma das mais sérias vulnerabilidades seria a possibilidade de um código malicioso (*malware*) ultrapassar as barreiras de isolamento de um locatário para outro, colocando os dados de uma ou mais organizações em risco.

- **Falha na interface de gerenciamento**

As interfaces de gerenciamento de clientes de um provedor de nuvem pública são acessíveis pela Internet e medeiam o acesso a conjuntos maiores de recursos (do que provedores

de hospedagem tradicionais) e, portanto, representam um risco maior, especialmente quando combinadas com vulnerabilidades de acesso remoto e de navegador da web (ENISA, 2012). Armbrust *et al.* (2009) acrescenta que, sobre a facilidade de escalabilidade por meio da interface de gerenciamento, apesar de este ser um dos argumentos de venda da computação em nuvem, os provedores têm enfrentado dificuldades técnicas para prover esta escalabilidade quando as estruturas de dados envolvidas se mostram complexas.

- **Exclusão dos dados incompleta ou insegura**

Segundo a ENISA (2009) quando uma solicitação para excluir um recurso de nuvem é feita, como na maioria dos sistemas operacionais, isso pode não resultar na limpeza real dos dados. A exclusão adequada ou oportuna de dados também pode ser impossível (ou indesejável do ponto de vista do cliente), seja porque cópias extras de dados são armazenadas, mas não estão disponíveis, ou porque o disco a ser destruído também armazena dados de outros clientes. No caso de múltiplos clientes reutilizando recursos de hardware, isso representa um risco maior para os clientes do que se utilizassem hardware dedicado (ENISA, 2009).

Segundo Valli e Woodward (2008), existem inúmeros exemplos de pesquisadores que obtêm discos usados de leilões on-line e outras fontes, e recuperam grandes quantidades de informações confidenciais destes dispositivos. Com as habilidades e equipamentos adequados, também é possível recuperar dados de unidades com falha, se elas não forem descartadas corretamente (SOBEY *et. al*, 2006).

- **Gestão de Identidade e Acessos**

Segundo o NIST (2011), evitar o acesso não autorizado a recursos de informações na nuvem também é uma consideração importante, e por isso a capacidade de adaptar os privilégios do consumidor de nuvem e manter o controle sobre o acesso aos recursos também é necessária.

A ENISA (2009) afirma que as atividades maliciosas de um usuário não autorizado poderiam ter um impacto sobre: a confidencialidade, integridade e disponibilidade de todos os tipos de dados, propriedade intelectual, todos os tipos de serviços e, portanto, indiretamente a

reputação da organização, a confiança do cliente e as experiências dos funcionários. Conforme ressaltado pelo NIST (2011), os níveis de autenticação devem ser apropriados para a sensibilidade das aplicações, ativos de informações acessados e o risco envolvido.

- **Invasores e Ataques**

Embora geralmente menos provável, o dano que pode ser causado por invasores mal-intencionados é geralmente de alta criticidade. Arquiteturas de nuvem exigem determinados papéis que são extremamente de alto risco. Exemplos incluem administradores de sistemas do CP e provedores de serviços de segurança gerenciados (ENISA, 2012). Kim (2009) expõe que provedores devem adotar instrumentos e procedimentos os mais avançados disponíveis e esforçar-se para prover níveis de segurança e privacidade melhores dos que os alcançáveis, utilizando-se do emprego recursos computacionais próprios.

A ENISA (2009) afirma que existem vários cenários diferentes nos quais os recursos de um cliente da nuvem podem ser usados por outras partes de maneira mal-intencionada, que por exemplo podem ser citados:

• Roubo de identidade: um invasor usa uma conta e usa os recursos do cliente para seu próprio ganho ou para prejudicar o cliente.

• O cliente não definiu limites efetivos para o uso de recursos pagos e pode arcar com custos inesperados como resultado de ações mal-intencionadas.

• Um invasor usa um canal público para usar os recursos do cliente.

III. Riscos Legais e Regulatórios

Na esfera de riscos legais e regulatórios foram considerados aqueles que estão relacionados ao cumprimento de determinadas obrigações jurídicas quanto ao uso da computação em nuvem, as quais podem influenciar a forma como as organizações são permitidas de utilizar a tecnologia em questão. Para os objetivos deste estudo, foram considerados os riscos pertinentes aos seguintes pontos:

- **Conformidade**

Kim (2009) evidencia que as empresas precisam atender a dispositivos legais, o que as obriga a preservar documentos e manter certas regras de conduta. Como consequência, é necessário que os provedores de nuvem agreguem às suas ofertas instrumentos que garantam aos seus clientes o atendimento a esses dispositivos legais. Já o NIST (2011) complementa que os provedores de serviços de nuvem estão se tornando mais sensíveis às questões legais e regulamentares, podendo estar dispostos a se comprometer pelo armazenamento e processamento de dados em jurisdições específicas, e a aplicar as proteções necessárias afim de manter a segurança e privacidade de seus clientes.

Armbrust et al. (2009) e a ENISA (2009) também evidenciam questões relacionadas ao licenciamento de software, afirmando que os sistemas de cobrança praticados pelos desenvolvedores para licenciar seus produtos podem inviabilizar o uso de determinadas aplicações em infraestruturas de Nuvem. As condições de licenciamento, como contratos por estação e verificações de licenciamento on-line, podem se tornar impraticáveis em um ambiente de nuvem. Por exemplo, se o software for cobrado por instância toda vez que uma nova máquina for instanciada, os custos de licenciamento do cliente da nuvem poderão aumentar exponencialmente, embora estejam usando o mesmo número de instâncias da máquina pela mesma duração.

- **Proteção de Dados**

O cliente da nuvem (em sua função de controlador de dados) pode enfrentar dificuldades em verificar efetivamente o processamento de dados que o provedor de nuvem executa e, assim, ter certeza de que os dados são tratados de maneira legal. O não cumprimento de leis que envolvem a proteção de dados pode levar a sanções administrativas, civis e criminais, que variam de país para país (ENISA, 2009).

Armbrust et al. (2009) também ressalta que a legislação de vários países faculta a órgãos governamentais e reguladores o acesso a dados para fins de inspeções e auditorias. Como consequência, muitos consumidores incomodam-se com a perspectiva de que os provedores de serviços em nuvem sejam obrigados a liberar a esses órgãos o acesso a dados confidenciais. Além de estarem suscetíveis a quebra de sigilo por instituições governamentais estrangeiras,

Rowe (2007) complementa que os registros de dados são considerados a nova moeda do século 21, e os armazenamentos de dados baseados em nuvem são o como cofres de bancos, tornando-os um alvo cada vez mais preferido também por atacantes e criminosos, devido ao valor coletivo concentrado neles.

- **Residência de Dados**

Segundo o NIST (2011), uma das características de muitos serviços de computação em nuvem é que os dados são armazenados redundantemente em vários locais físicos e informações detalhadas sobre a localização dos dados de um cliente não estão disponíveis ou não são divulgadas ao consumidor do serviço. Essa situação dificulta a verificação da existência de salvaguardas suficientes e do cumprimento dos requisitos de conformidade legal e regulatória. Quando as informações cruzam as fronteiras, os regimes legais, de privacidade e regulatórios podem ser ambíguos e suscitar uma série de preocupações (WEICHERT, 2011). Consequentemente, as restrições ao fluxo de dados sensíveis entre fronteiras, bem como os requisitos de proteção dos dados, tornaram-se objeto de leis e regulamentos nacionais e regionais de privacidade e segurança (EISENHAUER, 2005).

A ENISA (2009) ressalta que os dados de clientes podem ser mantidos em várias jurisdições de países distintos, alguns dos quais podem representar alto risco. Se os *data centers* estiverem localizados em países de alto risco - por exemplo, sem o estado de direito e com uma estrutura legal imprevisível, estados policiais autocráticos, estados que não respeitam acordos internacionais -, os locais que residem os dados podem ser invadidos por autoridades locais e as informações dos clientes podem estar sujeitas a divulgação forçada ou apreensão.

- **Auditoria e gestão de metadados**

As organizações possuem incentivos e obrigações para preservar e produzir documentos eletrônicos provenientes de metadados, como atender a solicitações de informações de auditoria e regulamentações, em conformidade com legislação vigente (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2011). Armbrust et al. (2009) também aponta sobre a confidencialidade sobre a auditoria destes dados, ressaltando que a legislação de vários países faculta a órgãos governamentais e reguladores o acesso a dados para fins de inspeções e auditorias e, como consequência, muitos consumidores incomodam-se com a perspectiva de

que os provedores de serviços em nuvem sejam obrigados a liberar a esses órgãos o acesso a dados confidenciais.

Segundo a ENISA (2009), no caso de confisco de hardware físico como resultado de intimação por órgãos de segurança pública ou processos civis, a centralização do armazenamento, bem como a locação compartilhada de hardware físico significa que mais clientes além do alvo principal correm o risco de terem as suas informações divulgadas para partes indesejadas. Ao mesmo tempo, pode ser impossível para a agência de uma única nação confiscar "uma nuvem", considerando os avanços tecnológicos em torno da distribuição geográfica dos dados.

Tratando-se de questões relacionadas à auditoria, a forma como o provedor de nuvem mantém os dados e disponibiliza ferramentas que permitem a descoberta e coleta destes dados (processo também conhecido como *Electronic Discovery ou e-discovery*), afetam a capacidade da organização de cumprir suas obrigações de maneira econômica, oportuna e em conformidade (MCDONALD, 2010). Por exemplo, os recursos de arquivamento de um provedor de nuvem podem não preservar os metadados originais conforme o esperado, causando degradação (ou seja, destruição intencional, imprudente ou negligente, perda, alteração material ou obstrução de evidência relevante para litígio), o que poderia impactar negativamente o litígio (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2011).

