Tatiana Hahn: Cloud computing na Administração Pública federal

11/08/2023

Um novo normativo com diretrizes sobre o uso e contratação de serviços de computação em nuvem está em construção na Administração Pública federal e abrangerá mais de 200 órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp).

A futura Portaria do Ministério da Gestão e da Inovação em Serviços Públicos (MGI) está em fase de consulta pública até 18 de agosto [1] e substituirá o atual guia de boas práticas [2] e seus respectivos modelos, mantendo a vinculação à Instrução Normativa (IN) da Secretaria de Governo Digital (SGD/ME) nº 94 [3], de 23 de dezembro e publicada em 29 de dezembro de 2022. O objetivo é estabelecer diretrizes estratégicas sobre o uso da tecnologia com ênfase na segurança, proteção da privacidade, na integridade e na governança dos dados mantidos pelos órgãos e entidades do Sisp [4] a partir das especificidades de cada carga de trabalho.

O tema não é recente no setor público. Há quase uma década [5], frente ao contexto já progressivo de expansão da computação em nuvem no Brasil e no mundo, o Tribunal de Contas da União (TCU), embora tivesse reconhecido os diversos benefícios [6] aplicáveis à implementação da tecnologia no setor público, alertou para a existência de riscos específicos à segurança dos dados e das informações, além de barreiras em matéria contratual pela Administração, o que trouxe mais cautela na opção pela computação em nuvem na época.

Ao tempo da conclusão do relatório do TCU em 2015, as demandas pela contratação de serviços de computação em nuvem ainda eram exceção no âmbito federal e a tecnologia ofertada, segundo o TCU, apresentava falhas e deficiências nos quesitos auditados e frente aos critérios técnicos de segurança informacional. Havia posicionamentos jurídicos mais restritivos diante do então vigente Decreto nº 8.135, de 2013 (revogado pelo Decreto nº 9.637, de 2018 [7]), no sentido de que a Administração apenas poderia celebrar contratos em tecnologia da informação (e de computação em nuvem) com empresas públicas. Nesse período, a oferta de serviços em nuvem pelas empresas públicas Serpro (Serviço Federal de Processamento de Dados) e pela

Dataprev (Empresa de Tecnologia e Informações da Previdência) era limitada [8].

A partir da realização dos pregões eletrônicos entre os anos de 2018 e 2020 no âmbito do governo federal, o cenário de contratação se ampliou e a análise do mapa de riscos identificados elevou a confiança na computação em nuvem no âmbito público como um todo, não apenas na esfera federal. As características centrais da computação em nuvem, como a ampla disponibilidade e acessibilidade pela internet, elasticidade, flexibilidade, dinamicidade, o auto provisionamento, ofereceram um conjunto compartilhado de recursos computacionais indispensáveis à prestação dos serviços públicos e ao melhor desempenho da gestão e ações administrativas.

Verificou-se na computação em nuvem a estabilidade, a organização e os processos de controle necessários ao melhor desenvolvimento dos serviços e prestações públicas, notadamente com a publicação da Lei nº 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD), que disciplinou a proteção aos dados pessoais e interferiu nas políticas de privacidade, de forma específica, em relação às leis até então vigentes no país.

Em 2022, a IN SGD/ME nº 94 estabeleceu que a contratação de soluções de TIC [9] deve seguir um Termo de Referência [10] com requisitos e obrigações em Segurança da Informação e Privacidade (SIP) confeccionados a partir de critérios legais e com base nos riscos de segurança da informação e da privacidade. Segundo a IN, tal análise cabe à equipe de planejamento da contratação que especificará quais são esses requisitos e obrigações a partir das seguintes definições: a) prevejam a realização de auditoria relativa à conformidade dos requisitos de segurança da informação e privacidade previstos pela contratação, b) implementem controles criptográficos, registros de logs, políticas de segurança da informação e privacidade, c) indiquem e implementem diretrizes para o desenvolvimento e obtenção de software seguro, d) assegurem a gestão e tratamento de incidentes de forma sistematizada, e) contemplem a realização de tratamento de dados pessoais, na forma da LGPD, além do tratamento de informações classificadas, conforme legislação vigente nacional e a Lei nº 12.527, de 2011, a Lei de Acesso à Informação (LAI).

