INTERFACE TECNOLÓGICA

ANÁLISE DE SEGURANÇA NA CONTRATAÇÃO DE SERVIÇOS EM NUVEM: Comparativo Estados Unidos e Brasil

SECURITY ANALYSIS WHEN HIRING CLOUD SERVICES: Comparison United States and Brazil

Marcio de Carli – marcio_de_carli@hotmail.com

Pontifícia Universidade Católica de Minas Gerais – Belo Horizonte – MG – Brasil

DOI: 10.31510/infa.v17i2.855

Data de publicação: 18/12/2020

RESUMO

Este trabalho tem o objetivo de descrever e analisar práticas correntes de avaliação da segurança da informação na adoção de serviços de computação em nuvem. Ele discute o esforço empregado na realização destas práticas e elenca as melhorias necessárias para aumento da eficiência na execução do processo de avaliação de riscos e implementação de controles no Brasil. O artigo realiza uma revisão de duas abordagens governamentais utilizadas na gestão de riscos para a adoção de serviços de computação em nuvem: O *Federal Risk and Authorization Management Program* ou *FedRAMP* e os processos do governo brasileiro para gestão de riscos em segurança da informação. O estudo elenca ações como a manutenção de conjuntos pré-definidos de controles, o reuso das análises realizadas para qualificação dos sistemas e a categorização das informações quanto ao sigilo em grandes blocos como formas de avançar no processo de avaliação no Brasil. As formas de execução desta avaliação impactam diretamente nos desenhos das soluções, no desenvolvimento dos serviços, e nos modelos de contratação.

Palavras-chave: Segurança da Informação, Computação em Nuvem, Gestão de Riscos.

ABSTRACT

This work aims to describe and evaluate current information security assessment practices in the adoption of cloud computing services. It discusses the effort employed in carrying out these practices and lists the necessary improvements to increase efficiency in the execution of the security assessment process risks and implementation of controls in Brazil. The article reviews two government approaches used in risk management for the adoption of cloud computing services: The Federal Risk and Authorization Management Program or FedRAMP and the Brazilian government's processes for risk management in information security. The regulatory framework of each country is the base for both processes. Finally, the study lists actions such as the maintenance of predefined sets of controls, the reuse of the analyzes carried out to qualify the systems, the categorization of information regarding secrecy in large blocks as ways to improve this evaluation process in Brazil. The ways of carrying out this

evaluation directly impact the design of solutions, the development of services, and the contracting models.

Keywords: Information Security, Cloud Computing, Risk Management.

1 INTRODUÇÃO

1.1 Motivação

As organizações precisam prover e suportar aplicações voltadas ao seu público-alvo e aos seus parceiros de negócio internos e externos. Estes serviços podem ser entregues de diversas formas, seja através da contratação de empresas de tecnologia ou do provimento feito pelas próprias organizações com infraestrutura e pessoal próprio (no modelo conhecido como *on-Premise*), em diversos tipos diferentes de contrato.

Com a chegada da computação em nuvem, consolidam-se os modelos de contratação de Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS), colocando os serviços *on-Premise* sob contínua comparação em características como preço, velocidade de entrega, funcionalidades, qualidade e segurança.

Com intuito de obter a resposta para a questão da confiança nos provedores de serviço de nuvem, as normas de gestão de riscos são vistas como a descrição dos processos que melhor atenderiam as necessidades de avaliação de segurança desses serviços. Dentre as normas tradicionais de gestão de riscos podemos elencar a ISO 31000 (ABNT, 2018), a ISO 27005 (ABNT, 2019), a NC04 (GSI/PR, 2013) e o NIST Risk Management Framework (COMMERCE, 2019). Contudo, dada a complexidade das novas arquiteturas a análise de riscos demanda evolução como a constituição de programas organizados, orçamento próprio e apoio de instituições especializadas.

O estudo busca justamente mostrar uma visão holística sobre a questão, que dificilmente será obtida observando somente as normas de execução ou as práticas internas das organizações.

1.2 Objetivos

Descrever riscos fundamentais de governança que refletem as principais preocupações dos analistas e gestores de negócios baseados em ativos de TI, no quesito segurança da informação aplicado a entrega de serviços hospedados em nuvem.

Analisar de forma macro, baseando-se em regulamentos nacionais, o modelo de dois processos reais com grande repercussão na gestão de riscos das contratações de serviços em nuvem. Mapear características da evolução da prática destes processos, apoiar os gestores de sistemas e especialistas de segurança da informação e discutir o esforço empregado na execução das práticas.

