MELHORES PRÁTICAS PARA A ADOÇÃO DE BACKUP EM NUVEM POR ÓRGÃOS DO PODER LEGISLATIVO FEDERAL[1]

Eduardo Ferraz dos Santos

Resumo: A adoção de *backup* em nuvem, com suas características de onipresença e amplo acesso pela rede, além do seu modelo de custo proporcional ao uso, é uma alternativa promissora para o armazenamento dos *backups* de dados e sistemas pelos órgãos da Poder Legislativo Federal. Tal adoção pela Administração Pública, entretanto, deve seguir uma série de dispositivos legais que dispõe sobre a segurança das informações e a continuidade de negócios. O presente artigo apresenta uma análise de tais dispositivos legais, em conjunto com um estudo sobre *backup* em nuvem e continuidade de negócios e com um levantamento das particularidades de *backup* de um órgão do Poder Legislativo Federal, com o objetivo de identificar as melhores práticas a serem seguidas para a adoção de *backup* em nuvem. Tal pesquisa permitiu a proposição alguns ajustes a serem considerados em suas políticas de *backup*, além de algumas recomendações adicionais.

Palavras-chave: Backup em nuvem. Gestão de continuidade de negócios. Melhores práticas. Poder Legislativo Federal.

1 INTRODUÇÃO

Segundo Lento (2014), antecipar-se aos possíveis incidentes e desastres é um dos maiores diferenciais para o sucesso das organizações. E a capacidade de se responder de maneira eficaz e eficiente aos incidentes e desastres é alcançada implementando-se uma gestão de continuidade de negócios.

A gestão de continuidade de negócios é um assunto amplamente tratado por normas brasileiras e internacionais, como a norma ABNT NBR ISO 22313:2015 – orientações com base em boas práticas internacionais, e a norma ABNT NBR ISO 22301:2013 – requisitos, ambas sobre o planejamento, criação, implantação, operação, monitoramento, análise crítica, manutenção e melhoria contínua de um sistema de gestão de continuidade de negócios

[1] Artigo apresentado como Trabalho de Conclusão do Curso de Especialização em Gestão de Segurança da Informação, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Gestão de Segurança da Informação.

documentado, que permita que as organizações se preparem para responder e se recuperar de incidentes de interrupção quando eles surgirem.

Dentre os procedimentos de continuidade de negócios, o foco deste estudo se concentra nos procedimentos de recuperação de desastres – aqueles que restabelecem as atividades de negócio de forma a suportarem as atividades normais da organização após a ocorrência de um desastre (ABNT, 2015) – e, mais especificamente, nas estratégias de *backups*.

De fato, já é de conhecimento entre os profissionais de TI que possuir um plano de *backup* é fundamental para a proteção dos dados e continuidade de negócios (MORAES, 2007). E dentre as melhores práticas para a implementação de planos de *backup*, há a indicação de que as cópias de segurança sejam armazenadas em localidades remotas, suficientemente distantes para escapar de um desastre ocorrido no local onde ficam armazenados os dados primários (ABNT, 2013b).

Escolher um local remoto, seguro e financeiramente viável para se armazenar as cópias de segurança de dados e sistemas não é uma tarefa fácil. E uma das alternativas a serem consideradas nessa escolha é o armazenamento de *backup* em nuvem. Isso porque a computação em nuvem é um modelo que se caracteriza pela onipresença e amplo acesso pela rede, pela capacidade de rápida elasticidade e auto provisionamento de recursos, pelo uso compartilhado de recursos e por serviços medidos por utilização (MELL, 2011).

No que diz respeito à adoção de *backup* em nuvem pela administração pública, o TCU (2015, pg. 12) considera que "é uma solução mais simples [que o *backup* tradicional *on-site*], ressalvando-se que depende de banda de internet suficiente para tal". Isso porque os dados já seriam armazenados "em um local remoto, seguro, disponível, com capacidade de expansão de espaço automática, intrínseca à escalabilidade característica da computação em nuvem".

Apesar disso, o TCU identificou que a utilização de computação em nuvem não tem sido incluída no planejamento dos gestores no âmbito da administração pública federal. Isso porque (TCU, 2015, pg. 41):

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

De fato, no que diz respeito à Administração Pública, é notório que qualquer contratação de produtos ou serviços deve ser realizada seguindo as determinações da Lei 8.666/93. Mas há também outros dispositivos legais que, embora nem sempre tão conhecidos, também devem ser

considerados pela Administração Pública ao se planejar a contratação de serviços de computação em nuvem.

Esse estudo teve como objetivo identificar as melhores práticas que devem ser seguidas pelos órgãos do Poder Legislativo Federal para a adoção de *backup* em nuvem, considerando tanto a particularidade de suas atribuições quanto o alinhamento com a legislação e jurisprudência vigentes.

Para alcançar esse objetivo, buscou-se: identificar as melhores práticas para a realização e restauração de *backups*; analisar as vantagens e preocupações a serem consideradas na adoção de *backups* em nuvem; identificar as leis, acórdãos, normas e demais dispositivos legais que dispõe sobre a utilização de computação em nuvem pela Administração Pública; e levantar particularidades dos órgãos do Poder Legislativo Federal que sejam relevantes para a adoção de *backups* em nuvem.