2.5.3. Recomendações para a Gestão de Riscos no uso da Nuvem

Segundo o NIST (2011), deve-se haver um programa de gerenciamento de riscos que seja flexível o suficiente para lidar com o cenário de riscos em constante evolução e mudança, principalmente quando se trata de tecnologias.

Considerando os riscos que foram mencionados anteriormente, esta seção trará recomendações que são aplicáveis para a gestão mais efetiva dos riscos relacionados ao uso da computação em nuvem.

Usados como base para a construção da norma ABNT NBR ISO/EIC 27017:2016, seguem os pontos de alta relevância elencados pelas organizações NIST, ENISA e Cloud Security Alliance (CSA), como também as exigências da legislação atual no que tange o uso de Nuvem pelo governo, incluindo recomendações para a gestão de tais riscos.

Para uma estruturação eficiente das informações deste tópico, optou-se por utilizar o modelo de agrupamento evidenciado no relatório *Security Guidance for Critical Areas of Focus in Cloud Computing*, publicado pela Cloud Security Alliance (CSA, 2017), que elenca as informações dentro certas dimensões, das quais serão abordadas neste estudo:

I. Governança
II. Legislação e Regulamentações
III. Conformidade e Auditoria
IV. Continuidade dos Negócios
V. Segurança
VI. Isolamento
VII. Gestão de Identidade e Acessos
VIII. Proteção de Dados
IX. Resposta à Incidentes

I. Governança

Na dimensão de Governança, são abordados tópicos relativos ao 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.

Conforme a Lei 13.709 – Lei Geral Brasileira de Proteção de Dados (LGPD), Art. 50, é definido que pode-se implementar programas de governança que, no mínimo: demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o à proteção de dados pessoais; seja adaptado à estrutura, bem como à sensibilidade dos dados tratados; seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Dando continuidade às recomendações da LGPD, a ABNT ISO/IEC 27017 também sugere que seja instituído um programa de gerenciamento de riscos que seja flexível o suficiente para adaptar-se ao cenário de risco em constante evolução e mudança para o ciclo de vida do sistema, desenvolvendo um modelo ou estrutura de governança em nuvem de acordo com as melhores práticas relevantes do setor, padrões globais e regulamentações (NIST, 2011; CSA, 2017);

Segundo a CSA (2017), para que estas ações sejam executadas da melhor maneira, é importante entender como um contrato afeta a estrutura / modelo de governança da instituição, a partir da análise de contratos (e quaisquer documentos referenciados) antes de entrar em um acordo com provedores de nuvem. Também é aconselhado determinar requisitos de governança para obter informações antes de planejar uma transição para a nuvem, incluindo requisitos legais e regulamentares, obrigações contratuais e outras políticas corporativas (CSA, 2017).

Já durante a migração, quando se trata de das práticas organizacionais relativas às políticas, procedimentos e padrões usados para o desenvolvimento de aplicativos e aquisição de serviços, bem como o design, implementação, teste, uso e monitoramento de serviços implantados ou envolvidos, devem ser estendidos para abranger inclusive os ambientes de computação em nuvem, efetuando-se também o monitoramento contínuo do estado de segurança para suportar decisões de gerenciamento de risco (NIST, 2011; CSA, 2017).

A CSA (2017) ressalta que, em vez de apenas transferir as arquiteturas de informações já existentes localmente para a nuvem, deve-se aproveitar a oportunidade da migração para repensar e reestruturar se necessário a infraestrutura existente de forma a torná-la mais eficiente.

II. Legislação e Regulamentações

Quando se trata da legislação e regulamentações relativas ao uso de nuvem, a gestão de riscos quanto à estes tópicos pode ser mais eficiente ao entender os vários tipos de leis e regulamentos que impõem obrigações de segurança e privacidade à organização e potencialmente impactam as iniciativas de computação em nuvem, incluindo aquelas envolvendo localização/residência de dados, controles de privacidade e segurança, gerenciamento de registros, capacidade de atender a requisições de *e-discovery* e outras obrigações legais (CSA, 2017).

De acordo com a ABNT NBR ISO/IEC 27002, antes de se concluir uma aquisição de serviços em nuvem, a instituição deve realizar uma avaliação e identificação da legislação aplicável e de requisitos contratuais, considerando das propostas de um fornecedor para entender se estão a preencher todos os requisitos. Conforme recomendado pelo NIST (2011), também deve-se atualizar regularmente essa avaliação, monitorando o escopo, a natureza e a consistência dos serviços a serem adquiridos.

- **Exigências quanto à residência de dados (*Data Residency Request*)**

Segundo a LGPD, operações de tratamento de dados realizadas dentro do território brasileiro estão invariavelmente sujeitas à aplicação das leis nacionais, assim como as operações que tenham por objetivo a oferta ou fornecimento de bens ou serviços a indivíduos localizados no território brasileiro, ainda que a empresa responsável por essa atividade esteja sediada ou localizada fora do país. Ao se referir ao "tratamento" de dados, a lei considera o conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Considerando um caso relevante do contexto atual sobre a residência de dados, a Portaria GSI n.º 9/2018, define que os dados, metadados, informações e conhecimento, produzidos ou custodiados por órgão ou entidade da administração pública federal, consideradas informações com restrição de acesso de acordo com a legislação vigente, podem ser tratadas em ambientes de nuvem, mas devem residir exclusivamente em território brasileiro, exigência também conhecida como *data residency request*.

- **Exigências quanto à Instrução Normativa Nº 1, de 4 de abril de 2019**

A Instrução Normativa nº 1, divulgada no dia 04 de abril de 2019 pela Secretaria de Governo Digital do Ministério da Economia prevê que "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", vedando a alocação de recursos em infraestrutura local, salvo nos casos em que o órgão ou entidade tenha obtido autorização prévia do Órgão Central do SISP mediante a apresentação de justificativa.

Tal instrução normativa pode representar a inclinação do governo para, no futuro, flexibilizar o uso da nuvem por instituições públicas por meio de mudanças na legislação, visto que o seu uso está sendo incentivado quando comparado ao investimento em infraestrutura local.

- **Exigências quanto à acórdão Nº 1739/2015 do TCU**

O Tribunal de Contas da União publicou em 2015 o Acórdão Nº 1739, que trata da gestão de riscos relacionados à contratação e uso de serviços de computação em nuvem por instituições do governo federal. O documento identifica 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.

No tocante aos riscos, à segurança das informações e à disponibilidade dos serviços, a unidade instrutiva destaca que, muito embora seja possível obter vantagem competitiva e/ou econômica por meio da adoção da computação em nuvem, devem ser adotadas ações com vistas a mitigá-los.

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

III. Conformidade e Auditoria

Para que uma organização possa executar uma gestão de riscos eficiente em torno de suas obrigações relativas à conformidade, devem ser usados 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 do sistema (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2011). Segundo a norma ABNT NBR ISO/EIC 27002, convém que as atividades e requisitos de auditoria sejam cuidadosamente planejados e acordados para minimizar interrupção dos processos do negócio. Tais tarefas devem ser contínuas, e não apenas atividades pontuais, de forma a garantir a conformidade do ambiente em nuvem (CSA, 2017).

A CSA (2017) recomenda que, para a execução de tais tarefas, sejam selecionados auditores com experiência em computação em nuvem, especialmente se as auditorias e certificações forem usadas para gerenciar o escopo de auditoria do instituição, certificando-se de que eles entendam quais artefatos de conformidade o provedor oferece para a coleta e gestão eficiente desses artefatos. Ainda é aconselhado assegurar-se de que os acordos de serviço tenham meios suficientes para permitir a visibilidade dos controles e processos de segurança e

privacidade empregados pelo provedor de nuvem e seu desempenho ao longo do tempo (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2011);

Segundo o NIST (2011), é importante analisar e avaliar as ofertas do provedor de nuvem com relação aos requisitos organizacionais de conformidade a serem cumpridos e garantir que os termos do contrato atendam adequadamente aos requisitos. As instituições precisam inclusive entender o conteúdo e o formato dos dados que o provedor de nuvem fornecerá para fins de análise e avaliar se os dados da perícia disponível satisfazem os requisitos legais (CSA, 2017).

IV. Continuidade dos negócios

Nesta dimensão serão tratadas recomendações quanto a continuidade dos negócios, que segundo Portaria GSI n.º 9/2018, define-se pela capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido. A publicação ainda destaca que o planejamento é necessário 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.

Segundo o NIST (2011), é essencial assegurar-se de 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. Recomenda-se entender as cláusulas e procedimentos contratuais para disponibilidade, backup e recuperação de dados e recuperação de desastres e garanta que eles atendam aos requisitos de continuidade e de contingência do planejamento da organização (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2011).

Considerando a um caso de indisponibilidade do provedor, uma alternativa pode ser a migração dos serviços para outro fornecedor, conforme a Lei 13.709 (LGPD) em seu Art. 17 inciso V, que define que o provedor deve garantir a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador.

No que tange ao planejamento prévio, a CSA (2017) aconselha construir uma arquitetura sempre levando em consideração as possibilidades de falhas, incluindo uma indisponibilidade geral do provedor. Porém, como na maioria das vezes não há recursos suficientes para manter uma disponibilidade completamente infalível do ambiente, deve-se priorizar os recursos utilizando uma abordagem baseada em riscos e probabilidade.

Buscando-se evitar situações dispendiosas, é interessante entender a história, as capacidades e as limitações dos provedores de nuvem, buscando-se aproveitar as vantagens das funcionalidades específicas de cada provedor da melhor forma possível, tratando-se da continuidade dos negócios (CSA, 2017).

V. Segurança

Na dimensão relativa à segurança, são abordadas algumas das principais medidas para garantir a disponibilidade, integridade, confidencialidade e a autenticidade da informação, conforme o conceito de segurança da informação e comunicações evidenciado na Portaria GSI n.º 9/2018.

