Nuvem Pública na APF - Recomendações na Contratação

Thiago Ferreira Lopes
tferreiralopes@gmail.com
UCB

João Souza Neto
szneto@globo.com
UCB

Resumo:A Computação em Nuvem é uma opção que gera ganhos com a sua adoção tanto pelo mercado privado, quanto por empresas ou órgãos públicos. Porem a sua adoção ainda é cercada de risco e incertezas, sendo a segurança da informação, propriedade dos dados e a responsabilização por sua custódia, questões legais e contratuais, exemplos dos principais temores apontados por pesquisas realizadas no mercado. Este resultado demonstra que nem sempre as dificuldades de implantação estão relacionadas a questões técnicas. Reconhecendo as lacunas e dúvidas existentes nesta modalidade de prestação de serviço de TI, o Governo Federal divulgou a norma complementar 14 em 2012 para nortear os trabalhos de adoção deste novo paradigma pelos órgãos da administração pública federal. Nela constam garantias mínimas que devem ser solicitadas ao fornecedor do serviço de computação em nuvem pelo órgão contratante do serviço. Baseado nestas garantias, foi feita uma pesquisa na legislação existente e recomendada pelo Departamento de Segurança da Informação e Comunicações em seu site, além da norma técnica ABNT NBR ISO/IEC 27002:2013, sendo que os pontos relevantes para o atendimento das garantias indicadas na instrução normativa foram listados e apresentados como recomendações que devem constar no contrato que irá reger o relacionamento do órgão com o provedor de serviço em nuvem.

Palavras Chave: Computação em Nuvem - APF - Segurança - SIC -

1. INTRODUÇÃO

A Computação em Nuvem é uma das opções que as empresas e o governo têm de tirar proveito das novas tecnologias, atendendo os anseios por informações e serviços que devem ser prestados de forma rápida e com qualidade. Porém, quando se aborda este novo paradigma da tecnologia, os riscos envolvidos trazem outros desafios para a organização, a começar pela contratação de recurso de TI, que deixa de ser um investimento e passa ser enquadrada como custeio.

Segundo o levantamento realizado pelo ISACA (2012), dentre os principais temores do mercado em relação à adoção da computação em nuvem estão: segurança da informação, propriedade dos dados e a responsabilização por sua custódia, questões legais e contratuais, viabilidade financeira do fornecedor, monitoramento do desempenho e estabilidade da tecnologia subjacente, ou seja, a adoção da computação em nuvem não é uma questão exclusiva de viabilidade técnica.

O governo também reconhece que existem lacunas e dúvidas nesse novo cenário a respeito de que medidas devem ser tomadas para que a nova tecnologia seja melhor aproveitada para atender, com segurança, aos objetivos estratégicos institucionais (BRASIL, 2012c). Como tentativa de nortear os trabalhos de adoção pelos órgão da Administração Pública Federal (APF), foi publicada pelo Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República a instrução normativa de número 14 de 2012, onde o governo identifica a computação em nuvem como uma forma de se prover recursos de tecnologia da informação de forma mais rápida e barata, identificando esforços e pontos de atenção por parte dos órgãos e entidades da APF para que estes usufruam dos benefícios viabilizando e assegurando a Segurança da Informação e Comunicação (SIC) da iniciativa (BRASIL, 2012c).

Diante deste cenário de insegurança e com a pretensão de investimentos nesta nova tecnologia pelo governo, conforme divulgado no programa TI Maior (Programa Estratégico de Software e Serviços de TI) do Ministério da Ciência, Tecnologia e Inovação (BRASIL, 2012a), este trabalho busca recomendar itens que devem constar do contrato de prestação de serviços entre um provedor de computação em nuvem e um cliente vinculado à APF.

2. COMPUTAÇÃO EM NUVEM

O *National Institute of Standards and Technology* (NIST) publicou em 2011, a definição de Mell e Grance (2011) de computação em nuvem como um modelo que permite acesso ubíquo, conveniente e sob demanda de um *pool* de recursos computacionais, como rede, servidores, armazenamento, aplicações e outros serviços. Foram propostos três modelos de provimento de compunção em nuvem, que possuem cinco características básicas. Esta definição abrangente destaca as principais características deste modelo e, por isso, foi utilizada neste trabalho.