Esse estudo foi motivado pela necessidade de identificação das melhores práticas a serem seguidas por um órgão do Poder Legislativo Federal ao considerar a adoção do *backup* em nuvem em total alinhamento com os dispositivos legais vigentes, o que o caracteriza, segundo Will (2016), como uma pesquisa aplicada.

O foco principal da pesquisa foi o levantamento e estudo das melhores práticas já consolidadas para o gerenciamento de *backups*, das vantagens e preocupações relacionadas à adoção de computação em nuvem e dos instrumentos normativos que afetem a contratação de serviços em nuvem pela Administração Pública. A bibliografia e as leis pesquisadas foram correlacionadas para que fosse possível identificar as melhores práticas que devem ser seguidas por um órgão do Poder Legislativo Federal ao considerar a adoção do *backup* em nuvem, o que a caracteriza, segundo Will (2016), como uma pesquisa teórica e exploratória.

A pesquisa também tem um componente empírico. Existem particularidades nas atribuições do Poder Legislativo Federal que influenciam a identificação das melhores práticas a serem seguidas. Tais particularidades foram diretamente coletas a partir de um estudo de caso, por meio de entrevistas realizadas com o chefe do setor de TI responsável pelo gerenciamento de backups corporativos, com o coordenador da área de infraestrutura de TI e com o diretor da área de TI da casa legislativa em questão.

O presente artigo está organizado em mais 3 seções subsequentes. Na seção 2 é apresentado um referencial teórico sobre *backup*, computação em nuvem e continuidade de serviço. Na seção 3 é apresentada uma análise dos dispositivos legais que devem ser considerados pela Administração Pública na adoção de *backup* em nuvem, além das

particularidades identificadas em um órgão do Poder Legislativo Federal, resultando na sugestão de melhores práticas que podem ser seguidas. Na seção 4 são apresentas as conclusões dessa pesquisa. Ao final do artigo há ainda 3 apêndices com as transcrições das entrevistas realizadas.

2 BACKUP

2.1 BACKUP E SUAS MELHORES PRÁTICAS

Já é de conhecimento entre os profissionais de TI que possuir um plano de *backup* é fundamental para a proteção dos dados e continuidade de negócios (MORAES, 2007).

Backups podem ser utilizados não só para a restauração de dados ou sistemas na ocorrência de desastres ou outros incidentes de segurança, mas também para a recuperação de versões anteriores de dados, ou ainda para o arquivamento de dados ainda necessários, mas raramente acessados (CERT.br, 2012). Minimamente, para a realização de *backups* é necessário que se decida quais dados serão copiados, bem como em qual lugar e com qual frequência.

Os métodos e estratégias de *backups* já foram motivo de estudo de vários autores e organizações, dando origem a várias recomendações de melhores práticas já amplamente divulgadas. Destacamos as melhores práticas recomendadas na Cartilha de Segurança para a Internet publicada pelo CERT.br (2012, item 7.5), no boletim do *Information Technology Laboratory* publicado pelo NIST (2002), na norma ABNT ISO/IEC 27002:2013 (ABNT, 2013b), e por Moraes (2007, item 2.4).

Uma estratégia de *backup* realmente eficaz deve ser muito bem planejada. Para isso, Moraes (2007) propõe a realização de um planejamento em quatro etapas bem definidas – conscientização da necessidade de *backup* de dados, definição dos responsáveis pelo planejamento, disponibilização de recursos e determinação das ações a serem planejadas, com a definição de um plano de *backup* – com o envolvimento de todas as áreas da organização e em integração com a política de segurança da informação e com o plano de continuidade de negócios da organização.

2.2 BACKUP COMO ESTRATÉGIA DE CONTINUIDADE DE NEGÓCIOS

A continuidade de negócios diz respeito à capacidade das organizações em responder aos incidentes ou desastres que prejudiquem substancialmente ou mesmo interrompam completamente as suas operações. Nessas situações, as organizações devem ser capazes de

continuar a ofertar seus produtos e serviços prioritários, em níveis mínimos aceitáveis e previamente definidos.

Durante o planejamento da gestão de continuidade de negócios, deve-se (ABNT, 2013a) determinar estratégias de continuidade adequadas para: proteger as atividades prioritárias; estabilizar, continuar, retomar e recuperar as atividades priorizadas, bem como suas dependências e recursos de apoio; e mitigar, responder e gerenciar impactos.

As estratégias de continuidade de negócios podem se enquadrar como sendo de contenção – as que buscam conter a propagação dos danos; de erradicação – as que buscam a eliminação das causas dos incidentes; e de recuperação – as que buscam a restauração do funcionamento normal das operações (LENTO, 2014). E a restauração de *backups* de dados e sistemas é uma das principais ações a serem tomadas ao se adotar uma estratégia de recuperação.