Sobre o tema, a Lei 13.709 (LGPD), em seu Art. 46, define que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Considerando medidas para uma gestão eficiente da segurança, segundo a ABNT NBR ISO/EIC 27002, convém que o cliente do serviço em nuvem deve determinar os requisitos de segurança da informação e avalie se o serviço oferecido pelo provedor do serviço em nuvem cumpre com tais requisitos. É essencial, inclusive, entender as tecnologias subjacentes que o provedor de nuvem usa para provisionar serviços, incluindo as implicações que os controles técnicos envolvidos têm na segurança e privacidade do sistema (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2011).

A CSA (2017) complementa que se deve estar de acordo com as limitações do provedor de nuvem em avaliações de vulnerabilidade e testes de penetração, revisando certificações e atestados de conformidade específicos do setor regularmente, de forma a obter garantia de que o provedor está seguindo as práticas recomendadas e os regulamentos da infraestrutura em

nuvem. É ressaltado inclusive que provedor tem a responsabilidade de garantir que as camadas físicas, de abstração e de orquestração subjacentes da nuvem sejam seguras.

A CSA (2017) ainda recomenda que sejam aplicados testes de segurança ao processo de implantação de soluções, minimizando a dependência de dispositivos virtuais que restrinjam a elasticidade ou causem gargalos de desempenho, também levando em consideração as novas opções e requisitos de arquitetura na nuvem. As políticas e padrões de segurança devem ser atualizadas, e não apenas aplicar os padrões pré-existentes em um modelo de computação totalmente diferente.

VI. Isolamento

Na dimensão de isolamento, as recomendações e o conceito relativo ao tópico são resumidas pelo Art. 39 do Decreto Nº 7.845/2012, que define que os equipamentos e sistemas utilizados para a produção de documento com informação classificada em qualquer grau de sigilo deverão estar isolados ou ligados a canais de comunicação seguros, que estejam físicas ou logicamente isolados de qualquer outro, e que possuam recursos criptográficos e de segurança adequados à sua proteção.

A maior parte da segurança fundamental da virtualização recai sobre o provedor de nuvem, porém é dever do consumidor entender a virtualização e outras técnicas de isolamento lógico que o provedor de nuvem emprega em sua arquitetura de software de multi-locação e avaliar os riscos envolvidos para a 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 (NIST, 2011; CSA, 2017).

A CSA (2017) recomenda a utilização dos recursos de isolamento disponibilizados pelo provedor para a variedade de redes virtuais, contas e segmentos de nuvem para aumentar o isolamento da rede, pois contas separadas e redes virtuais limitam drasticamente o volume de danos no caso de um incidente, quando em comparação com os data centers tradicionais (CSA, 2017).

VII. Gestão de Identidade e Acessos

A dimensão de Gestão de Identidade e Acessos, segundo o seu conceito evidenciado na Portaria GSI n.º 9/2018, trata do conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso aos meios de tecnologia oferecidos.

Para uma gestão de riscos eficiente, segundo o Decreto Nº 7.845/2012, Art. 38, aconselha que os sistemas de informação de que tratam de informações classificadas deverão ter níveis diversos de controle de acesso e utilizar recursos criptográficos adequados aos graus de sigilo, como também deverão manter controle e registro dos acessos autorizados e não-autorizados e das transações realizadas por prazo igual ou superior ao de restrição de acesso à informação.

O NIST (2011), aconselha que as instituições devem assegurar-se de que as proteções adequadas estejam em vigor para proteger as funções de autenticação, autorização e outras funções de gerenciamento de identidade e acesso e sejam adequadas para a organização. A CSA (2017) acrescenta que é interessante manter um controle rígido das credenciais da conta de administrador global, considerando o uso de dupla autoridade e/ou múltiplo fator de autenticação para acessá-las, considerando também utilizar contas de superadministrador para casos especiais e outras com menos privilégios para a administração do dia-a-dia, em vez de apenas uma conta principal.

Dando continuidade ao tema, propõe-se que as organizações implementem consistentemente uma política de privilégios mínimos para o acesso a funcionalidades específicas que podem colocar o ambiente em risco, separando os privilégios de contas de desenvolvimento e teste por exemplo (CSA, 2017). Também é sugerido sempre incluir funcionalidades para tornar a segurança de acesso mais robusta no caso de contas privilegiadas, como a autenticação multifator, biometria, permissionamento com base em local geográfico, rede, horários de acesso, dentre outros (CSA, 2017).

VIII. Proteção de dados

No que se refere à dimensão de proteção de dados, a ABNT NBR ISO/EIC 27002 aponta que convém que a privacidade e a proteção das informações sejam asseguradas conforme requerido por legislação e regulamentação pertinente. Sobre o tópico, são abordadas as questões evidenciadas na LGPD, como também na Lei Nº 12.527 (Lei de Acesso à Informação) Art. 6º, que define que cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a: gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação; proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e proteção da informação sigilosa e da informação

pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

Para gerenciar riscos relativos à esta dimensão, cabe às instituições avaliar a adequação das soluções de gerenciamento de dados do provedor de nuvem para os dados organizacionais relevantes e a capacidade de controlar o acesso às informações, protegê-las enquanto estão em repouso, em trânsito e em uso, enquanto também se estabelece direitos de propriedade claros e exclusivos sobre os dados (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2011);

Levando em consideração os riscos à segurança, o NIST (2011) adverte que é importante analisar o risco de agrupar dados organizacionais com o de outras organizações cujos perfis de ameaça são altos ou cujos dados coletivamente representam um valor concentrado significativo. Ainda é ressaltado que se deve entender e avaliar totalmente os riscos envolvidos no gerenciamento de chaves criptográficas com os recursos disponíveis no ambiente de nuvem e os processos estabelecidos pelo provedor.

Além destas recomendações, a CSA (2017) indica utilizar a opção de criptografia apropriada com base nos modelos de gestão de riscos para os dados, negócios e requerimentos técnicos, considerando o uso de opções de criptografia e armazenamento gerenciadas pelo provedor, e sempre que possível, deve-se utilizar uma chave gerenciada pela organização. Também é concluído que não se deve confiar e depender completamente dos controles de acesso e criptografia, informando que o ideal é que se construa uma arquitetura que, por natureza de sua estrutura, possa prevenir problemas relacionados à segurança de dados.

IX. Resposta à incidentes

A dimensão de resposta à incidentes abrange, de acordo com a Portaria GSI n.º 9/2018, as ações definidas por receber, filtrar, classificar e responder às solicitações e alertas, como também realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências.

Sobre o assunto, a Lei 13.709 (LGPD), em seu Art. 50, define que se devem estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de possíveis impactos e riscos à privacidade, contando com a elaboração de planos de resposta a incidentes e remediação.

Para a gestão de riscos relativos a este tema, é preciso que a instituição tenha conhecimento das disposições contratuais e dos procedimentos para resposta a incidentes e assegurar-se de que eles atendam aos requisitos da organização (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2011). Ressalta-se inclusive que o contrato de especificações de serviço, também conhecido como Service Level Agreement (SLA), com cada provedor de serviços em nuvem deve garantir suporte para o tratamento de incidentes necessário para a execução efetiva do plano de resposta a incidentes corporativos, abrangendo cada estágio do processo de tratamento de incidentes: detecção, análise, contenção, erradicação e recuperação (CSA, 2017).

Também é aconselhado garantir que o provedor de nuvem tenha um processo de resposta transparente e mecanismos suficientes para compartilhar informações durante e após um incidente (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2011), conforme exigido pela LGPD em seu Art. 48, que evidencia o dever de um provedor de comunicar à autoridade nacional e ao titular a ocorrência do incidente de segurança que possa acarretar risco ou dano relevante aos titulares. A lei inclusive ressalta que a comunicação deve ser feita em prazo razoável, e deverá mencionar, dentre outros pontos: a descrição da natureza dos dados pessoais afetados; a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados; os riscos relacionados ao incidente; e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Tratando-se das recomendações às instituições, o NIST (2011) indica 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. Segundo a CSA (2017), as organizações devem inclusive adotar o monitoramento contínuo para detectar possíveis problemas com a maior antecedência possível, executar testes recorrentes e possuir caminhos de comunicação adequados com o provedor que podem ser utilizados no caso de um incidente.

Por fim, é também apontado que as fontes de dados devem ser armazenadas ou copiadas em locais que mantenham a disponibilidade durante incidentes, e os aplicativos baseados em nuvem devem aproveitar a automação e a orquestração para otimizar e acelerar a resposta, incluindo contenção e recuperação (CSA, 2017).

3. MÉTODO E TÉCNICA DE PESQUISA

De modo a cumprir com os objetivos da pesquisa, seria ainda necessário, respectivamente: (a) explorar e verificar a pertinência e adequação dos benefícios apontados e das proposições relativas às barreiras e aos riscos associados à computação em nuvem e (b) fazer recomendações destinadas a auxiliar os tomadores de serviços oferecidos em Nuvem a tratar a questão dos riscos.

Para se obter de maneira eficiente as informações para esta pesquisa, ela deverá ser executada com uma abordagem qualitativa, com objetivos exploratórios e utilizando-se o procedimento conceituado de entrevistas semiestruturadas.

3.1. Quanto a Abordagem

De acordo com Goldenberg (1997), "enquanto os métodos quantitativos supõem uma população de objetos comparáveis, os métodos qualitativos enfatizam as particularidades de um fenômeno em termos de seu significado para o grupo pesquisado". Já Minayo (2001), aponta que "a pesquisa qualitativa trabalha com o universo de significados, motivos, aspirações, crenças, valores e atitudes, o que corresponde a um espaço mais profundo das relações, dos processos e dos fenômenos que não podem ser reduzidos à operacionalização de variáveis".

Relacionando elementos que compõem uma pesquisa qualitativa ao objetivo desta pesquisa, entende-se que seria a melhor abordagem em função da busca pelos posicionamentos dos gestores de órgãos públicos federais a respeito da utilização de serviços de Nuvem, considerando seus riscos e benefícios.