2.1. VANTAGENS E CARACTERÍSTICAS ESSENCIAIS

Segundo o Mell e Grance (2011), um modelo de serviço de computação em nuvem deve ser estruturado para atender as características essenciais descritas no Quadro 1.

Característica	**Descrição**

On-demand self-service	O cliente deve ser capaz de provisionar os recursos necessários de forma automática, sem a necessidade de interação humana;
Acesso via rede	Todo o acesso aos recursos deverá ser via rede, podendo utilizar mecanismos heterogêneos de acesso como: celulares, *tablets*, computadores e outros;
Recursos em *Pool*	Recursos de computação do provedor são agrupados para atender vários consumidores através de um modelo *multi-tenant*, com diferentes recursos físicos e virtuais atribuídos e realocados dinamicamente de acordo com a demanda do cliente;
Elasticidade rápida	O recurso previsto no contrato pode ser elasticamente provisionado e liberado, em alguns casos, automaticamente. Para o cliente, os recursos disponíveis para provisionamento podem parecer ilimitados e podem ser requisitados em qualquer quantidade a qualquer momento;
O serviço medido	O uso dos recursos deve ser monitorado, controlado e reportado, oferecendo transparência tanto para o provedor quanto para o cliente em relação ao serviço utilizado

Quadro 1: Descrição das características essenciais da Computação em Nuvem.

Segundo o ISACA (2012), serviços com as características listadas no quadro 1 agregam valor e geram vantagem competitiva para a empresa cliente. Entender esses valores e vantagens, os quais orientam a adoção e o uso, seja como a principal estratégia de sistemas de informação ou como complemento para os serviços de tecnologia em períodos com maior demanda é extremamente importante.

2.2. PRESTAÇÃO DO SERVIÇO

Ainda segundo o Mell e Grance (2011), existem três modelos de prestação de serviço pelo provedor de serviço em nuvem, que são: Software como Serviço, Plataforma como Serviço e Infraestrutura como Serviço.

O Software como Serviço (*Software as a Service* - SaaS) é o modelo onde o cliente executa as suas aplicações no provedor de nuvem, porém não tem acesso à infraestrutura que suporta a mesma. Já no Plataforma como Serviço (*Platform as a Service* - PaaS), o cliente tem um pouco mais de liberdade, pois a capacidade fornecida permite implantar sobre uma infraestrutura em nuvem aplicações adquiridas ou criadas usando linguagens de programação, bibliotecas, serviços e ferramentas suportadas pelo provedor. Neste modelo, o consumidor não gerencia nem controla a infraestrutura da nuvem, que inclui rede, servidores, sistemas operacionais ou armazenamento, mas tem controle sobre os aplicativos implementados e, possivelmente, definições de configuração para o ambiente de hospedagem dos mesmos.

O terceiro modelo, Infraestrutura como Serviço (*Infrastructure as a Service* - IaaS), é um modelo de serviço automatizado, onde os recursos de computação, complementados por recursos de armazenamento e de rede, são oferecidos a um cliente sob demanda. Os clientes devem ser capazes de provisionar esse tipo de recurso conforme necessário, utilizando uma interface gráfica de usuário baseada na Web e/ou através de uma API integrando em algum programa cliente.

A computação em nuvem pode ser desenvolvida das seguintes formas: Nuvem Privada, Nuvem Pública, Nuvem Comunitária e Nuvem Híbrida.

Na Nuvem Privada, a infraestrutura de nuvem é provisionada para o uso exclusivo de uma única organização que agrupa vários clientes (por exemplo, unidades de negócios). Ela pode ser gerenciada e operada pela própria organização, por um terceiro, ou por alguma combinação destes. A infraestrutura pode ser criada dentro ou fora da organização.