A adoção de *backups* como parte da estratégia de continuidade de negócios da organização deve ser feita em alinhamento com seu processo de análise de impacto nos negócios (*BIA – Business Impact Analysis*).

A análise de impacto nos negócios é um processo que busca determinar as prioridades de continuidade e recuperação dos negócios, devendo incluir (ABNT, 2013a, seção 8.2.2): a identificação das atividades que suportam o fornecimento de produtos e serviços; a avaliação dos impactos ao longo do tempo de não se realizar essas atividades; a fixação de prazos para a retomada dessas atividades, num nível mínimo de execução tolerável, considerando-se os tempos em que os impactos dessas interrupções se tornam inaceitáveis; e a identificação das dependências e recursos que suportam essas atividades.

Uma estratégia de *backup* alinhada com a análise de impacto nos negócios deve levar em consideração dois fatores essenciais: o *Recovery Point Objective* (RPO) e o *Recovery Time Objective* (RTO). O RPO define a quantidade de dados, em unidades de tempo, que a organização aceita ser perdida na ocorrência de um desastre, sendo fundamental para a determinação da frequência com que os *backups* serão feitos. Já o RTO define quanto tempo a organização aceita esperar pela recuperação de seus dados e sistemas após a ocorrência de um desastre, sendo fundamental para a determinação do modelo de armazenamento dos *backups*.

2.3 COMPUTAÇÃO EM NUVEM

Uma das possibilidades atuais de armazenamento de *backups* é na nuvem. O NIST define a computação em nuvem como sendo (MELL, 2011, tradução nossa)

> um modelo que permite o acesso, através da rede e de forma ampla, conveniente e sob demanda, a um conjunto de recursos computacionais configuráveis, (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente provisionados e liberados com um mínimo de esforço de gerenciamento ou de interação com o provedor de serviços.

A computação em nuvem é normalmente comercializada seguindo os três modelos de serviço definidos pelo NIST:

- Software como serviço (*SaaS – Software as a Service*) – quando o cliente utiliza aplicações do provedor hospedadas na infraestrutura de nuvem do próprio provedor. Tais aplicações tem a característica de serem acessíveis por diferentes tipos de dispositivos, por meio de um navegador web ou mesmo por um software específico;
- Plataforma como serviço (*PaaS – Platform as a Service*) – quando o cliente utiliza a infraestrutura de nuvem do provedor para implantar aplicações criadas pelo próprio cliente, ou adquiridas de terceiros, seguindo as linguagens de programação, bibliotecas, serviços e ferramentas suportadas pelo provedor;
- Infraestrutura como serviço (*IaaS – Infrastructure as a Service*) – quando o cliente tem a capacidade de provisionar os recursos computacionais (como armazenamento, processamento e rede) onde poderá implantar e executar qualquer tipo software, incluindo o sistema operacional e as aplicações de sua escolha, tudo isso na infraestrutura de nuvem do provedor.

Dependendo do modelo de implantação da sua infraestrutura, pode ainda ser classificada como (MELL, 2011) como:

- Nuvem privada – para o uso exclusivo de uma única organização;
- Nuvem comunitária – para o uso exclusivo de uma comunidade formada por organizações que possuem objetivos em comum;
- Nuvem pública – para o uso do público em geral;
- Nuvem híbrida – composta por duas ou mais infraestruturas de nuvem distintas (privada, comunitária ou pública) que se mantém independentes, mas que se interligam por meio de alguma tecnologia que permita a portabilidade de aplicações e de dados entre as nuvens.

As principais vantagens da adoção de computação em nuvem são decorrentes dos ganhos de escala: ao se consolidar datacenters isolados como um grande pool de recursos computacionais compartilhados, reúne-se um conjunto muito maior de recursos que podem ter seus custos unitários reduzidos, enquanto melhora seu aproveitamento e balanceamento de

demandas pelos diversos clientes, otimizando o nível de uso dos recursos e dividindo os custos fixos de manutenção por uma base maior de usuários (TCU, 2015).

No caso da Administração Pública, é importante destacar que o TCU (2015) considera que a computação em nuvem permite também uma maior agilidade na entrega de serviços e em sua atualização tecnológica, o suporte a iniciativas de abertura de informações governamentais, o atendimento a picos de demanda sazonal sem a necessidade de alocação prévia de grandes recursos fixos, a redução de desvios e irregularidades, e a agilidade e economia na entrega de serviços para órgãos com unidades descentralizadas.

2.4 BACKUP EM NUVEM E SUAS MELHORES PRÁTICAS

As vantagens da adoção do modelo de computação em nuvem para o armazenamento de *backups* foram muito bem descritas pelo Tribunal de Contas da União (TCU, 2015, pg. 12):

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

O CERT.br (2012) indica um conjunto de melhores práticas a serem consideradas ao se utilizar serviços de *backup online*, que são igualmente aplicáveis ao *backup* em nuvem:

- Observar a disponibilidade do serviço;
- Observar os tempos estimados para a realização e recuperação dos *backups*, considerando a largura de banda disponível e a quantidade de dados a serem transmitidos. Dependendo desses tempos, o *backup online* pode se tornar inviável;
- Considerar o tempo de manutenção dos dados, o espaço disponível de armazenagem e as políticas de privacidade e de segurança do fornecedor do serviço;
- Utilizar criptografia na transmissão de dados para o provedor de serviços.