3.2. Quanto aos Objetivos

Segundo Gil (2007), a pesquisa exploratória tem como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses. O autor afirma que a grande maioria destas pesquisas envolve: (a) levantamento bibliográfico; (b) entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado; e (c) análise de exemplos que estimulem a compreensão.

Considerando-se as características de uma pesquisa exploratória, entende-se que ela é apropriada para este caso em que haverá execução de entrevistas estruturadas com profissionais de TI para entender diversos pontos de vista relacionados aos riscos de Nuvem no governo.

3.3. Quanto aos Procedimentos

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. 2007).

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 et al. 2006). Os autores complementam que, por conta disso, técnicas de grupos estáticos envolvem respostas agregadas de especialistas de uma rodada de questionamentos.

Segundo Dayananda et al. (2002), aplicações de entrevistas são caracterizadas por uma rodada de coleta de informações de indivíduos conhecedores com interação moderada entre o facilitador e os respondentes e pouca ou nenhuma comunicação entre os entrevistados. A autora relata que entrevistas envolvem a coleta de informações subjetivas de respondentes qualificados e a subsequente agregação dos resultados.

Já Longhurst (2010), introduzindo o conceito de entrevista semiestruturada como um intercâmbio verbal em que uma pessoa, o entrevistador, tenta extrair informações de outra pessoa fazendo perguntas. O autor afirma que, embora o entrevistador prepare uma lista de perguntas pré-determinadas, as entrevistas semiestruturadas se desdobram de maneira coloquial, oferecendo aos participantes a oportunidade de explorar questões que consideram importantes (LONGHURST, 2010).

A opção de procedimento para esta pesquisa foi definida pelo uso de entrevistas semiestruturadas, buscando adquirir opiniões e posicionamentos individuais dos entrevistados, tomando por base as proposições relativas a barreiras, riscos e as indicações dos benefícios, conforme identificadas na literatura relativa à computação em nuvem e já devidamente condensadas, estruturadas e comentadas no Referencial Teórico.

3.4. Entrevistas semiestruturadas

Na execução de uma entrevista, segue-se um roteiro previamente estabelecido, as perguntas são predeterminadas e o objetivo é obter diferentes respostas à mesma pergunta, possibilitando que sejam comparadas (GERHARDT; SILVEIRA, 2009).

Entrevistas semiestruturadas (às vezes chamadas de entrevistas informais, conversacionais ou "suaves") tratam de conversar com pessoas, mas de maneiras que são autoconscientes, organizadas e parcialmente estruturadas (LONGHURST, 2010). Krueger e Casey (2000) explicam que a entrevista semiestruturada é sobre falar, como também sobre ouvir, criando um ambiente confortável para as pessoas compartilharem suas opiniões.

Nas entrevistas foram analisadas as opiniões dos entrevistados quanto à sua percepção de importância dos riscos e benefícios relacionados ao uso de nuvem no governo federal, incluindo perguntas abertas para identificar os motivos de sua instituição estar ou não aderindo à tecnologia, como também quais os fatores que o influenciariam a tomar outros posicionamentos quanto à aderência de tais soluções. O questionário de entrevista semiestruturada utilizado nesta pesquisa pode ser conferido na seção de apêndices deste documento.

- **Participantes das entrevistas**

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, 2002).

Para esta pesquisa, os entrevistados deverão ser funcionários de instituições do Governo Federal, fazendo parte de departamentos relacionados a Tecnologia da Informação, infraestrutura, segurança ou equivalentes, e estar incluídos 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 na coordenação 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).

3.5. Análise dos dados

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

Os dados levantados com a execução das entrevistas foram utilizados para compor as conclusões relativas ao posicionamento dos órgãos federais entrevistados com relação à gestão de riscos do uso da computação em Nuvem.

4. REALIZAÇÃO DAS ENTREVISTAS

Para o cumprimento dos objetivos desta pesquisa, explorou-se a pertinência e o tratamento dos riscos considerados mais relevantes para a amostra de entrevistados do Governo Federal, e uma vez tendo sido selecionado o método de pesquisa para tal e definida uma sistemática para sua aplicação, na sequência, realizou-se efetivamente a aplicação. Neste capítulo é, então, detalhado o processo de realização das entrevistas semiestruturadas, que foram conduzidas em abril de 2019, seguindo a sistemática definida no tópico 3.4.

Para selecionar os entrevistados a participar da pesquisa, foi estabelecido um elenco de fatores de qualificação, que deveriam se encaixar em algum dos critérios elencados no tópico 3.4, sendo que todos deveriam ser membros de instituições públicas e/ou relacionadas ao governo federal.

A amostra desta pesquisa contém entrevistas com 10 instituições atuantes em diferentes áreas da administração pública federal, incluindo o poder judiciário, executivo, do setor financeiro e agências reguladoras, das quais são elencadas:

- 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
- Conselho da Justiça Federal (CJF)
- Ministério da Economia
- Ministério do Desenvolvimento Regional (MDR)
- Secretaria do Tesouro Nacional (STN)

Considerando que parte dos assuntos da pesquisa pode expor as organizações de maneira inconveniente por se tratar de contextos relacionados à segurança da informação e demais aspectos da infraestrutura tecnológica das instituições entrevistadas, optou-se por segmentar as respostas de maneira anônima, utilizando-se uma numeração de 1 a 10 para identificar cada entrevistado, incluindo também siglas como, por exemplo, *E01*, *E02* em diante.

Para conduzir a entrevista, foi elaborado um roteiro de pesquisa que aborda questões relativas à maturidade das instituições quanto ao uso de tecnologias baseadas em nuvem, como também as percepções dos entrevistados sobre as dimensões de recomendações elencadas no ponto 2.8, dentro do contexto da gestão de riscos.

4.1. Maturidade no uso de nuvem

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

- **Entrevistado 01**

O entrevistado da instituição 01 afirma que a sua instituição utiliza serviços em nuvem há 1 ano no modelo SaaS, porém foram apenas liberadas para os funcionários do departamento de TI. Atualmente existe um receio quanto ao impacto do uso de soluções IaaS, ressaltando que a equipe ainda não possui experiência suficiente para a sua implementação e, portanto, ainda estão executando testes.

- **Entrevistado 02**

A instituição 02 já utiliza SaaS e IaaS há 2 anos, disponibilizando os serviços de colaboração para a maioria de seus usuários, e hospedando aplicações e sistemas de monitoramento. Antes de proverem acesso aos serviços por toda a organização, estão executando análises de riscos para decidir se realmente será feito. É ressaltando pelo entrevistado que, em breve, será buscado contratar mais serviços em nuvem, considerando inclusive que os serviços críticos do órgão devem estar hospedados nesta tecnologia por conta de sua alta disponibilidade, como também não pretendem alocar mais recursos em hardware e em outras soluções locais.

- **Entrevistado 03**

A organização 03 utiliza, há 5 anos, PaaS, SaaS e IaaS, hospedando por exemplo os sistemas de avaliação de desempenho de RH, plataforma de gestão de relacionamento com

clientes (CRM), controladores de rede e soluções de colaboração. Durante os últimos anos, existiram casos em que deixaram de utilizar certos serviços por conta de finalizações de contrato e/ou troca de fornecedores, porém estes foram substituídos por outras soluções em nuvem. Considerando o futuro, o entrevistado afirma que a sua primeira opção é adquirir serviços em nuvem por conta da redução dos custos, segurança e escalabilidade mais eficiente que uma infraestrutura local oferece.

- **Entrevistado 04**

O entrevistado 04 relatou que o órgão público em que trabalha utiliza SaaS para colaboração e comunicação há 1 ano e meio, disponível para a maioria de seus funcionários. Tratando-se de infraestrutura, atualmente estão em fase de piloto e testes com usuários limitados, enquanto ainda aguardam os posicionamentos dos provedores quanto a questões relativas à residência dos dados e outros requisitos legais. Atualmente os planos para transferir a infraestrutura para a nuvem estão suspensos por conta da falta de maturidade da instituição e a inexperiência dos funcionários com as soluções.

- **Entrevistado 05**

A entidade 05 utiliza soluções em SaaS para colaboração e teletrabalho há 3 anos para uma parcela dos funcionários. Existem planos para fortalecer a adoção e utilização de nuvem por parte de todo o órgão, fomentando questões relativas à transformação digital e teletrabalho.

- **Entrevistado 06**

A instituição governamental 06 utiliza SaaS há 6 anos, com soluções de produtividade, colaboração e comunicação disponíveis atualmente para a maior parcela dos funcionários. Durante este período, houve um caso de insucesso com o desempenho no uso da nuvem de um fornecedor que acarretou a desistência nos planos de migração de algumas aplicações, o que hoje gera certa desconfiança quanto ao uso de nuvem para tais fins. Para o futuro planeja-se implementar soluções de monitoramento e gestão de riscos, como também migrar bases de dados para a nuvem com o objetivo de gerar relatórios em tempo real, mas, porém, ambos os planos ainda estão em desenvolvimento.

- **Entrevistado 07**

A organização 07 atualmente possui alta maturidade quanto ao uso de nuvem, em que há 3 anos utilizam serviços de inteligência artificial, gestão inteligente de hospedagem de aplicações (*containers*), soluções de produtividade, colaboração e comunicação. Há uma premissa de que a nuvem deve ser usada pela instituição apenas como plataforma PaaS, pois a sua infraestrutura é autossuficiente quanto às demandas que supostamente seriam atendidas com IaaS. Para o futuro, pretende-se trazer para a nuvem o máximo de sistemas e dados que forem permitidos pela legislação que, atualmente, não permite o tratamento de dados sigilosos em tais ambientes.