Na Nuvem Comunitária a infraestrutura de nuvem é provisionada para uso exclusivo de uma comunidade específica de organizações que têm preocupações como missão, os requisitos de segurança, política e considerações de *compliance* em comum. Pode ser gerenciada e operada por uma ou mais organizações da comunidade, por um terceiro ou por uma combinação destes, podendo ser construída em uma das organizações ou fora delas.

Na Nuvem Pública, a infraestrutura de nuvem é provisionada para uso aberto ao público em geral. Pode ser gerenciada e operada por uma empresa, universidade, organização governamental ou uma combinação destes.

Na Nuvem Híbrida, a infraestrutura de nuvem é uma composição de dois ou mais modelos de infraestrutura de nuvem (privada, comunitária ou pública), formando uma única nuvem através de padrões públicos ou proprietários de tecnologia padronizada, que permitam a portabilidade dos dados e a aplicação entre nuvens.

3. LEGISLAÇÃO RELACIOADA A COMPUTAÇÃO EM NUVEM

A Presidência da República instituiu, através do Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional (GSI/PR) a norma complementar de número 14 em 2012 (BRASIL 2012c), com regras imperativas para utilização de serviços em computação em nuvem pela Administração Pública Federal (APF). A norma estabelece que ao contratar ou implementar um serviço de computação em nuvem, o órgão ou entidade da APF deve garantir que:

- A legislação brasileira prevaleça sobre qualquer outra, de modo a ter todas as garantias legais enquanto tomadora do serviço e proprietária das informações hospedadas na nuvem;

- O ambiente de computação em nuvem, sua infraestrutura e canal de comunicação estejam aderentes às diretrizes e normas de SIC, estabelecidas pelo GSIPR, e às legislações vigentes;

- O contrato de prestação de serviço, quando for o caso, deve conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço.

A primeira premissa descrita acima não é impeditiva para a utilização de nuvem pública pela APF, porem impõe uma restrição para utilização de centros de dados para hospedagem e processamento das informações fora do Brasil, pois a soberania do Estado é reconhecida, no direito internacional, em seu próprio território. Neste caso, não será possível garantir que a legislação brasileira seja cumprida em outro país.

3.1 GARANTINDO A ADERÊNCIA ÀS DIRETRIZES E NORMAS DE SIC

O site do DSIC do GSI/PR disponibiliza uma compilação da legislação vigente a respeito da Segurança da Informação e Comunicações - SIC, com o objetivo de facilitar o acesso e fortalecer a cultura de SIC. O quadro 2 indica as leis, normas e instruções normativas relacionadas à SIC que devem ser seguidas pelo órgão ou empresa vinculada à APF.

TIPO	**DENOMINAÇÃO**
LEIS	LEI 12.527, DE 18 DE NOVEMBRO DE 2011 LEI 9.983, DE 14 DE JULHO DE 2000
DECRETOS	DECRETO Nº 3.505, DE 13 DE JUNHO DE 2000 DECRETO Nº 7.724, DE 16 DE MAIO DE 2012 DECRETO Nº 7.845, DE 14 DE NOVEMBRO DE 2012 DECRETO Nº 8.097, DE 4 DE SETEMBRO DE 2013
INSTRUÇÕES NORMATIVAS	INSTRUÇÃO NORMATIVA GSI Nº 1; INSTRUÇÃO NORMATIVA GSI Nº 2; INSTRUÇÃO NORMATIVA GSI Nº 3; INSTRUÇÃO NORMATIVA Nº 4 - SLTI/MPOG
NORMAS COMPLEMENTARES	NC Nº 01/IN01/DSIC/GSIPR, NC Nº 02/IN01/DSIC/GSIPR, NC Nº 03/IN01/DSIC/GSIPR, NC Nº 04/IN01/DSIC/GSIPR, NC Nº 05/IN01/DSIC/GSIPR, NC Nº 06/IN01/DSIC/GSIPR, NC Nº 07/IN01/DSIC/GSIPR, NC Nº 08/IN01/DSIC/GSIPR, NC Nº 09/IN01/DSIC/GSIPR, NC Nº 10/IN01/DSIC/GSIPR, NC Nº 11/IN01/DSIC/GSIPR, NC Nº 12/IN01/DSIC/GSIPR, NC Nº 13/IN01/DSIC/GSIPR, NC Nº 14/IN01/DSIC/GSIPR, NC Nº 15/IN01/DSIC/GSIPR, NC Nº 16/IN01/DSIC/GSIPR, NC Nº 17/IN01/DSIC/GSIPR, NC Nº 18/IN01/DSIC/GSIPR, NC Nº 19/IN01/DSIC/GSIPR, NC Nº 20/IN01/DSIC/GSIPR, NC Nº 21/IN01/DSIC/GSIPR, NC Nº 01/IN02/NSC/GSIPR.