2.5 BACKUP EM NUVEM E CONTINUIDADE DE NEGÓCIOS

Considerando os valores de RPO e RTO estabelecidos para os dados e sistemas prioritários da organização durante seu processo de análise de impacto nos negócios, a Opus Software (2015) sugere dois possíveis modelos de implementação de recuperação de desastres baseados em *backup* na nuvem e voltados para a continuidade dos negócios:

- *Backup* na nuvem (*cold start*) – nesse modelo o *backup* da infraestrutura primária da organização é armazenado na nuvem, podendo ser então restaurado para uma infraestrutura secundária da própria organização;
- *Backup* e infraestrutura secundária na nuvem (*warm start*) – nesse modelo tanto o *backup* quanto a infraestrutura secundária ficam na nuvem. Em caso de desastres, essa infraestrutura secundária entra em operação com o *backup* dos dados que se encontra na própria nuvem, possibilitando o atendimento de baixos valores de RTO.

3 ANÁLISE DOS DISPOSITIVOS LEGAIS E PARTICULARIDADES DO PODER LEGISLATIVO FEDERAL

A adoção de computação em nuvem e, em particular, de *backup* em nuvem pela Administração Pública é foco de considerações adicionais de segurança da informação e de continuidade de negócios, assunto que é tratado por uma série de dispositivos legais.

3.1 ANÁLISE DOS DISPOSITIVOS LEGAIS

O caso de Edward Snowden, que foi prestador de serviço da NSA (*National Security Agency*) e revelou um esquema de espionagem de dados por parte do governo dos EUA, incluindo a comunicação pessoal de chefes de estado, resultou numa preocupação do governo brasileiro com a segurança de suas informações e comunicações (TCU, 2015).

Tal preocupação se manifesta num conjunto de dispositivos legais que regulamentam a contratação tanto de serviços de comunicação quanto de computação em nuvem pelos órgãos da Administração Pública: Decreto nº 8.135/2013 (Brasil, 2013), Portaria Interministerial MP/MC/MD nº 141/2014 (Brasil, 2014b), Instrução Normativa GSI/PR Nº 1/2008 (Brasil, 2008), Norma Complementar 14/IN01/DSIC/GSIPR (Brasil, 2018), Norma Complementar 19/IN01/DSIC/GSIPR (Brasil, 2014a), Portaria MP/STI Nº 20/2016 (Brasil, 2016), Boas práticas, orientações e vedações para contratação de Serviços de Computação em Nuvem (MPOG, 2016) – vinculado à Portaria MP/STI Nº 20/2016, e Acórdão 1.739/2015-TCU-Plenário (TCU, 2015).

Em síntese, tais dispositivos legais estabelecem que:

- Deve-se avaliar previamente quais informações serão hospedadas na nuvem, considerando: a classificação da informação, o valor do ativo de informação, os controles de acesso físicos e lógicos, o modelo de computação em nuvem a ser

adotado e a localização geográfica onde as informações serão fisicamente armazenadas;

- Deve-se armazenar os dados e informações exclusivamente em território nacional, incluindo suas réplicas e *backups*, de forma que a Administração Pública disponha de todas as garantias previstas na legislação brasileira, que deve sempre prevalecer sobre qualquer outra;
- É vedado o tratamento de informações em ambientes de computação em nuvem não autorizados pela alta administração do respectivo órgão;
- A alta administração do órgão é a responsável pela definição das informações e serviços de TI que, no todo ou em parte, possam comprometer a segurança nacional;
- Informações e serviços de TI que possam comprometer a segurança nacional devem ser hospedados por serviços de TI próprios de cada órgão (sem a contratação de terceiros) ou em ambientes de computação em nuvem fornecidos por órgãos ou entidades da Administração Pública Federal;
- Informações e serviços de TI relativos aos sistemas estruturantes da Administração Pública (Brasil, 2014a, item 3.9) poderão ser hospedados em nuvem somente nos modelos de nuvem própria ou nuvem comunitária, desde que restritas às infraestruturas dos órgãos ou entidades da administração pública federal;
- Demais informações e serviços de TI que não comprometam a segurança nacional podem ser hospedados em ambientes de computação em nuvem fornecidos por órgãos públicos ou privados, preferencialmente no modelo de nuvem híbrida;
- Deve-se evitar o tratamento de informações sigilosas em ambiente de computação em nuvem;
- Deve-se respeitar a seguinte ordem de prioridade ao se contratar serviços de computação em nuvem: Software como Serviço (SaaS), Plataforma como Serviço (PaaS) e Infraestrutura como Serviço (IaaS);
- Deve-se assegurar que o serviço de nuvem a ser contratado permita a portabilidade de dados e serviços, estando disponíveis para transferência de localização, de modo a garantir a continuidade de negócios e as transições contratuais.