- **Entrevistado 08**

O entrevistado da empresa 08 afirma que, apesar de ter acesso à certos serviços, atualmente não há utilização de soluções em nuvem em produção pelos seus funcionários, majoritariamente por preocupações relativas à segurança. Apenas estão sendo executados pilotos e testes nos últimos 6 meses. Para o futuro, pretende-se implementar uma utilização maior de soluções em nuvem por conta de capacidade de processamento escalável e a disponibilidade de serviços cognitivos baseados em inteligência artificial.

- **Entrevistado 09**

A instituição 09 utiliza IaaS, PaaS e SaaS há 1 ano e 6 meses. Por conta de ser uma implementação recente, a adoção das tecnologias ainda está em fase inicial, com disponibilidade limitada a certos usuários. Considerando o futuro, o entrevistado afirma que está sendo planejada a migração de todos os serviços da instituição para a nuvem nos próximos anos, considerando as recomendações da IN 01/2019.

- **Entrevistado 10**

O órgão público 10 utiliza SaaS para a colaboração, comunicação e produtividade de seus funcionários há 8 meses, porém apenas parte dos servidores estão utilizando, devido que ainda se está promovendo a adoção destes programas. Há interesse em utilizar mais recursos da computação em nuvem no futuro por conta das normas mais recentes que incentivam a utilização pelas instituições do governo, porém atualmente estão estruturando os seus planos quanto às migrações e possíveis aquisições de serviços em nuvem.

4.2. Percepções relativas às recomendações para a gestão de riscos na Nuvem

Após serem avaliados quanto à maturidade, a abordagem se estruturou ao redor dos pontos elencados na seção 2.8, tratando-se de como as organizações estão se posicionando quanto à gestão de riscos em cada uma das dimensões citadas anteriormente, de acordo com estrutura do relatório publicado pela *Cloud Security Alliance* (CSA, 2017). Nesta etapa da entrevista, o objetivo foi elencar as maiores preocupações das organizações e avaliar quais são os seus planos para mitigar os riscos relacionados. Buscou-se categorizar cada instituição com base na situação atual de seu planejamento estratégico, observando se estão sendo executadas ações para a gestão dos riscos ou não, como também se há planos de se implementar práticas ou políticas a respeito dos riscos em questão.

4.2.1. Governança

Segundo todos os entrevistados, atualmente os planejamentos quanto à governança específica para o uso de nuvem estão em andamento e em fase inicial. Portanto, ainda não há implementação de políticas e diretrizes sendo executadas neste momento, mas estão se desenvolvendo à medida que a maturidade dos órgãos também evolui quanto ao uso desta tecnologia.

Tratando-se das maiores tendências de governança dentre os entrevistados, destacam-se as questões relativas à Portaria GSI n.º 9/2018, 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, atualmente, não há controles implementados nas instituições para identificar se esta orientação está sendo executada propriamente pelos usuários.

Em seguida, ressalta-se a atenção para a 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, que, se estiverem fora do orçamento, podem gerar um impacto no funcionamento de sistemas críticos da organização.

Dentre os entrevistados, 3 instituições ainda não iniciaram o seu planejamento para estruturar uma governança específica de nuvem, enquanto os demais 7, 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 trafegados em nuvem com base em análises dos riscos elencados pelo Acórdão 1739/2015 do TCU.

4.2.2. Legislação e regulamentações

Quanto à legislação e regulamentações, 6 das instituições entrevistadas demonstraram maior relevância quando se tratam 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, e que correm o risco de armazenar informações em lugares considerados indevidos por sua classificação.

Destaca-se inclusive que a regulação atual implica em consequências negativas quanto a 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.

É afirmando pelo *E09* que a legislação possui posicionamento genérico quanto à regulamentação de uso de nuvem pelo poder público, e que ainda pode se desenvolver de forma a fomentar a evolução tecnológica do governo. O entrevistado complementa que gestores da administração pública federal se encontram receosos ao se fazer contratações de serviços em nuvem por conta da falta de especificidade da legislação atual, e por correr o risco de sofrerem auditoria por órgãos de controle como o TCU.

Já os demais 4 entrevistados se posicionam de maneira oposta, 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 acordam que, após a divulgação da IN 01/2019 pela Secretaria de Governo Digital do Ministério da Economia, que fomenta o uso de

nuvem por todas as instituições da esfera pública, a legislação está se adequando gradativamente para que o governo tenha mais abertura para se desenvolver tecnologicamente.

Atualmente as estratégias de gerenciamento de riscos sendo implementadas pelos entrevistados 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 1739/2015 para a implantação de quaisquer soluções em nuvem; e promovendo treinamentos para os diferentes departamentos quanto às questões de conformidade com as leis.

4.2.3. Conformidade e auditoria

Tratando-se dos temas relacionados à conformidade e auditoria, 7 dos entrevistados acreditam que a utilização de soluções em nuvem é mais adequada quando se trata das 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 se necessitar atender a alguma demanda de *e-discovery* ou auditoria.

Os demais 3 entrevistados demonstram receio com questões relativas à efetividade das funcionalidades ofertadas pelo provedor no caso de se avaliar a conformidade das instituições com a LGPD ou demais regulamentações referentes ao uso de nuvem.

O *E01* aponta questões quanto à forma que os órgãos categorizarão todas as informações trafegadas, as definindo como confidencial ou não, como também a efetividade de tal execução. O entrevistado levanta que é possível fazer a coleta de dados para a análise e verificar a aplicação das políticas em casos pontuais, por amostragem, porém não é uma forma conveniente para ser usada sempre em todos os casos.

Todos os respondentes concluem que não há um processo de verificação de conformidade com maturidade suficiente em suas instituições, na maioria dos casos por conta de que o ambiente ainda está em fase de testes com um número limitado de usuários.

Apesar do momento de adaptação, estão sendo implementadas estratégias para que sejam desenvolvidos processos mais estruturados. Dentre as ações que estão sendo executadas atualmente, destacam-se as exigências contratuais das instituições para que o provedor de

nuvem forneça as funcionalidades necessárias, como também a implementação de soluções de classificação automática de arquivos por meio da identificação de palavras-chave.

4.2.4. Continuidade dos negócios

Sobre os riscos relacionadas à continuidade dos negócios, os entrevistados evidenciaram, dentre outros, a finalização do contrato com o provedor. Tal fato pode ocorrer após uma série de fatores inerentes ao 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, e neste caso são considerados riscos de *Lock-in*.

É evidenciado pelo *E07* que podem ocorrer situações indesejadas quando se trata da transferência da responsabilidade de gestão da plataforma para o provedor de nuvem, em vez do próprio órgão possuir total controle quanto a sua manutenção. Neste contexto, o *E03* ressalta que atualmente enfrenta dificuldades com o seu provedor pois não é oferecida uma flexibilização para a personalização das configurações de backup de certos sistemas, que já são pré-determinadas pelo provedor e não possuem possibilidade de ajustes pelo órgão público.

Os entrevistados 05 e 06 apontam que em casos de falhas de conexão, indisponibilidade dos sistemas, degradação de performance e perda de dados são riscos altamente relevantes com potencial para causar a interrupção de suas atividades. Também é destacado pelo *E10* que, em casos que se necessitam de uma performance maior, a escalabilidade da capacidade computacional pode ser prejudicada se a instituição não possuir orçamento previsto para custear os recursos adicionais, consequentemente colocando em risco o funcionamento apropriado de seus serviços.

Dentre as instituições entrevistadas, 5 organizações já possuem 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 (*multicloud*) para possibilitar a portabilidade quando necessário; provisionamento de canais de conectividade com a internet secundários; e planos de contingência já estruturados no caso da interrupção de serviços essenciais para as entidades governamentais.

As outras 5 organizações entrevistadas ainda não possuem planos 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, estes órgãos públicos estão 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.

4.2.5. 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. Os entrevistados 03, 07 e 09 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.

Se tratando das estratégias das instituições entrevistadas, são evidenciadas táticas para reduzir a probabilidade de certos riscos, como a preferência do *E03* pelo uso apenas de Software como Serviço (SaaS) em vez de Infraestrutura como Serviço (IaaS), visto que no primeiro todos os aspectos de manutenção do ambiente, incluindo a segurança, são gerenciados pelo provedor, enquanto no segundo ainda há procedimentos que devem ser executados pelas instituições públicas para garantir a segurança do ambiente.

Ao se considerar o risco no uso de softwares de fontes públicas, o *E07* afirma que estão limitando as permissões de usuários que podem utilizar tais recursos, de forma que os detentores do acesso analisem e armazenem tais soluções em um repositório onde os demais usuários do órgão tenham acesso, formando uma biblioteca de *software* aprovada pela organização.

Ainda são elencadas estratégias atuais de normatização interna, como pelo *E05* a produção e implementação certificações referentes à segurança da utilização de nuvem, com o objetivo de orientar os variados departamentos da instituição a executar uma análise de risco mais aprofundada e recorrente quanto ao tema. Destaca-se inclusive o planejamento do *E09* de padronizar as arquiteturas de todos os serviços e tecnologias gerenciados pelo órgão, instituindo um comitê de segurança de informação com o objetivo de avaliar e mitigar questões relativas à segurança desde o desenvolvimento dos sistemas até a sua implementação.

As seis demais organizações entrevistadas afirmaram que ainda estão desenvolvendo as suas táticas para reforçar a segurança de seus ambientes em nuvem, visto que no momento estão em fase de testes ou no processo de aquisição. Nestes casos, as instituições evidenciaram que no momento 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.

4.2.6. 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, cinco instituições entrevistadas afirmam não possuir preocupações quanto ao isolamento de seus ambientes, acreditando-se 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 locais.

O entrevistado 10 também ressalta que, mesmo com a implementação de todas as funcionalidades de isolamento lógico nos servidores locais, em um caso em que a sala-cofre do órgão público seja acessada por um indivíduo não autorizado, existe a possibilidade de que ele tenha mais chances de acesso aos sistemas, fato que não é igualmente provável quando se considera a infraestrutura de um provedor de nuvem.