Quadro 2: Leis, normas e instruções normativas relacionadas à SIC publicadas no sítio do DSIC.

Apesar de relacionadas à SIC, nem todas as leis, normas complementares ou instruções normativas listadas estão relacionadas à contratação de serviços de computação em nuvem. O quadro 3, a seguir, dá foco nos itens que devem ser considerados na elaboração de editais para este tipo de contratação.

Lei/ Decreto/ Instrução Normativa/ Norma	**Itens que devem ser observados**

Complementar	
Lei 12.527 de 18 de novembro de 2011 (BRASIL, 2011)	- Seção III - Parágrafo único: A pessoa física ou entidade privada que, em razão de qualquer vínculo com o poder público, executar atividades de tratamento de informações sigilosas, adotará as providências necessárias para que seus empregados, prepostos ou representantes observem as medidas e procedimentos de segurança das informações resultantes da aplicação desta Lei. - Capítulo V, conforme parágrafo único do mesmo: o disposto neste artigo aplica-se a pessoa física ou entidade privada que, em virtude de vínculo de qualquer natureza com órgãos ou entidades, tenha acesso a informação sigilosa ou pessoal e a submeta a tratamento indevido.
Decreto Nº 7.845 de 14 de novembro de 2012 (BRASIL, 2012b)	- Seção IX – Da Celebração de Contratos Sigilosos e todos os seus subitens. - ANEXO I – Termo de Compromisso de Manutenção de Sigilo (TCMS)
Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013 (BRASIL, 2013a)	- Art. 6º Compete ao Posto de Controle: I - armazenar e controlar as informações classificadas, inclusive as credenciais de segurança, sob sua responsabilidade; II - manter a segurança lógica e física das informações classificadas, sob sua guarda; IV - encaminhar, periodicamente, ao Órgão de Registro que o credenciou relatórios de suas atividades; V - notificar o Órgão de Registro que o credenciou, imediatamente, quando da quebra de segurança das informações classificadas por ele custodiadas; - Art. 7º O acesso, a divulgação e o tratamento de informação classificada em qualquer grau de sigilo ficarão restritos a pessoas que tenham necessidade de conhecê-la e que tenham Credencial de Segurança segundo as normas fixadas pelo GSI/PR, por intermédio do NSC, sem prejuízo das atribuições de agentes públicos autorizados por Lei. - Parágrafo único. O acesso à informação classificada em qualquer grau de sigilo a pessoa não credenciada ou não autorizada por legislação poderá, excepcionalmente, ser permitido mediante assinatura de Termo de Compromisso de Manutenção de Sigilo - TCMS, conforme Anexo I do Decreto nº 7.845, de 2012, pelo qual a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da Lei. - Art. 21. Na hipótese de troca e tratamento de informação classificada em qualquer grau de sigilo, com país ou organização estrangeira, o credenciamento de segurança no território nacional, se dará somente se