1.3 Estrutura do Trabalho

O trabalho está dividido em cinco seções: introdução (seção 1), fundamentação teórica (seção 2), procedimentos metodológicos (seção 3), resultados (seção 4) e considerações finais (seção 5). A fundamentação teórica lista quatro aspectos fundamentais de governança: a condição de *lock-in*, a questão da territorialidade e jurisdição, a gestão de orçamento e custos, a capacidade e forma de categorizar quanto ao sigilo a informação que vai para a nuvem. Nos resultados e discussão são descritas duas abordagens práticas: o programa norte-americano FedRAMP (GSA, 2019) e o normativo do governo brasileiro para gerenciamento de riscos envolvendo segurança da informação nas contratações de soluções baseadas em computação em nuvem. As diferenças encontradas são discutidas nas considerações finais.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Questões fundamentais de governança

Esta seção discute questões fundamentais de governança que aparecem de forma repetida nos estudos para adoção de soluções em nuvem, impactam diretamente pilares segurança da informação (Disponibilidade, Integridade, Confidencialidade), e levam os gestores a tomar decisões que alteram o desenho dos sistemas, o desenvolvimento do serviço ou modelo de contratação. Tais questões, estão em evolução, não possuem uma solução simples definitiva e dependem de gestão e monitoramento.

2.1.1 A condição de *lock-in*

Sempre que celebrado um contrato de prestação de serviço, certo grau de dependência entre as partes é estabelecido. Em nuvem, o *lock-in* ocorre basicamente quando o contratante, depois de utilizar o serviço por algum tempo e empreender esforço para integrar sistemas, aumentando a complexidade e a dependabilidade, acaba por não poder mais portar o ativo para outro provedor ou para outra tecnologia.

Em pesquisa realizada junto aos gestores de tecnologia de pequenas e médias empresas do Reino Unido (OPARA-MARTINS; SAHANDI; TIAN, 2016), a condição de lock-in foi identificada como uma das principais preocupações para a adoção de serviços de nuvem, juntamente com a questão da segurança no provedor. A pesquisa revelou ainda que existem lacunas no tratamento da questão por parte das organizações pesquisadas.

Nos grandes provedores de nuvem, após a contratação de um serviço básico inicial, o contratante percebe a oportunidade da utilização de serviços agregados, sejam eles do próprio provedor ou de seus parceiros. Há centenas desses serviços, e normalmente, não são totalmente padronizados. A sua adoção, acaba por aumentar a complexidade das soluções. Conforme a complexidade das soluções aumenta, cresce o risco da situação de *lock-in*.

O TCU em (TCU, 2015) aponta, como possíveis consequências do risco de lock-in: a dependência frente ao fornecedor, a dificuldade em portar dados de provedor para outro por problemas de interoperabilidade, a falta de previsão dos custos de saída e a indisponibilidade do fornecedor. Para o NIST a ausência de padrões nos dados e metadados entre os diversos provedores, pode implicar no perigo da criação de ilhas de serviços não interoperáveis e no lock-in junto a um único prestador de serviço (COMMERCE, 2013).

Encontrar o equilíbrio entre aprofundar o uso e manter uma portabilidade exequível é uma tarefa importante para os gestores, e impacta diretamente no desenho do serviço.

Em muitas aplicações críticas, uma situação de *lock-in* pode comprometer os serviços prestados pela organização, ou acabar por absorver recursos que poderiam ser liberados através de uma ação de portabilidade. Por outro lado, algum grau de dependência sempre estará presente, até mesmo nos serviços *on-Premise*, com a própria equipe interna da organização.

2.1.2 Custos e Disponibilidade Orçamentária

Manter visibilidade e controle dos custos é uma questão fundamental na administração dos serviços contratados na nuvem. No datacenter *on-Premise*, muitas máquinas podem ter recursos superdimensionados ou pertencer a serviços obsoletos. Como a despesa nem sempre envolve pagamentos diretos, o uso individual de recursos de cada serviço não é necessariamente mapeado.

Já na nuvem a despesa é elástica e depende diretamente da quantidade e das características dos recursos utilizados, sendo assim fundamental manter meios de rastrear os custos em cada ativo. A mudança para nuvem exige novas formas de compreensão e execução da gestão de custos, das formas de monitoramento, da divisão de reponsabilidades entre os processos de controle, da gestão de contratos, da gestão de conformidade e muitas vezes exige até contratação de outros serviços agregados de nuvem para apoiar a gestão, que quase sempre não estão previstos no momento inicial da contratação (MAKHLOUF, 2020).