No que tange à escolha dos gestores em termos de infraestrutura, tanto a nova Portaria quanto o atual guia indicam a preferência pela adoção de uma abordagem estratégica de nuvem híbrida [11], notadamente quando o órgão ou entidade não possua maturidade suficiente na contratação de serviços em nuvem ou no caso de impedimentos técnicos ou normativos para migração de alguns *workloads*. No guia, a nuvem híbrida foi a mais recomendada como modelo de implantação para os serviços de tecnologia da informação e comunicação que não comprometessem a segurança nacional [12] e acolhia tanto fornecedor público quanto privado.

Pela infraestrutura da nuvem híbrida, a Administração Pública conjuga os benefícios dos modelos de nuvem pública (elasticidade e agilidade) com os da nuvem privada (desempenho garantido devido ao recurso dedicado). Ela permite também minimizar os riscos à descontinuidade dos serviços, à preservação e à integridade dos dados, além de otimizar os investimentos e custos. Acrescenta-se ainda que, ao contexto que a Administração Pública federal, a portaria em regime de consulta pública trabalha o conceito de nuvem de governo como aquela que pode ser tanto uma nuvem privada ou uma nuvem comunitária, mas que são

geridas exclusivamente por órgãos ou empresas públicas.

Caso a opção seja por um fornecedor privado e especificamente no que tange à mitigação dos riscos relativos à segurança da informação, entende-se que os órgãos federais deverão exigir, nos termos do guia vigente, no momento da contratação de serviços em nuvem, que o ambiente do serviço contratado esteja em conformidade com a norma ABNT NBR ISO/IEC 27001:2013. A norma técnica especifica quais são os requisitos para implementar, estabelecer e melhorar, de modo contínuo, um sistema de gestão da segurança da informação a partir do contexto de cada organização.

O objetivo dessa norma técnica é manter a confidencialidade, a disponibilidade e a integridade da informação através da gestão de riscos internos e externos. O texto da Portaria em consulta até o dia 18 de agosto, ao contrário, não faz qualquer menção específica à ISO 27001, tendo disposto, de forma mais geral, ao atendimento padrão ISO ao tratar sobre datacenters, serviços prestados pelo integrador (*cloud broker*) e acerca da padronização vocabular no campo da computação em nuvem com a referência à recente ISO/IEC 22123-1:2023.

Ocorre que, especificamente quanto à privacidade e à proteção de dados pessoais, a Organização Internacional de Normalização (ISO) publicou uma nova versão da norma ISO/IEC 27001:2013, a qual foi lançada em outubro de 2022 pela ABNT. Embora a ISO 27001 seja a norma principal, as organizações já certificadas pela versão de 2013 terão até 2025 para se atualizarem com a ISO/IEC 27002. A ISO/IEC 27002 incorporou recursos e controles mais intensos justamente ao resguardo de informações críticas e sensíveis das organizações com ênfase à melhor gestão da segurança da informação, à proteção da privacidade e aos desafios da cibersegurança. A norma trouxe alterações mais substanciais no seu Anexo A, no qual se identifica o quanto as organizações precisam intensificar a compreensão e a clareza (em seus processos, procedimentos, por parte de seus usuários e colaboradores) sobre a rigidez da segurança informacional e à importância de uma cultura à privacidade.

Aliás, a norma confere controles adicionais à segurança da informação para uso de serviços em nuvem e enfatiza a necessidade de exigência pelas organizações de padrões de segurança que são mais específicos para serviços em nuvem. Também ganharam espaço o planejamento de mudanças, quantidades de controles indicados pela ISO, a atenção a vulnerabilidades por vazamentos, o controle de acessos (filtragem) a sites pelos usuários, o gerenciamento de configurações para evitar alterações não autorizadas, o mascaramento de dados voltado à proteção de informações e o controle à exclusão de dados não necessários, o qual atende os interesses de preservação da privacidade e do princípio da finalidade.