	houver tratado, acordo, memorando de entendimento ou ajuste técnico firmado entre o país ou organização estrangeira e a República Federativa do Brasil
Instrução Normativa GSI/PR nº 3 de 6 de março de 2013 (BRASIL, 2013b)	- Art. 4º. A cifração e decifração de informações classificadas, em qualquer grau de sigilo, devem utilizar recurso criptográfico baseado em algoritmo de Estado em conformidade com os padrões e parâmetros mínimos estabelecidos na NC 09/IN01/DSIC/GSI/PR (Revisão 01), de fevereiro de 2013, reproduzidos no Anexo desta Instrução Normativa. - Art. 5º. O recurso criptográfico baseado em algoritmo de Estado deverá ser de desenvolvimento próprio ou por órgãos e entidades do Poder Executivo Federal, mediante acordo ou termo de cooperação, vedada a participação e contratação de empresas e profissionais externos, para tal finalidade. § 1º. Excepcionalmente, com anuência da Alta Administração do órgão ou entidade, o previsto no caput poderá ser terceirizado, desde que atendidas obrigatoriamente as seguintes condições: I - seja realizado exclusivamente por meio de Contrato Sigiloso, nos termos dos arts. 48 e 49 do Decreto7.845, de 14 de novembro de 2012; II - seja previsto em cláusula contratual que fica vedado ao contratado os direitos de propriedade e de exploração comercial do recurso criptográfico com algoritmo de Estado, objeto do presente contrato; - Art. 6º, IV - prever explicitamente nos entendimentos, contratos, termos ou acordos de aquisição e manutenção de equipamentos, dispositivos móveis, sistemas, aplicativos ou serviços que disporão de recurso criptográfico baseado em algoritmo de Estado, o fiel cumprimento do disposto na presente Instrução Normativa, sem prejuízo da legislação vigente; - Art. 9º. Todo recurso criptográfico baseado em algoritmo de Estado constitui material de acesso restrito e requer procedimentos especiais adequados de controle para o seu acesso, manutenção, armazenamento, transferência, trânsito e descarte, em conformidade com a legislação vigente, sob pena de responsabilização da Alta Administração. Parágrafo único. O Gestor de Segurança da Informação e Comunicações e todo Agente Responsável, usuários de recurso criptográfico baseado em algoritmo de Estado, devem possuir Credencial de Segurança, ou excepcionalmente, assinar o Termo de Compromisso de Manutenção de Sigilo - TCMS, conforme Anexo I do Decreto 7.845, de 14 de novembro de 2012.
Instrução Normativa nº 4 SISP de 11 de setembro de 2014, redação	- Apesar de a instrução não tratar diretamente itens de SIC relacionados à computação em nuvem, ela traz

dada pela Instrução Normativa N° 2 de 12 janeiro 2015 (BRASIL, 2015)	todas as diretrizes para contratação de serviços da APF e deve ser considerada na integra pelo órgão no processo de contratação.
Norma Complementar nº 06/IN01/DSIC/GSIPR de 11 de novembro de 2009 (BRASIL, 2009)	- Item 5.7 Sugere-se que os contratos firmados com empresas terceirizadas que suportem atividades críticas contenham cláusula segundo a qual as referidas empresas possuam Planos de Continuidade dos seus Negócios, bem como as evidências dos testes realizados.
Norma Complementar nº 07/IN01/DSIC/GSIPR de 15 de julho de 2014 (BRASIL, 2014a)	- 6.3.1. Conter ferramentas de proteção contra acesso não autorizado aos ativos de informação, que favoreça, preferencialmente, a administração de forma centralizada. - 6.3.2. Respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação; - 6.3.3. Utilizar ativo de informação homologado nas aplicações de controle de acesso, de tratamento das informações sigilosas e de criptografia; - 6.3.4. Registrar eventos relevantes, previamente definidos, para a segurança e rastreamento de acesso às informações sigilosas. - 6.3.5. Criar mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação. - 7.3.1. Estabelecer distância mínima de segurança para manutenção das mídias contendo as cópias de segurança (*backups*);
Norma Complementar nº 21/IN01/DSIC/GSIPR de 8 de outubro de 2014 (BRASIL, 2014b)	6.1 O horário dos ativos de informação deve ser ajustado por meio de mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a “Hora Legal Brasileira (HLB)”, de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).

Quadro 3: Leis, normas e instruções normativas relacionadas a SIC na adoção da computação em nuvem pela APF.

3.2 RECOMENDAÇÕES DE CONTROLES

A terceira premissa da norma complementar de número 14 é que o contrato de prestação de serviço, quando for o caso, deve conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço (BRASIL 2012b).