Sob a ótica de segurança, a gestão de identidades, gestão de chaves, registros de logs para auditoria, *anti-malware*, serviços de mitigação de robôs, serviços para controle de configuração dos ativos, prevenção de perdas de dados, controles de uso de aplicações estão entre os exemplos de soluções de segurança que tem custo e podem ser utilizados como aplicações centralizadas, comuns entre vários sistemas entregues em ambiente de nuvem.

2.1.3 Territorialidade e Jurisdição

Do ponto de vista tecnológico, a questão de territorialidade não é um item que limita adoção dos serviços de nuvem. Apesar de que alguns serviços possam demandar proximidade, em função da latência de conexão ou necessidade de banda para transferência de grandes blocos de informação, esta é uma condição contornável. Os grandes provedores possuem redes próprias, com excelente desempenho e bordas próximas a localização do cliente. Os casos que costumam preocupar os gestores são eventuais litígios com provedores de serviço sediados no exterior, além de possíveis violações de acesso, que em nuvem, podem fugir da capacidade de controle do gestor ou da justiça do seu país.

Não há nenhuma dúvida jurídica ao afirmar que um provedor de computação em nuvem sediado no Brasil está sujeito as leis brasileiras (VASCONCELOS, 2017). Porém,

quando se trata de um fornecedor de serviço sediado no exterior, a aplicabilidade da lei brasileira depende da presença de alguns fatores como:

- o local de celebração do contrato,
- o local do cumprimento das obrigações,
- presença de indicação contratual da observância da lei brasileira,
- se o provedor tem filial no Brasil,
- se o provedor promove oferta direcionado a consumidores brasileiros,
- se o tema é tocante à coleta, guarda, armazenamento ou tratamento de registros, dados pessoais ou de comunicações.
- se as medidas punitivas contratuais são aplicáveis no exterior.

2.1.4 Enquadramento da informação em hipótese de sigilo

A Norma Complementar no 20 IN01/DSIC/GSI/PR (GSI/PR, 2014), elenca, de forma resumida, algumas das diversas hipóteses legais de sigilo no Brasil:

- Ostensivos: Transparência ativa ou Passiva,
- Documentos Classificados: Reservado, Secreto, Ultrassecreto,
- Protegidos por lei específica: Direitos de personalidade, fiscal, bancário, comercial, empresarial, contábil, processos e procedimentos, inquérito policial, informação de natureza patrimonial (direito autoral, segredo industrial, propriedade intelectual).
- Sigilo pessoal.

Ao enquadrar os conjuntos de dados na hipótese de sigilo correspondente, os possíveis problemas que podem surgir:

- Dois gestores possuem conjuntos de dados distintos, com alguns atributos em comum, mas os enquadram em hipóteses de sigilo diferentes;
- Depois de categorizar um atributo como sigiloso, o gestor descobre conjuntos de dados externos, com os mesmos atributos, porém, enquadrados como ostensivos;
- O atributo sigiloso pode ser reidentificado através de “quasi-identificadores” (VIMERCATI; FORESTI, 2011) contidos na mesma tupla, ou em uma referência direta externa;

- Dados não estruturados dependem da visualização de documento a documento para o enquadramento, ou dependem da execução automatizada desta tarefa, o que inclui sistemas especializados como as soluções de prevenção de perda de dados como os descritos em (HART; MANADHATA; JOHNSON, 2011), além de desenvolvimento e manutenção de regras complexas;
- O trabalho de classificação ou enquadramento pode ser tão extenso, dependendo do número de sistemas e atributos, que na prática é inexequível no curto e médio prazo.

As complexas hipóteses de sigilo dispostas nas normas jurídicas não devem ser mapeadas para o mundo tecnológico da mesma forma que estão descritas. É possível agrupá-las por uma característica comum, ou ainda verificar a adequação do enquadramento delas a um determinado nível de segurança de software de forma a padronizar conjuntos de controles implementáveis.

3 PROCEDIMENTOS METODOLÓGICOS

Através de uma revisão da regulamentação em âmbito federal do Brasil e Estados Unidos foram descritos os processos e as implementações envolvendo avaliação de segurança na contratação de serviços de nuvem. A partir deste levantamento os processos foram apresentados em uma visão macro nos resultados. Os aspectos fundamentais de governança listados na fundamentação foram observados em ambos os processos e são discutidos nas considerações finais, que trazem diferenças relevantes encontradas, e propostas para novos trabalhos.