Quanto às estratégias para mitigar os riscos, as instituições entrevistadas afirmam praticar determinadas medidas para evitá-los, incluindo: a segmentação de acessos para funcionalidades de administração dos recursos; isolamento de ambientes de desenvolvimento, homologação e produção; e a construção de exigências em cláusulas contratuais para garantir que este fator de segurança seja gerenciado pelo provedor.

4.2.7. Gestão de identidade 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. O entrevistado 01 afirma que na sua organização a política atual de gestão de senhas é ultrapassada, em que se faz necessária à sua reestruturação com a implementação de serviços de controle mais eficientes.

O entrevistado *03* destaca que o processo de elaboração das políticas de acessos para os gestores dos serviços em nuvem é altamente demandante, considerando a granularidade de centenas de níveis de privilégios que precisam ser segmentados e reavaliados com recorrência, evidenciando o risco de não ser à prova de falhas por conta de sua complexidade. Segundo o *E05*, também é necessário considerar os riscos inerentes ao permissionamento de acessos por usuários externos ao órgão, que necessitam estar colaborando com os funcionários dentro do ambiente virtual da instituição.

Como parte das estratégias para a remediação dos riscos relacionados ao tema, todas as instituições pesquisadas afirmaram estar planejando ou 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 pelos entrevistados 1, 6 e 10 que ainda não foram implementadas soluções mais robustas de gestão de acessos, porém está sendo executado um plano de controle de acessos e identidade, e está previsto para ser tratado em futuras contratações, considerando os riscos inerentes ao tema.

4.2.8. 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 e pela Portaria GSI Nº 9/2018, afirmando que, por se tratarem de organizações governamentais, um vazamento pode acarretar em significativos problemas econômicos e políticos com impacto de nível nacional. Além do vazamento, também são considerados possíveis perdas de dados e o tratamento de tais por terceiros de maneira não autorizada conforme a legislação vigente.

O entrevistado 07 expõe outros receios também quanto à LGPD, em que se possui restrições de tratamento dos dados por sistemas distintos, inclusive pela reutilização dos dados em outras ocasiões, o que pode afetar a forma como a instituição gerencia seus negócios. Preocupa-se em interpretar a lei de maneira correta para que a instituição se mantenha em conformidade enquanto executa as suas atividades.

Além destes, é evidenciado também pelo *E10* que se atenta aos riscos do tratamento de dados sensíveis fora do território nacional, considerando a possibilidade de acesso às informações por outros governos ou entidades não autorizadas.

Trazendo a atenção para as próprias instituições públicas e seus funcionários, o entrevistado 09 cita a possível ocorrência de ataques de engenharia social, como o *phishing*, que consistem em enganar ou persuadir usuários a informar as suas credenciais de acesso à invasores, colocando em risco a proteção dos dados sensíveis do órgão.

No cenário atual da amostra desta pesquisa, todas as instituições ainda encontram-se desenvolvendo processos e práticas para garantir a proteção dos dados conforme a legislação. Dentre as táticas citadas, os entrevistados *03* e *07* afiram estar buscando apoio jurídico-legal para que as instituições se mantenham em conformidade por meio de serviços de consultoria para verificar a maturidade do órgão quanto a aderência aos requisitos das leis que tangem a proteção de informação. A partir dos resultados dessa consultoria, será elaborado um plano de trabalho que será priorizado pelo comitê de segurança.

Em meio às demais estratégias citadas pela amostra da pesquisa, estão: evitar o tráfego de informações não públicas em ambientes de nuvem; executar o tratamento de metadados de forma a evitar o vazamento de informação pessoal identificável; implementação de processos

de classificação das informações e 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 em questão.

4.2.9. Resposta à incidentes

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

Foi pontuado pelo entrevistado 08 que, inclusive, atualmente há riscos conexos à escassez de profissionais devidamente capacitados nas instituições para executar a gestão e manutenção de incidentes relativos a ambientes específicos em nuvem. Em casos em que não há mão de obra disponível para executar o tratamento de incidentes, o risco é consideravelmente maior.

Conforme exibido pelo entrevistado 10, preocupa-se também com riscos inerentes à velocidade de detecção e monitoramento de incidentes, em que os mecanismos de resposta devem ser rápidos e efetivos, levando em consideração ainda os prazos que os fornecedores de nuvem determinam para efetuar a comunicação de tais acontecimentos.

A respeito das estratégias dos entrevistados, em todos os casos não existem planos completamente estruturados quando se trata de tecnologias em nuvem, porém, conforme evidenciado por 5 entrevistados, estão se estabelecendo equipes dedicadas para de tratamento de incidentes com planos de comunicação e alertas definidos.

Em alguns casos, como na instituição do entrevistado 06, está sendo mantido um backup local e se executando testes com informações e sistemas menos críticos na nuvem para avaliar a execução dos planos de contingência. Já a organização 07 está buscando automatizar o tratamento de incidentes de indisponibilidade por meio de sistemas de abertura de chamados, com maior autonomia da equipe de suporte para o provisionamento de recursos mediante demanda.

Nos demais casos, conforme os entrevistados 10 e 04 que estão em processo de renovação contratual, estão sendo avaliados os riscos elencados pelo acórdão do TCU e classificados quanto à sua criticidade, buscando-se elencar tais questões no momento da contratação de forma a fazer requisições para que os provedores de nuvem disponibilizem recursos que auxiliem no tratamento de incidentes.

4.3. Análises dos dados da pesquisa

Cumprindo-se os objetivos a que este estudo se propôs, este capítulo trata das conclusões e das considerações finais, explorando os aspectos mais relevantes relacionados maturidade quanto ao uso de nuvem das instituições entrevistadas, como também de suas percepções quanto aos riscos inerentes ao uso destes ambientes pelo governo e as maiores tendências de práticas de gestão de riscos elencadas pelos entrevistados.

4.3.1. Maturidade de uso da nuvem

Ao analisar os perfis dos entrevistados quanto à maturidade de uso de nuvem, é possível apontar que, atualmente, predominam-se as instituições que estão utilizando esta tecnologia por 3 anos ou menos, e que ainda estão desenvolvendo a sua experiência com a gestão destes ambientes.

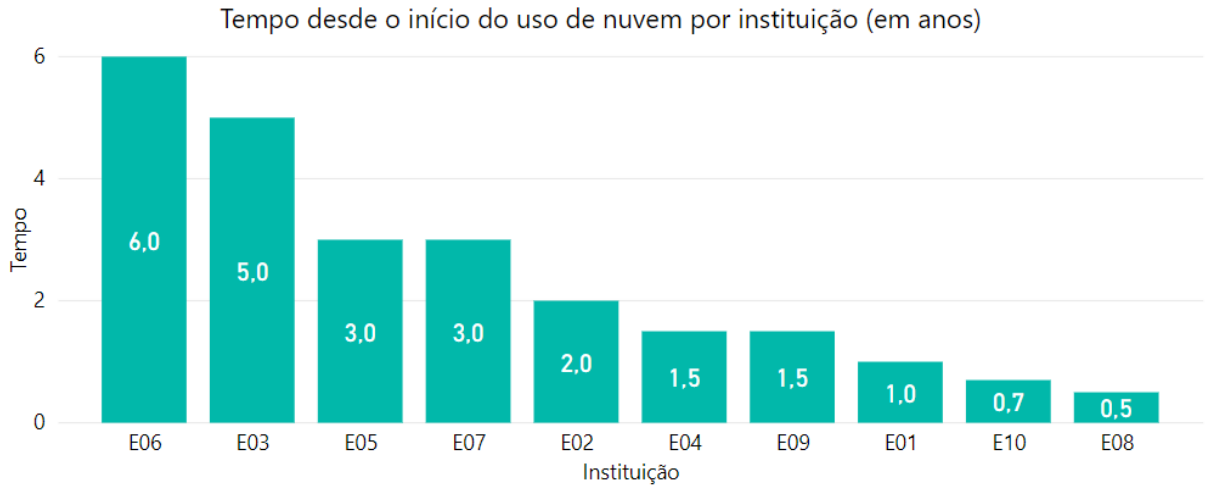


Gráfico 1 – Tempo de uso de nuvem pelas instituições participantes da pesquisa.

Complementado esta questão, as instituições ainda enfrentam 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 atual de transformação digital em que o governo se encontra.

Dentro da perspectiva dos órgãos que já possuem uma maturidade avançada neste aspecto, nota-se que estes estão hospedando diversos sistemas e utilizando ostensivamente as

funcionalidades oferecidas pela nuvem, de forma a tornar a gestão de TI mais eficiente quando se trata de custos e performance. Também foi apontado que os usuários destas instituições estão familiarizados com as plataformas de forma a usá-las em seu dia a dia, como nos casos em que há a possiblidade de teletrabalho.

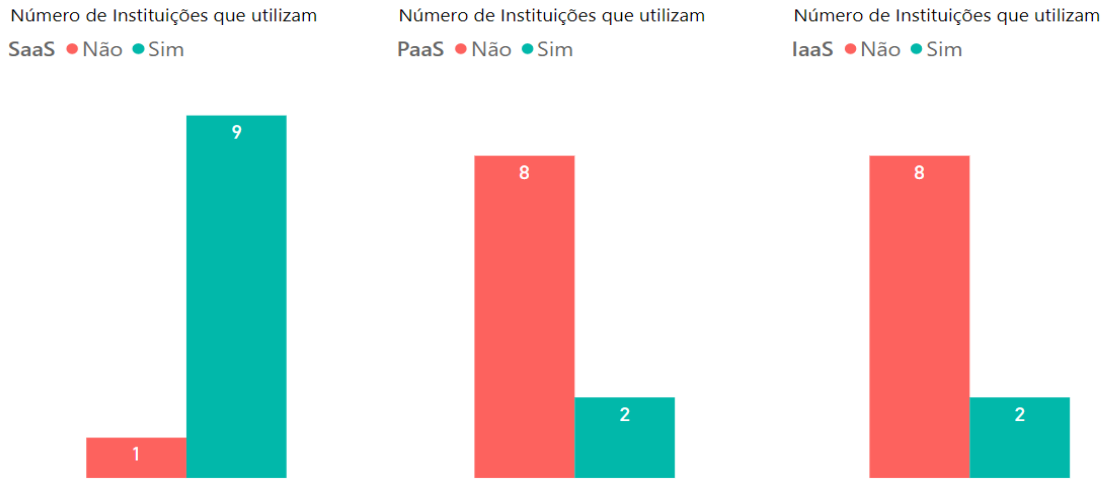


Gráfico 2 – Número de instituições participantes da pesquisa que utilizam IaaS, PaaS e SaaS.