Uma das formas de garantir o atendimento desta é solicitar no edital/contrato que o provedor de serviço atenda itens das normas ABNT NBR ISO/IEC 27002:2013 que trazem recomendações de controles de segurança da informação (ABNT, 2013).

O quadro 4 indica quais os controles recomendados na norma indicada anteriormente devem ser delegados para o provedor de serviço em computação em nuvem, sendo recomendado a indicação deste no edital/contrato.

Controles da ABNT NBR ISO/IEC 27002:2013 (ABNT, 2013)
6.1.1 - Responsabilidade e papéis pela segurança da informação Controle: Convém que todas as responsabilidades pela segurança da informação sejam definidas e atribuídas.
6.1.3 - Contato com autoridades Controle: Convém que contatos apropriados com autoridades relevantes sejam mantidos
7.2.2 - Conscientização, educação e treinamento em segurança da informação Controle: Convém que todos os funcionários da organização e, onde pertinente, partes externas devem recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais
9.1.1 – Política de controle de acesso Controle: Convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios.
9.2.2 – Provisionamento para acesso de usuário Controle: Convém que um processo formal de provisionamento de acesso do usuário seja implementado para conceder ou revogar os direitos de acesso do usuário para todo os tipos de usuários em todos os tipos de sistemas e serviços.
9.2.3 – Gerenciamento de direitos de acesso privilegiados Controle: Convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados.
9.2.4 – Gerenciamento da informação de autenticação secreta de usuários Controle: Convém que a concessão de informação de autenticação secreta seja controlada por meio de um processo de gerenciamento formal.
9.4.2 – Procedimentos seguros de entrada no sistema (*log-on*) Controle: Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações sejam controlados por um procedimento seguro de entra no sistema (*log-on*)
10.1.1 - Política para o uso de controles criptográficos Controle: Convém que seja desenvolvida e implementada uma política sobre o uso de controle criptográficos para a proteção da informação
10.1.2 – Gerenciamento de chaves Controle: Convém que uma política sobre o uso, proteção e tempo de vida das chaves criptográficas seja desenvolvida e implementada ao longo de todo o seu ciclo de vida.
11.1.1 – Perímetro de segurança física Controle: Convém que perímetros de segurança sejam definidos e usados para proteger tanto as instalações de processamento da informação como as áreas que contenham informações críticas ou sensíveis
11.1.2 – Controles de entrada física Controle: Convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.
11.1.3 – Segurança em escritórios, salas e instalações Controle: Convém que seja projetada e aplicada segurança física para escritórios, salas e instalações.
11.1.4 – Proteção contra ameaças externas e do meio ambiente Controle: Convém que seja projetada e aplicada proteção física contra

desastres naturais, ataques maliciosos ou acidentes.
11.2.1 – Localização e proteção do equipamento Controle: Convém que os equipamentos sejam protegidos e colocados em locais para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.
12.1.2 – Gestão de mudanças Controle: Convém que mudanças na organização, nos processos do negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação, sejam controladas.
12.2.1 – Controles contra *malware* Controle: Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra *malware*, combinados com um adequado programa de conscientização do usuário.
12.3.1 – Cópias de segurança das informações Controle: Convém que cópias de segurança das informações, dos *softwares* e das imagens do sistema sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.
12.4.1 – Registro de eventos Controle: Convém que registros (*log*) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares.
12.4.2 – Proteção das informações dos registros de eventos (*logs*) Controle: Convém que as informações dos registros de eventos (*log*) e os seus recursos sejam protegidos contra acesso não autorizado e adulteração.
12.4.3 – Registros de eventos (*log*) de administrador e operador Controle: Convém que as atividades dos administradores e operadores do sistema sejam registradas e os registros (*logs*) protegidos e analisados criticamente, a intervalos regulares.
12.4.4 – Sincronização dos relógios Controle: Convém que os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, sejam sincronizados com uma única fonte de tempo precisa.
12.6.1 – Gestão de vulnerabilidades técnicas Controle: Convém que informações sobre vulnerabilidades técnicas dos sistemas de informação em uso sejam obtidas em tempo hábil; convém que a exposição da organização a estas vulnerabilidades seja avaliada e que sejam tomadas as medidas apropriadas para lidar com os riscos associados.