4 RESULTADOS E DISCUSSÃO

4.1 O programa de qualificação das soluções para aquisições no governo federal dos EUA

No sentido de analisar soluções de nuvem, principalmente de software como serviço, o governo americano possui uma abordagem que busca viabilizar a contratação dos sistemas em nuvem pelas suas agências através de um processo de gestão de riscos.

O framework de gestão de riscos do NIST (COMMERCE, 2019) consiste num conjunto de publicações para o suporte ao gerenciamento de riscos em segurança da informação. Os passos previstos pelos documentos do framework são: Categorizar o sistema, selecionar os controles, implementar os controles, analisar os controles, autorizar o sistema e monitorar os controles.

Os principais documentos considerados neste framework são:

- NIST 800-37 (COMMERCE, 2018): trata-se de uma publicação que descreve o processo de gestão de riscos de segurança da informação e serve como guia para a sua implementação.
- NIST 800-53 (COMMERCE, 2015): É um catálogo de controles de segurança não focado em tecnologias específicas. Os controles são divididos em famílias. O documento define ainda 3 baselines listando conjuntos de controles, baixo, moderado e alto.

As análises de risco são feitas em três níveis distintos: organizacional, de negócios e de sistemas. A qualificação das soluções é feita dentro de um escopo particular apartado do processo de contratação. Sem a qualificação de segurança, as soluções não podem ser contratadas pelas agências de governo, de forma que o processo impacta de forma direta o desenvolvimento e evolução dos serviços. Há requisitos de segurança em aquisições, no desenvolvimento de aplicações e integrações e também nos componentes de hardware, firmware e software. Requisitos também estão em políticas e procedimentos, elementos de gestão e operacionais em diferentes níveis de detalhe.

O programa norte-americano FedRAMP (GSA, 2019) é um dos exemplos de utilização deste framework. Trata-se de um programa para análise de risco, autorização e monitoramento de soluções de nuvem, serve como referência para empresas de auditoria, e é pré-requisito para aquisição destes serviços pelas agências de governo.

O processo é complementado por regulamentação fim a fim, tratando diversas questões enfrentadas por outras instituições, envolvendo, ainda as seguintes normas:

- Federal Information Security Management Act (FISMA) (US, 2002): lei americana sobre segurança da informação.
- FIPS Publication 200 (COMMERCE, 2006): requisitos mínimos de segurança para informação e sistemas de informação no âmbito federal (Implementa o FISMA 2002).

- FIPS Publication 199 (COMMERCE, 2004): usado para determinar a categoria de segurança do sistema de informação. Em primeiro lugar, a categoria (baixo, moderado e alto) é determinada, somente depois, os controles listados na NIST 800-53 (COMMERCE, 2015) são selecionados.

No catálogo NIST 800-53 (COMMERCE, 2015) os controles são organizados de forma que a instituição pode escolher conjuntos pré-definidos, para impacto baixo, moderado e alto de acordo com a classificação FIPS 199 (COMMERCE, 2004). A instituição pode selecionar os controles considerando as especificidades da aplicação bem como a disponibilidade de recursos, priorizando controles básicos e adotando novos controles de acordo com a necessidade.

A medida que os serviços são qualificados, eles seguem para a etapa de monitoramento, descrita no processo de gestão de risco do NIST (COMMERCE, 2019), e passam a alocar recursos de forma contínua.

4.2 Descrição do processo de avaliação de segurança em serviços de nuvem no Brasil

No governo federal do Brasil, não há um processo centralizado de qualificação das soluções e gestão de riscos para autorizar a aquisição. O instrumento das atas de registros de preço, pode ser utilizado para que os órgãos participem do processo de especificação, quando da necessidade da aquisição conjunta de uma mesma solução em nuvem.

Neste processo, os órgãos elaboram os estudos técnicos preliminares que contém inclusive as especificações de controles de segurança da informação (ME, 2019). No entanto, sem um procedimento de qualificação, a cada nova aquisição, os controles necessários a mitigação dos riscos de segurança da informação, que constavam no processo anterior precisam ser reestudados. Obviamente, o processo anterior serve como referência inicial para o novo, mas certamente haverá esforço a ser repetido.

Já as aquisições seguem o processo comum de contratação de bens de tecnologia da informação. Um dos artefatos do processo é um documento de análise de riscos, que contém os riscos de ordem técnica e os riscos de ordem administrativa. Após uma fiscalização no ato do recebimento, os requisitos serão monitorados durante a gestão do contrato. O processo é definido através da IN01/2019 (ME, 2019).