Além disso, os dispositivos legais reforçam que a adoção de computação em nuvem deve estar alinhada com as diretrizes estabelecidas pela política de segurança da informação e

pelos processos de gestão de riscos de segurança da informação e de gestão de continuidade de negócios de cada órgão.

3.2 PARTICULARIDADES DA ADOÇÃO DE BACKUP EM NUVEM POR UM ÓRGÃO DO PODER LEGISLATIVO FEDERAL

Para identificar particularidades da adoção de *backup* em nuvem por um órgão do poder legislativo federal, foram realizadas entrevistas aos seus profissionais de TI diretamente envolvidos na definição das políticas de segurança da informação e continuidade de negócios do órgão, bem como da política de *backup* e de sua implementação e operação.

Para os entrevistados, a maior vantagem da adoção de computação em nuvem no órgão seria a maior racionalidade no uso dos recursos públicos, tanto financeiros quanto humanos. Os recursos financeiros seriam gastos na mesma proporção das necessidades dos serviços, de forma mais uniforme ao longo do tempo, evitando os altos montantes de gastos de compras de infraestrutura de TI. Já os recursos humanos necessários para se implantar, operar e manter a infraestrutura de TI de órgão seriam desonerados, possibilitando que seus esforços sejam redirecionados para outras áreas mais alinhadas com as suas atividades de negócios.

Já a adoção específica de *backup* em nuvem é considerada uma boa opção para o armazenamento de dados críticos do órgão, que ficariam imunes a possíveis desastres que possam acontecer em seus *datacenters* próprios.

Em relação aos riscos ou dificuldades para a adoção de computação em nuvem no órgão, uma das principais preocupações diz respeito à dificuldade de precificação prévia dos serviços, que é uma etapa necessária para as contratações do órgão. Nesse caso, a adoção de *backup* em nuvem aparenta ser uma contratação mais simples, com menos itens de precificação, sendo uma boa opção para contratação inicial de computação em nuvem.

Outra preocupação é quanto à obtenção de autorização da alta administração para a hospedagem na nuvem de sistemas, informações e seus *backups*. Os entrevistados enxergam uma certa insegurança na alta administração em permitir que as informações sejam hospedadas fora dos *datacenters* próprios do órgão. Entendem ser necessário apresentar à alta administração os benefícios da contratação em nuvem para cada caso particular, principalmente os benefícios financeiros. Para isso, é necessário não só identificar corretamente os custos de contração na nuvem, como também os custos de implantação, operação e manutenção dos mesmos serviços quando hospedados nos *datacenters* do órgão.

No que diz respeito às políticas de segurança e de *backup*, os entrevistados afirmaram que é preciso que contenham a previsão para que sistemas, informações e seus *backups* possam ser hospedados em nuvem. Nesse caso, as políticas devem prever também a prévia autorização expressa da alta administração e das áreas de negócio do órgão.

Finalmente, os entrevistados acreditam que quaisquer dados públicos podem ter seu *backup* armazenado em nuvem, desde que em concordância com a legislação vigente e com a autorização da alta administração e das respectivas áreas de negócio do órgão.

3.3 MELHORES PRÁTICAS PARA A ADOÇÃO DE BACKUP EM NUVEM POR ÓRGÃOS DO PODER LEGISLATIVO FEDERAL

Todas as boas práticas encontradas durante a análise da bibliografia e das normas sobre *backups*, continuidade de negócios e computação em nuvem são integralmente válidas no que diz respeito à adoção de *backup* em nuvem pelos órgãos do Poder Legislativo Federal.

Destaca-se a importância da realização do processo de análise de impacto nos negócios, como método de identificação das suas atividades prioritárias e dos seus respectivos requisitos de RPO (*Recovery Point Objective*) e RTO (*Recovery Time Objective*), que será de extrema importância na elaboração da política de *backup* dos órgãos, servido de base para a definição da periodicidade com a qual os *backups* devem ser realizados e do modelo de implementação de *backup* em nuvem que será utilizado. Os valores de RTO e RPO são igualmente importantes para se validar a eficiência dos *backups* armazenados em nuvem pública, já que estes são dependentes das bandas de internet contratadas pelos órgãos e de todo o roteamento de internet necessário para se alcançar os provedores de computação em nuvem.

A análise da legislação vigente demonstrou a importância da classificação da informação para a adoção de *backup* em nuvem pela administração pública. Os dispositivos legais impõem a identificação de quais informações podem comprometer a segurança nacional, de quais informações fazem parte de sistemas estruturantes e de quais informações tem caráter sigiloso. Mesmo já dispondo de normas que dispõe sobre a classificação das informações, é importante que os órgãos do Poder Legislativo Federal incluam explicitamente tais classificações em suas políticas de *backup*, de forma a orientar qual modelo de computação em nuvem pode ser contratado de qual entidade púbica ou privada em cada caso.

No caso específico dos órgãos que compõem o Poder Legislativo Federal, é igualmente importante que a política de *backup* determine a autorização prévia da alta administração e da respectiva área de negócio do órgão para que determinada informação possa ser armazenada na

nuvem. Assim, mesmo que determinada informação tenha alcançado todos os requisitos técnicos e legais para ter seu *backup* armazenado em nuvem, a administração do órgão ainda terá a oportunidade de avaliar se, por exemplo, a informação carrega algum risco político que torne inadequado o seu armazenamento em nuvem.