Quadro 4: Recomendações baseadas na norma ABNT NBR ISO/IEC 27002:2013

Como pode-se notar no quadro 4, muitas das recomendações deverão ser verificadas através de auditorias e comprovações técnicas que o órgão deverá fazer por meio de diligências antes do fechamento do contrato e periodicamente no decorrer do mesmo.

4. CONCLUSÕES

A adoção da computação em nuvem por parte de órgãos públicos exige que os seus gestores de TI estejam respaldados legalmente de suas ações nesse novo paradigma. Neste cenário, a elaboração dos editais e termos de referência deve buscar o atendimento dos diversos requisitos indicados neste trabalho de modo a preservar a informação tratada.

A classificação das informações para o correto atendimento dos itens recomendados neste artigo é essencial, pois algumas podem ser irrelevantes dependendo do grau de sigilo atribuído.

Como trabalho futuro, sugere-se a criação de um modelo de avaliação da maturidade dos órgãos no que tange à classificação das informações, buscando indicar um grau mínimo de maturidade recomendado para a migração das informações para o serviço em nuvem.

5. REFERÊNCIAS

ABNT NBR ISO/IEC 27002:2013. Tecnologia da Informação — Técnicas de Segurança — Código de prática para controles de segurança da informação. São Paulo: ABNT, 2013.

BRASIL. Ministério da Ciência, Tecnologia e Inovação. **TI maior**: programa estratégico de software e serviços de tecnologia da informação 2012 – 2015. Brasília, 2012a

BRASIL. **Lei nº 12.527**, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 23 mai. 2015

BRASIL. **Decreto nº 7.845**, de 14 de novembro de 2012. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. Brasília, 2012b. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/D7845.htm>. Acesso em: 23 mai. 2015

BRASIL. Presidência da República. **Norma complementar nº 06**, de 23 de novembro de 2009. Brasília, 2009. Disponível em: <https://dsic.planalto.gov.br/documentos/nc_6_gcn.pdf>. Acesso em: 23 mai. 2015

BRASIL. Presidência da República. **Norma complementar nº 07**, de 16 de julho de 2014. Brasília, 2014a. Disponível em: <https://dsic.planalto.gov.br/documentos/nc_07_revisao_01.pdf>. Acesso em: 23 mai. 2015

BRASIL. Presidência da República. **Norma complementar nº 14**, de 10 de fevereiro de 2012. Brasília, 2012c. Disponível em: <https://dsic.planalto.gov.br/documentos/nc_14_nuvem.pdf>. Acesso em: 23 mai. 2015

BRASIL. Presidência da República. **Norma complementar nº 21**, de 10 de outubro de 2014. Brasília, 2014b. Disponível em: <https://dsic.planalto.gov.br/documentos/nc_21_preservacao_de_evidencias.pdf>. Acesso em: 23 mai. 2015

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Instrução Normativa nº 2**, de 05 de fevereiro de 2013. Brasília, 2013a. Disponível em: <https://dsic.planalto.gov.br/documentos/instrucao_normativa_nr2.pdf>. Acesso em: 23 mai. 2015

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Instrução Normativa nº 3**, de 06 de março de 2013. Brasília, 2013b. Disponível em: <https://dsic.planalto.gov.br/documentos/instrucao_normativa_nr3.pdf>. Acesso em: 23 mai. 2015

BRASIL. Secretaria de Logística e Tecnologia da Informação. **Instrução Normativa nº 4**, de 12 de novembro de 2010. Brasília: SLTI/MPOG, 2015. Disponível em: <http://www.governoeletronico.gov.br/biblioteca/arquivos/instrucao-normativa-nb0-4-de-11-de-setembro-de-2014/download>. Acesso em: 23 mai. 2015

ISACA. Guiding Principles for Cloud Computing Adoption and Use. Rolling Meadows, 2012

MELL, P., GRANCE, T. The NIST definition of cloud computing. Gaitherburg: NIST, 2011