A Norma Complementar 14 IN01/DSIC/GSI/PR (GSI/PR, 2018) é a principal norma vigente com foco diretamente nas aplicações de nuvem. Esta norma limita a adoção de

serviços hospedados em território estrangeiro, além de colocar restrições adicionais em caso de sigilo de estado nos órgãos e entidades da administração pública federal, caso configurado através da classificação das informações. A Norma ainda preconiza a adoção de um processo de gestão de riscos e solicita que cada órgão obtenha a aprovação de seus dirigentes para continuidade da contratação.

O Acórdão 1739/2015-TCU-Plenário apresenta uma tabela contendo uma análise de gestão de riscos voltada principalmente a contratação dos serviços de nuvem de forma genérica (não aborda uma solução específica), inclui ainda controles semelhantes aos mencionados na NC 14 (GSI/PR, 2018) e também traz os requisitos de territorialidade e jurisdição, bem como a necessidade de classificar a informação (TCU, 2015).

5 CONSIDERAÇÕES FINAIS

Dentre os objetivos do estudo, foi feita uma descrição dos riscos de governança comuns a grande maioria das instituições. Os riscos envolvendo lock-in, territorialidade e jurisdição, e de controle orçamentário são desafios para o gestor na tomada de decisão para adoção de soluções de nuvem. Em particular no governo federal brasileiro, devido as oscilações de períodos de disponibilidade e indisponibilidade de recursos além de variações cambiais, os riscos envolvendo orçamento e a condição de *lock-in* formam uma dupla inseparável e crítica para decisão.

Quanto ao segundo objetivo, os principais pontos observados são discutidos a seguir. Em ambos os países questão da territorialidade e jurisdição colocada existe, mas são encontrados principalmente nos documentos citados no processo Brasileiro. A oferta majoritária de serviços é de soluções de empresas transnacionais, sediadas no exterior. Há preocupações como a aplicabilidade da lei brasileira e a imputação em território estrangeiro. Já no caso norte-americano há grande oferta de soluções de nuvem de empresas nacionais, qualificadas através do programa *FedRamp* (GSA,2019), o que facilita a decisão sobre que informações podem ir para a nuvem, pois quase sempre há alternativas de serviços sob jurisdição americana.

Quanto a forma de enquadramento da informação em hipótese de sigilo, há diferenças relevantes entre os dois processos, que tem implicações importantes na produtividade e na possibilidade de reuso das análises de risco efetuadas. O enquadramento da informação, de

acordo com a norma FIPS 199 é feito em bloco para cada sistema, de acordo com o impacto (baixo, moderado e alto) para cada um dos pilares da segurança da informação (confidencialidade, disponibilidade e integridade). Esta forma de qualificação da solução é muito mais simples, quando comparada a forma em que o gestor analisa as informações observando diretamente o enquadramento legal. Isto ocorre porque a hipótese legal de sigilo não necessariamente se desdobra em um requisito de software específico, mas sim em um conjunto macro de requisitos de segurança, com conjuntos de controles aplicáveis, necessários a proteção de toda informação, e não de apenas um ou outro atributo.

No programa FedRAMP (GSA, 2019) a avaliação se dá por solução. Uma vez qualificada, a solução fica disponível para aquisição por todos os participantes do programa, reduzindo, portanto, os esforços que seriam alocados dentro de cada instituição participante. A instituição ainda fica com a obrigação de realizar o controle vinculado ao enquadramento das informações nas categorias de impacto descritas na norma FIPS 199 (baixo, moderado e alto). Já no modelo brasileiro, os requisitos são publicados a cada contratação, e podem ser distintos, em duas contratações, para a informação enquadrada na mesma categorização, ou para o mesmo tipo de solução. A centralização de aquisições é uma forma de tentar contornar essa condição.

São propostas de trabalhos futuros: Descrever como os serviços de nuvem são implementados nos grandes provedores e alinhar essas informações aos aspectos envolvendo a jurisdição. Encontrar como as instituições estão tratando a condição de *lock-in*, de maneira pontual, alternativas e procedimentos no tratamento desta condição, bem como descrever práticas de como tratar o *lock-in* em conjunto com o orçamento. Discutir, no processo brasileiro, as formas e a regulamentação para classificação e tratamento dos dados em conjunto com a implementação dos serviços de nuvem nos provedores.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000:2018**: Gestão de riscos - Diretrizes. Rio de Janeiro, 2018. 17 p.