Para facilitar o processo de adoção de *backup* em nuvem, os órgãos do Poder Legislativo Federal podem, como boa prática, iniciar pelas informações que possuam o caráter o mais público possível.

O estudo identificou ainda a necessidade de estabelecimento de cláusulas contratuais que garantam o sigilo das informações armazenadas em nuvem, a disponibilidade das informações durante os períodos de transição contratual e o prevalecimento da legislação brasileira sobre qualquer outra na relação entre a administração pública e os prestadores de serviço em nuvem.

4 CONCLUSÕES

O estudo mostrou que há uma farta bibliografia recomendando boas práticas para o gerenciamento de *backups*, inclusive considerando a sua adoção em nuvem como estratégia de recuperação para a continuidade de negócios.

Entretanto, apesar do modelo de computação em nuvem se apresentar como um ambiente computacional que conta com uma segurança da informação aprimorada, ficou clara a preocupação governamental com a posse, sigilo e inviolabilidade das informações a serem armazenadas nesse ambiente.

Essa preocupação resultou numa diversidade de dispositivos legais que dispõe sobre as comunicações e sobre a adoção de computação em nuvem pela Administração Pública, dispositivos esses que não se apresentam de forma consolidada e provocam incertezas sobre a forma correta de contratação que deve ser utilizada. Isso explica a ainda baixa utilização de computação em nuvem pela Administração Pública. O próprio órgão participante do estudo de caso, apesar de contar com diretivas estratégias para a adoção de computação em nuvem, ainda não a adotou.

O estudo buscou diminuir essas incertezas ao apresentar de forma consolidada os dispositivos legais que influenciam a adoção de *backup* em nuvem por órgãos do Poder Legislativo Federal, bem como outras particularidades desses órgãos que possam afetar tal adoção.

Como resultado, foram propostos alguns ajustes em suas políticas de *backup*, de forma a contemplarem todas as informações necessárias para se definir qual modelo de computação em nuvem é mais adequado para cada caso, em alinhamento com a legislação vigente.

Outras recomendações dizem respeito aos instrumentos contratuais, que devem garantir o sigilo das informações armazenadas em nuvem, a disponibilidade das informações durante os períodos de transição contratual e o prevalecimento da legislação brasileira sobre qualquer outra na relação entre a Administração Pública e os prestadores de serviço em nuvem.

O estudo identificou ainda a necessidade de esclarecimento da alta administração e das áreas de negócio dos órgãos sobre os modelos de computação em nuvem, sua segurança e nas vantagens de sua adoção. Apesar do incentivo explícito da adoção de computação em nuvem dado pela legislação vigente e pelas diretrizes estratégicas dos órgãos, ainda há uma aparente insegurança na sua efetiva adoção.

Por fim, ficou claro que a identificação de possíveis vantagens financeiras na adoção de *backup* em nuvem fica mais necessária quando se trata dos órgãos do Poder Legislativo Federal. É uma boa prática realizar a modelagem dos custos de contratação de *backup* em nuvem em comparação aos custos de manutenção de *backup* na infraestrutura de TI do próprio órgão, para auxiliar a alta administração a as áreas de negócios dos órgãos na tomada de decisão de quais *backups* devem ou não ser armazenados em nuvem.

Tais modelagens, entretanto, não são fáceis de serem realizadas, devendo considerar custos indiretos como refrigeração e ambientes, alimentação elétrica e recursos humanos de operação, por exemplo. A definição de uma metodologia para a modelagem desses custos se apresenta como um próximo passo a ser dado para se alcançar com sucesso a adoção de *backup* em nuvem pelos órgãos do Poder Legislativo Federal.

REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. NBR ISO/IEC 22313:2015 – Segurança da sociedade — Sistemas de gestão de continuidade de negócios — Orientações. Rio de Janeiro, ABNT, 2015.

ABNT – Associação Brasileira de Normas Técnicas. NBR ISO/IEC 22301:2013 – Segurança da sociedade — Sistema de gestão de continuidade de negócios — Requisitos. Rio de Janeiro, ABNT, 2013a.

ABNT – Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002:2013 – Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. Rio de Janeiro, ABNT, 2013b.

Brasil – Decreto Nº 8.135/2013, de 4 de novembro de 2013. Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional. Brasília, DF, nov 2013.

Brasil – Instrução Normativa GSI/PR Nº 1/2008, de 13 de junho de 2008. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. Brasília, DF, jun 2008.

Brasil – Norma Complementar Nº 14/IN01/DSIC/GSIPR, de 13 de março de 2018. Estabelece princípios, diretrizes e responsabilidades relacionados à segurança da informação para o tratamento da informação em ambiente de computação em nuvem, nos órgãos e entidades da Administração Pública Federal, direta e indireta. Brasília, DF, mar 2018.