Já os órgãos com adoção mais recente geralmente ainda se encontram executando testes e planejando as formas de alavancar a adoção destas plataformas pelos seus usuários, majoritariamente com uma abordagem de lançamento limitado à certos departamentos como forma de piloto. Tratando-se de hospedagem de sistemas na nuvem, é predominante nestas instituições o receio quanto ao fato de suas equipes ainda não possuírem conhecimentos técnicos avançados, e ainda se encontram testando os tais serviços.

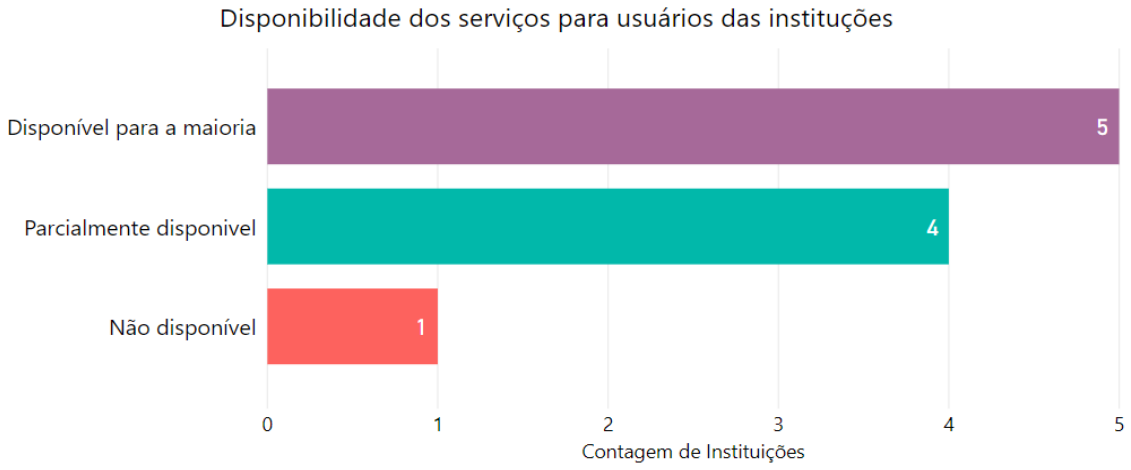


Gráfico 3 – Contagem de instituições participantes da pesquisa com a atual liberação dos serviços em nuvem para usuários.

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 para a sua implementação, está a mudança da cultura das organizações para adotar todas as soluções em nuvem que a princípio poucos possuem conhecimentos aprofundados.

4.3.2. Percepções dos riscos

Analisando-se os resultados da pesquisa, nota-se que as instituições entrevistadas majoritariamente acreditam nas vantagens dos aspectos segurança oferecidos pelos os ambientes de nuvem, 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 do modelo, ainda existem preocupações que exercem alta relevância nas considerações e planejamentos em torno da contratação de serviços de nuvem e da migração dos dados e sistemas governamentais para estes.

Dentre 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 a 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 à 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.

4.3.3. Tendências de gestão de riscos

Após avaliar os posicionamentos das organizações governamentais entrevistadas, é possível concluir que estas em sua maioria estão em fase de planejamento e estruturação dos seus processos voltados para mitigar os riscos levantados nos outros capítulos desta pesquisa.

Estes, que se encontram no momento de avaliação, são compostos pelos órgãos que estão utilizando as tecnologias em nuvem por um menor volume tempo, e que inclusive estão ainda testando tais soluções, e não chegaram ao ponto de efetivamente implementar estratégias robustas de gestão de riscos.

Apesar da baixa maturidade destas instituições quanto ao uso de nuvem, existem iniciativas em todas as entrevistadas para elaborar planos estruturados que tratam da gestão dos riscos, abordando principalmente questões em torno da contratação destes serviços. Para tais demandas, estão sendo instituídos comitês para executar a avaliação de riscos e os planejamentos de segurança, resposta a incidentes e demais atividades relacionadas.

Com os estudos e definições trazidas pelos comitês de análise de riscos, é ressaltado pelos entrevistados que a suas organizações estão elaborando cláusulas contratuais que exigem dos provedores a prestação de funcionalidades quanto aos temas em pauta, como por exemplo a gestão de acessos, isolamento de recursos críticos e portabilidade para outros provedores. Também é apontada a tendência de se adotar modelos de aquisição *multicloud*, em que há possibilidade de o órgão migrar os seus serviços para diversos provedores de acordo com a sua necessidade em um eventual incidente.

Com relação aos riscos no contexto das imposições regulatórias e legislativas, os órgãos entrevistados afirmam estar buscando apoio jurídico-legal por meio de consultorias, de forma a garantir a sua conformidade com as leis e para exigir recursos específicos dos provedores no momento das contratações e renovações.

A partir de tais posicionamentos, conclui-se que, embora estejam em fase inicial de sua transformação digital, 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 estudo objetivou explorar questões relevantes relativas a um tema atual e de importância crescente no campo de administração de empresas dentro do âmbito de Tecnologia da Informação: a computação em nuvem e a gestão de riscos relacionados ao seu uso, mais especificamente abordando a esfera da Administração Pública Federal.

Com os resultados da pesquisa, foi possível cumprir o objetivo de avaliar a situação atual das instituições que participaram do estudo, trazendo questões sobre a permeabilidade desta tecnologia no Governo Federal, sobre a maturidade no uso de tais soluções e a identificação das maiores tendências de gestão de riscos sendo praticadas por estas entidades governamentais.

Porém, este é um tema que ainda traz um certo desconforto aos executivos de TI do governo federal, principalmente quando se deparam com questionamentos acerca riscos que estão atrelados ao seu uso, com maior atenção ao tratamento de dados sensíveis.

Realmente, a computação em nuvem não é uma tecnologia simples de ser adotada. Opostamente, para adotá-la pode ser necessário enfrentar riscos de transposição complexa, os quais acabam por postergar a implementação pelas entidades governamentais.

Porém, atualmente o Governo Federal encontra-se em estado de grandes mudanças, caminhando cada vez mais na direção da transformação digital com a implementação de tecnologias inovadoras, como pode ser evidenciado com o anúncio da Instrução Normativa nº 01 do dia 4 de abril de 2019, em que se incentiva a expansão para a nuvem e o abandono da cultura de se investir em infraestrutura local.

Apesar do governo se posicionar a favor de sua transformação, ainda há um longo caminho a ser percorrido, principalmente quanto trata-se da estruturação de regulamentações eficientes, que não gerem empecilhos na jornada que as organizações públicas estão seguindo para se modernizar. Em um cenário ideal, tais tecnologias trarão uma maior eficiência para a máquina pública, onde há oportunidade de se reduzir gastos à medida que se eleva a performance das atividades do governo que, em breve, poderá ter o potencial de se tornar um governo completamente digital, como já é realidade em certos países desenvolvidos.

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 trais mudanças da máquina pública. Como contribuição maior, este estudo oferece, acima de tudo, uma visão acerca do posicionamento do governo quanto à computação em nuvem, e coloca à disposição daqueles que efetivamente por ela se interessam, por vontade própria ou dever de ofício, um rol de observações sobre a situação contemporânea no cenário de gestão de riscos de TI no Brasil.

REFERÊNCIAS BIBLIOGRÁFICAS

AGYEI-MENSAH; KWAME, B. **Impact of Adopting IFRS in Ghana: Empirical Evidence in Economics and Political Implications of International Financial Reporting Standards.** Hershey: IGI Global, 2016.

ANDERSON, K; TERP, A. **Risk Management, Andersen T.J. (ed.), Perspectives on Strategic Risk Management.** Denmark: Copenhagen Business School Press, 2016.

ARMBRUST; MICHAEL et al. **Above the clouds: a Berkeley view of cloud computing. Technical Report No. UCB/EECS-2009-28**. Berkeley, CA (US): University of California, Berkeley – Electrical Engineering and Computer Sciences, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000:2009 – Gestão de Riscos: Princípios e Diretrizes.** Segunda edição. Rio de Janeiro: ABNT, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001: Tecnologia da Informação, técnicas de segurança, sistemas de gestão de segurança da informação, requisitos**. Rio de Janeiro: ABNT, 2006.

ÁVILA. **Gestão De Riscos No Setor Público: Controle Estratégico Para Um Processo Decisório Eficiente**. Fortaleza: Revista Científica Semana Acadêmica, 2013.

BANDYOPADHYAY, SUBHAJYOTI et al. **Cloud computing: the business perspective.** Florida, Estados Unidos: University of Florida, 2009.

BARAFORT et al. **Integrating risk management in IT settings from ISO standards and management systems perspectives**. Amsterdã, Holanda: Computer Standards & Interfaces, 2017.

BARRETO, L. C. **Gerenciamento de riscos em projetos da administração pública: características, requisitos e possibilidades de melhoria para o estado de minas gerais**. Brasília: CONSAD, 2009.

BEAL, A. **Segurança da Informação. Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações.** São Paulo: Atlas, 2005.