_____. **ISO/IEC 27005:2018**: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. Rio de Janeiro, 2019. 66 p.

BRASIL. GSI/PR**. Norma Complementar 04/IN01/DSIC/GSI/PR**. Brasília, DF, 15 fev. 2013. Disponível em: <http://dsic.planalto.gov.br/legislacao/nc_04_grsic.pdf>. Acesso em: 23

nov. 2018.

_____. **Norma complementar 14/IN01/DSIC/GSI/PR**. Brasília, DF, 19 mar. 2018. Disponível em: <http://dsic.planalto.gov.br/arquivos/documentos-pdf/NC_14_R01.pdf>. Acesso em: 25 jul. 2018.

_____. **Norma complementar 20/IN01/DSIC/GSI/PR**. Brasília, DF, 15 dez. 2014. Disponível em: <http://dsic.planalto.gov.br/legislacao/copy_of_NC20_Revisao01.pdf>. Acesso em: 23
nov. 2018.

BRASIL. MINISTÉRIO DA ECONOMIA**. Instrução normativa no 1, de 10 de janeiro de 2019**. Diário Oficial da União, Brasília, DF, 10 jan. 2019. Disponível em: <https://www.comprasgovernamentais.gov.br/index.php/legislacao/instrucoes-normativas/1068-in-1-de-2019>. Acesso em: 18 fev. 2020.

_____. **Pregão eletrônico no 29/2018**. Brasília, DF, 2018. Disponível em: <http://www.planejamento.gov.br/acesso-a-informacao/licitacoes-e-contratos/licitacoes/pregao/2018/pregao-eletronico-no-29-2018>. Acesso em: 18 fev 2020.

GSA. **FedRAMP**: The federal risk and authorization management program. 2019. Disponível em: <https://www.fedramp.gov/>. Acesso em: 05 dez. 2019.

HART M., MANADHATA P., JOHNSON R. (2011) **Text Classification for Data Loss Prevention.** In: Fischer-Hübner S., Hopper N. (eds) Privacy Enhancing Technologies. PETS 2011. Lecture Notes in Computer Science, vol 6794. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-22263-4_2.
MAKHLOUF, R. **Cloudy transaction costs**: a dive into cloud computing economics. J Cloud Comp 9, 1 (2020). DOI: https://doi.org/10.1186/s13677-019-0149-4.

OPARA-MARTINS, J., SAHANDI, R. & TIAN, F. **Critical analysis of vendor lock-in and its impact on cloud computing migration**: a business perspective. J Cloud Comp 5, 4 (2016). DOI: https://doi.org/10.1186/s13677-016-0054-z.

TCU. **Acórdão no 1.739/2015**. Brasília, DF, 15 jul. 2015. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20150720/AC_1739_24_15_P.doc>. Acesso em: 25 jul. 2018.

U.S DEPARTMENT OF COMMERCE. **FIPS 200**. 2006. Disponível em: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf>. Acesso em: 05 dez. 2019.

_____. **FIPS 199**. 2004. Disponível em: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf>. Acesso em: 05 dez. 2019.

_____. **FISMA Implementation Project**: Risk management framework (rmf) overview. 2019. Disponível em: <https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview>. Acesso em: 05 dez. 2019.

_____. **NIST-SP 500-291 v2**. 2013. Disponível em: <https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf>. Acesso em: 01 dez. 2020.

_____. **NIST SP 800-37 rev.2**. 2018. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>. Acesso em: 18 fev. 2020.

_____. **NIST SP 800-53 rev.4**. 2015. Disponível em:<https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>. Acesso em: 05 dez. 2019.

U.S. **FISMA. 2002**. Disponível em: <https://csrc.nist.gov/CSRC/media/Projects/Risk-Management/documents/FISMA-final.pdf>. Acesso em: 05 dez. 2019.

U.S. **FISMA. 2014**. Disponível em: <https://www.congress.gov/bill/113th-congress/senate-bill/2521>. Acesso em: 19 fev. 2020.

VASCONCELOS, F. V. et al. **A segurança jurídica da computação em nuvem:** Responsabilidade jurídica na proteção de dados digitais por parte dos provedores de aplicação de internet. 2017.

VIMERCATI, S. C.; FORESTI, S. Quasi-identifier. In**: Encyclopedia of Cryptography and Security**. Boston, MA: Springer US, 2011. p. 1010–1011. ISBN 978-1-4419-5906-5. DOI: https://doi.org/10.1007/978-1-4419-5906-5_763.