Brasil – Norma Complementar Nº 19/IN01/DSIC/GSIPR, de 15 de jul de 2014. Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta. Brasília, DF, jul 2014a.

Brasil – Portaria Interministerial MP/MC/MD nº 141/2014, de 2 de maio de 2014. Dispõe que as comunicações de dados da Administração Pública Federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da Administração Pública Federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias, observado o disposto nesta Portaria. Brasília, DF, mai 2014b.

Brasil – Portaria Ministerial MP/STI nº 20/2016, de 14 de junho de 2016. Dispõe sobre orientações para contratação de soluções de Tecnologia da Informação no âmbito da Administração Pública Federal direta, autárquica e fundacional e dá outras providências. Brasília, DF, jun 2016.

CERT.br – Centro do Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de Segurança para Internet. São Paulo, CERT.br, 2012.

MELL, Peter; GRANCE, Timothy. The NIST Definition of Cloud Computing – Recommendations of the National Institute of Standards and Technology. NIST, 2011.

MORAES, Eliana Márcia. Planejamento de Backup de Dados. Dissertação (Mestrado em Gestão e Desenvolvimento Regional do Departamento de Economia, Contabilidade e Administração) – Universidade de Taubaté. Taubaté, p. 125. 2007.

MPOG – Ministério do Planejamento, Orçamento e Gestão. Boas práticas, orientações e vedações para contratação de Serviços de Computação em Nuvem. Brasília, MPOG, 2016.

NIST – National Institute of Standards and Technology. ITL Bulletin – Techniques for System and Data Recovery. NIST, 2002.

Opus Software – O que Você Realmente Precisa Saber Sobre Computação em Nuvem – São Paulo, 2015

LENTO, Luiz Otávio Botelho; LUZ, Théo Augustus. Gestão de Continuidade do Negócio – Livro Digital. Unisul Virtual, 2014.

TCU – Tribunal de Contas da União. Acórdão 1.739/2015-TCU-Plenário. – Referência para os auditores do TCU em futuras auditorias de contratações de serviços de computação em nuvem, bem como para os gestores públicos encarregados de avaliar e, se for o caso, contratar serviços de TI segundo esse modelo. Brasília, TCU, 2015.

WILL, Daniela Erani Monteiro. Metodologia de Pesquisa Científica – Livro Digital. Unisul Virtual, 2016.

APÊNDICE A – TRANSCRIÇÃO DA ENTREVISTA CONJUNTA COM O DIRETOR EXECUTIVO E COM O DIRETOR EXECUTIVO ADJUNTO DA ÁREA DE TI DO ÓRGÃO, REALIZADA EM 19/10/2018

1. Quais as possíveis vantagens da adoção de backup em nuvem pelo órgão?
    - Atendimento às diretrizes estratégias da alta direção, que incentivam o uso de computação em nuvem;
    - Obter uma melhor relação custo x benefício na alocação de recursos financeiros;
    - Maior homogeneidade de despesas ao decorrer do tempo (troca de CAPEX por OPEX);
    - Desoneração de recursos humanos alocados para a manutenção da infraestrutura de TI do órgão, possibilitando sua realocação para outras áreas;

- Dentre os serviços que poderiam ser hospedados em nuvem, o de backup aparenta ser um dos de menor complexidade.

2. Quais os possíveis riscos ou dificuldades para a adoção de backup em nuvem pelo órgão?
   - Identificar quais informações podem ser hospedadas na nuvem, sem que tal decisão cause resistências, ou uma sensação de falta de autonomia e controle sob as informações, ou ainda uma sensação de insegurança política à alta administração e às áreas de negócio do órgão;
   - Obter anuência para hospedar as informações e sistemas na nuvem, tanto da alta administração do órgão quanto das áreas de negócios, uma vez que a área de TI do órgão se posiciona como custodiante das informações;
   - Modelar corretamente os custos de contratação de computação em nuvem, em alinhamento com a legislação vigente;
   - Identificar, para cada caso concreto, os benefícios da adoção de computação em nuvem, para serem apresentados à alta administração do órgão e para as áreas de negócios, de forma a auxilia-los na tomada de decisão do que será autorizado a ser hospedado na nuvem;
   - Risco de ocorrência de problemas jurídicos/contratuais nas situações em que afetem a continuidade ou a disponibilidade dos serviços hospedados na nuvem;
   - Sincronizar o início da adoção de computação em nuvem para um serviço, com o final do ciclo de vida e dos contratos de manutenção da infraestrutura de TI anteriormente adquirida para a hospedagem do mesmo serviço, maximizando os altos recursos já investidos no datacenter do órgão;
   - Modelar, para cada caso concreto, o custo de operação/manutenção de cada serviço no datacenter do órgão, de forma a poder se aferir se a mudança para a nuvem será (ou foi) financeiramente vantajosa;
   - Risco de ter que retornar um serviço hospedado na nuvem para o datacenter do órgão, sem que se tenha mantido a infraestrutura de TI necessária para hospedar tal serviço.

3. O que poderia constar da Política de Segurança da Informação e da Política de Backup do órgão para auxiliar a adoção de backup em nuvem?