BERG, H. P. **Risk management: Procedures, methods and experiences**. Salzgitter, Alemanha: RT&A, 2010.

BRASIL. **Acórdão Nº 1739/2015**. Brasília, DF: Tribunal de Contas da União, 2015.

BRASIL. **Circular nº 3.909, de 16 de agosto de 2018**. Brasília, DF: Banco Central do Brasil, 2018.

BRASIL. **Decreto nº 7.845 de 14 de novembro de 2012**. Brasília, DF: Casa Civil - Subchefia para Assuntos Jurídicos, 2012.

BRASIL. **Instrução Normativa nº 1, De 4 De Abril De 2019 do Ministério da Economia/Secretaria Especial de Desburocratização, Gestão e Governo Digital/Secretaria de Governo Digital**. Brasília, DF: Diário Oficial da União, 2019.

BRASIL. **Lei nº 12.527 de 18 de novembro de 2011. Lei de acesso à informação**. Brasília, DF: Casa Civil - Subchefia para Assuntos Jurídicos, 2011.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados**. Brasília, DF: Casa Civil - Subchefia para Assuntos Jurídicos, 2018.

BRASIL. **Portaria GSI nº 9 de 15 de março de 2018**. Brasília, DF: Gabinete de Segurança Institucional da Presidência da República, 2018.

BRASIL. **Resolução nº 4.658, de 26 de abril De 2018**. Brasília, DF: Banco Central do Brasil, 2018.

BURLESON, D.R.; LEVINE, B.J; SAMTER, W. **Decision making and decision quality**. Estados Unidos da América: Human Communication Research, 2006.

CAIÇARA, J. **Informática, Internet e Aplicativos**. 1 ed. Paraná, Brasil: IBPEX, 2007.

CAMERON, D.; KNEALE, P.; SEE, L. **An evaluation of a traditional and a neural net modelling approach to flood forecasting for an upland catchment.** Leeds, Reino Unido: Hydrological Processes, 2002.

CAPRINO; OKUHARA, W.; CABRAL, C. **Trilhas em Segurança da Informação: Caminhos e ideias para a proteção de dados**. 1ª ed – Rio de Janeiro: Brasport, 2015.

CIENFUEGOS, I. J. **Developing a risk management maturity model: a comprehensive risk maturity model for Dutch municipalities**. Enschede, Holanda: Universiteit Twente, 2013.

CÔRTE, K. **Segurança da informação baseada no valor da informação e nos pilares tecnologia, pessoas e processos.** Brasília: Universidade de Brasília, 2014.

COSO (COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION). **Gerenciamento de Riscos Corporativos - Estrutura Integrada**. Edição brasileira. São Paulo: PriceWaterhouseCoopers, 2007.

CSA (CLOUD SECURITY ALLIANCE). **Security Guidance for Critical Areas of Focus in Cloud Computing.** Versão 4.0. Seattle, Estados Unidos: CSA, 2017.

DAYANANDA et al. **Capital Bidgeting**. Cambridge, Reino Unido: Cambridge University Press, 2002.

DELOITTE. **Cloud growth focused on IaaS, and IaaS and PaaS combined.** Estados Unidos: Deloitte on Cloud, 2018.

EISENHAUER, M. P. **Privacy and Security Law Issues in Off-shore Outsourcing Transactions**. Estados Unidos: Hunton & Williams LLP, 2005.

ENISA (EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY). **Cloud Computing: benefits, risks and recommendations for information security**. Heraklion, Grécia: ENISA, 2009.

EUROSTAT. **Cloud computing - statistics on the use by enterprises.** Luxemburg: Eurostat Statistics Explained, 2018.

FONTES, E. **Praticando a segurança da informação**. Rio de Janeiro: Brasport, 2010.

GARTNER. **Forecast Analysis: Public Cloud Services, Worldwide, 2Q18 Update.** Estados Unidos: Gartner, 2018.

GERHARDT, T. E.; SILVEIRA, D. T. **Métodos de Pesquisa.** Porto Alegre: Universidade Federal do Rio Grande do Sul, 2009.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2007

GOLDENBERG, M. **A Arte de Pesquisar: como fazer pesquisa qualitativa**. Rio de Janeiro: Record, 1997.

GREGORIO, D. **Re-thinking country risk: insights from entrepreneurship theory.** Albuquerque, Estados Unidos da América: International Business Review, 2005.

GRIFFITH, E. **What Is Cloud Computing?** Estados Unidos: PCMAG, 2015.

KIM, W. **Cloud computing: today and tomorrow. Journal of Object Technology**. Zurich, Alemanha: ETH Zurich, 2009.

KITCHIN R.; TATE N. J. **Conducting Research in Human Geography: theory, methodology and practice**. Estados Unidos: Routledge, 2000.

KNECHEL, W. R.; SALTERIO, S. E. **Auditing: Assurance and Risk**. Abingdon, Reino Unido: Routledge, 2016.

KRUEGER, R. A.; CASEY, M. A. **Focus Groups: A Practical Guide for Applied Research.** 3rd ed. Thousand Oaks, Estados Unidos: Sage, 2000.

LONGHURST, R. **Key Methods in Geography: Semi-structured Interviews and Focus Groups**. Londres: SAGE, 2010

MCDONALD, Steve. **Legal and Quasi-Legal Issues in Cloud Computing Contracts, Workshop Document, EDUCAUSE and NACUBO Workshop on Cloud Computing and Shared Services**. Tempe, Estados Unidos: 2010.

MCPHEE, I. **Risk and risk management in the public sector**. Canberra, Austrália: Australian National Audit Office, 2005.

MELL, P.; GRANCE, T. **The NIST Definition of Cloud Computing: Special Publication 800-145**. Gaithersburg, Estados Unidos: U.S. Department of Commerce, 2011.

MILES, M.; HUBERMAN, A. **Qualitative Data Analysis**. Londres, Reino Unido: Sage, 1994

MILLER, M. **Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online**. Estados Unidos: Que, 2008.

MINAYO, M. C. S. **Pesquisa social: teoria, método e criatividade**. Petrópolis: Vozes, 2001.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **The NIST Definition of Cloud Computing**. Estados Unidos: US Department of Commerce, 2011.

QIAN, L. et al. **Cloud computing: an overview**. Pequim, China: 2009 *apud* JAATUN, M G. et al. **Proceedings of the 1st Conference on Cloud Computing (Lecture Notes in Computer Science)**. Heidelberg: Springer, 2009.

ROWE, B. R. **Will Outsourcing IT Security Lead to a Higher Social Level of Security?** Estados Unidos: Research Triangle Institute International, 2007.

SMITH, R. **Computing in the cloud.** Estados Unidos: Research-Technology Management**,** 2009.

SOBEY, et al. **Drive-Independent Data Recovery: The Current State-of-the-Art**. Estados Unidos: IEEE Transactions on Magnetics, 2006.

SOMMERVILLE, I. **Engenharia de Software**. 8 ed. São Paulo: Editora Pearson Addison Wesley, 2007.

STRATEGY UNIT. **Risk: Improving government's capability to handle risk and uncertainty**. Londres: Strategy Unit, Cabinet Office, 2002.

TANG et al. **Incentives in the Chinese Construction Industry**. Estados Unidos: Journal of Construction Engineering and Management, 2007

TAURION, C. **Cloud computing: computação em nuvem: transformando o mundo da Tecnologia da Informação**. Rio de Janeiro: Brasport, 2009.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679** do Parlamento Europeu e do Conselho da União Europeia de 27 de abril de 2016: Regulamento Geral sobre a Proteção de Dados (GDPR). Bruxelas, Bélgica: Jornal Oficial da União Europeia, 2016.

VALENTINE, G. Tell me about using interviews as a research methodology *apud* FLOWERDEW R.; MARTIN D. **Methods in Human Geography: A Guide for Students Doing a Research Project** (2nd edn). Edinburgh Gate: Addison Wesley Longman, 2005.

VALLI C.; WOODWARD A. **The 2008 Australian Study of Remnant Data Contained on 2nd Hand Hard Disks: The Saga Continues**, Perth, Australia: The 6th Australian Digital Forensics Conference, 2008.

VERAS, M. **Cloud Computing: nova arquitetura da TI**. Rio de Janeiro: Brasport, 2012.

WEICHERT, T. **Cloud Computing and Data Privacy.** Estados Unidos: The Sedona Conference**,** 2011.

WEISS, A. **Computing in the clouds.** Nova York, Estados Unidos: Association for Computing Machinery (ACM), 2007.

ZAPATER, M.; SUZUKI, R. **Segurança da Informação: Um diferencial determinante na competitividade das corporações.** São Paulo: Promon Business & Technology Review, 2005

ZINS, A.; WEILL L. **Islamic banking and risk: The impact of Basel II**. França: Economic Modelling, 2017.

APÊNDICES

1. Apêndice 1: Questionário de Entrevista

MATURIDADE NO USO DE NUVEM

1. Hoje a sua instituição utiliza serviços ou soluções baseados 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?

SOBRE OS RISCOS DE USO NA NUVEM

1. Quais são as maiores preocupações da organização quanto ao uso de nuvem e seus riscos?

PEROTEÇÃO DE DADOS

1. Quais são as maiores preocupações da organização quanto a 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 este assunto?

LEGISLAÇÃO E REGULAMENTAÇÕES

1. Você enxerga riscos à 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?

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?

CONFORMIDADE E AUDITORIA

1. Você enxerga riscos à sua organização referentes à conformidade e auditoria relacionados ao uso de sistemas em nuvem?

2. Existe um planejamento para lidar com tais riscos?

CONTINUIDADE DOS NEGÓCIOS

1. Quais são as maiores preocupações quanto a riscos do uso de nuvem que possam impedir as atividades da instituição?

2. Existe um planejamento para lidar com tais riscos?

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?

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?

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 estes riscos?

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?