- Constar a previsão de identificação e aprovação prévia, por parte da alta administração e/ou áreas de negócio do órgão, das informações que poderiam ser hospedadas na nuvem.

4. Quais dados do órgão poderiam ter seu backup hospedado na nuvem?
    - Qualquer dado ostensivo, o mais público possível, desde que cumpra os requisitos legais e que conte com a anuência prévia da alta administração e/ou das áreas de negócio do órgão.

APÊNDICE B – TRANSCRIÇÃO DA ENTREVISTA COM O CHEFE DO SETOR RESPONSÁVEL PELO BACKUP CORPORATIVO DO ÓRGÃO, REALIZADA EM 19/10/2018

1. Quais as possíveis vantagens da adoção de backup em nuvem pelo órgão?
    - Ter mais uma opção onde armazenar e restaurar os dados críticos do órgão, e que esteja disponível mesmo em caso de grandes desastres da infraestrutura de backup implantada nos datacenters do órgão;
    - Maior flexibilidade de alocação de recursos de armazenamento, de forma que possa ser alocado/adquirido conforme a necessidade contínua do órgão, sem a necessidade da compra prévia de todo o espaço de armazenamento necessário para atender as demandas do órgão durante cada período contratual.
2. Quais os possíveis riscos ou dificuldades para a adoção de backup em nuvem pelo órgão?
    - Falta de certeza se, em caso da ocorrência de um desastre, a restauração de um backup armazenado em nuvem será realmente efetiva, em tempo hábil e adversidades contratuais. Se um backup desse tipo e importância não puder ser efetivamente recuperado, o setor de TI terá falhado em sua missão;
    - Incerteza da real segurança das informações a que os backups em nuvem estarão sujeitos, mesmo com a previsão de mecanismos contratuais que garantam tal segurança;
    - Dificuldade da constatação se o custo de armazenamento e, principalmente, de envio/recuperação de dados, é realmente mais vantajoso na nuvem.
3. O que poderia constar da Política de Segurança da Informação e da Política de Backup do órgão para auxiliar a adoção de backup em nuvem?

- Prever a possibilidade de armazenamento de backup em nuvem, desde que atenda as demandas e restrições das áreas de negócio do órgão.

4. Quais dados do órgão poderiam ter seu backup hospedado na nuvem?
   - Todos os dados do órgão, em ordem de criticidade: bancos de dados de produção, dados de CPI's (Comissões Parlamentares de Inquérito), dados de produção legislativa dos gabinetes parlamentares e dados administrativos, desde que tais dados atendam aos requisitos legais para serem hospedados em nuvem.
5. Outras considerações:
   - Há diretrizes do órgão para a adoção de computação em nuvem, sendo importante realizar uma avaliação inicial da efetividade e dos custos de adoção de backup em nuvem.

APÊNDICE C – TRANSCRIÇÃO DA ENTREVISTA COM O COORDENADOR DA DIRETORIA RESPONSÁVEL PELA INFRAESTRUTURA DE TI DO ÓRGÃO, REALIZADA EM 22/10/2018

1. Quais as possíveis vantagens da adoção de backup em nuvem pelo órgão?
   - Ter uma alternativa previamente contratada para implantações urgentes, sem a necessidade de se esperar pela instalação e início de operação habituais em uma compra de infraestrutura;
   - Suportar picos sazonais ou inesperados de demanda;
   - Evitar os custos ocultos na manutenção de infraestrutura, como o de pessoal necessário para manter e operar os equipamentos;
   - Trazer o esforço de trabalho mais para a finalidade dos serviços, e não para os meios de alcança-los.
2. Quais os possíveis riscos ou dificuldades para a adoção de backup em nuvem pelo órgão?
   - Não conseguir fazer uso da computação em nuvem como se deveria, por ter que se enquadrar nos modelos contratuais permitidos para a administração pública;
   - Dificuldade de se fazer uso ou contratar novas funcionalidades disponibilizadas pelo fornecedor de serviços em nuvem, por já estar limitado por um contrato vigente;

- Possível falta de maturidade do órgão em relação à segurança da informação, fazendo com que se armazene alguma informação na nuvem que não deveria estar lá;
- Possibilidade de *lock-in* de fornecedor de serviços de nuvem, pela adoção de uma funcionalidade exclusiva do fornecedor, por exemplo, causando dificuldades nas transições contratuais;
- Rigidez da estrutura administrativa do órgão, dificultando a formação de um núcleo específico para o estudo de adoção de computação em nuvem, no lugar de se ter recursos espalhados pelas diversas áreas de TI pesquisando sobre o assunto.

3. O que poderia constar da Política de Segurança da Informação e da Política de Backup do órgão para auxiliar a adoção de backup em nuvem?
   - Na verdade, poderia ser criada uma política específica de computação em nuvem, com os critérios de seleção do que se poderia se nela hospedado.
4. Quais dados do órgão poderiam ter seu backup hospedado na nuvem?
   - Os de domínio público, tudo que não tiver caráter pessoal, sigiloso ou restrito.