Essas alterações corroboram o que Daniel Solove e Woodrow Hartzog defendem em termos de segurança da informação e incidentes em dados pessoais. Mesmo após um significativo período de vigência de leis em matéria de proteção de dados pessoais e privacidade com notório amadurecimento da matéria no contexto organizacional, as violações a dados envolvem os mesmos erros identificados no passado.

Os autores argumentam que as organizações públicas e privadas investem vultuosas somas de dinheiro em tecnologias de segurança da informação, em serviços tais como computação em

nuvem, mas o principal ainda é identificar uma forma assertiva e eficaz de treinamento e capacitação dos envolvidos nesses processos [13]. As organizações investem muitas vezes em treinamentos longos e desmotivadores, sem focar no engajamento humano e na conscientização do porquê e do quanto a proteção dos dados e da privacidade é tão fundamental. Isto é, ainda se desconsidera, na prática, que o investimento central deve estar nas pessoas, pois são elas (somos nós) as mais suscetíveis a falhas, ao esgotamento mental frente à insuficiência nas equipes, o que gera uma réplica de ciclos internos pela impossibilidade de criação e identificação de aprimoramentos. Outro ponto que igualmente se conecta nesse cenário e atinge a gestão de riscos, a governança de dados e à eficiência pública é o armazenamento excessivo, duplicado, desnecessário de dados sejam eles pessoais ou não.

Essas são preocupações que integram a futura Portaria no tópico sobre gerenciamento dos principais riscos desde o planejamento, uso até a fase de transição e encerramento contratual da computação em nuvem quando o órgão ou entidade deve estabelecer um procedimento com, no mínimo, a obrigação do integrador/provedor na devolução dos dados, informações e sistemas à contratante pública, com a respectiva eliminação de dados e a garantia ao direito ao esquecimento para os dados pessoais.

Nesse contexto, os desafios em segurança da informação e proteção de dados pessoais vivenciados pelos maiores atores do setor privado são igualmente enfrentados pelo setor público. Contudo, no setor público o dever de prestar contas, de transparência, de atenção aos princípios da legalidade e da participação, bem como a necessária otimização de recursos financeiros e humanos, impõe controles internos e externos intensos e de maior proporção. Em maio de 2023, a Autoridade Nacional de Proteção de Dados (ANPD) listou a Serpro e a Dataprev (empresas públicas e fornecedores de serviços de nuvem) entre os entes públicos com fiscalização em curso [14] e demonstrou essa tendência de rigor no controle e no monitoramento das empresas públicas federais que coletam e realizam tratamento de dados e de dados pessoais. Isso, além de trazer mais confiança também aos serviços em nuvem prestados no setor público e privado pelas empresas públicas, reverte em incentivos responsivos aos processos de verificação, às auditorias, às revisões internas com ganhos de eficiência, de aperfeiçoamento das técnicas de segurança e promove uma cultura organizacional de proteção de dados pessoais entre os atores envolvidos nessas atividades.

A computação em nuvem e a proteção de dados pessoais têm nos oferecido uma lição valiosa quanto ao nosso *modus operandi* diante dos benefícios e riscos do avanço da tecnologia: precisamos reforçar os elementos de motivação ativa e de tomada de decisão humanas. Por um lado é importante renovar e ampliar critérios de segurança, aprimorar normas e controle, revisar padrões técnicos e guias, na busca pela maior mitigação possível dos riscos à segurança informacional e à proteção de dados pessoais. Por outro, os melhores resultados extraíveis desses recursos tecnológicos dependem das pessoas que operam e aplicam esses procedimentos, normas, padrões, controles e revisões. Por isso, é crucial centralizar esforços, de forma repetida e incansável, na capacitação e na difusão compreensiva da fundamentalidade da privacidade dentro de cada contexto organizacional seja ele utilizador ou não da computação em nuvem. Será pelo engajamento participativo das equipes, de capacitações orgânicas e não meramente formais que as práticas de segurança e de privacidade melhor se sustentarão ao longo do tempo e que permitirão antecipar potenciais riscos e resolver, de forma ágil e menos

danosa, eventuais incidentes com dados.

[1] Consulta pública vigente entre 28 de julho a 18 de agosto. Disponível em: https://www.gov.br/gestao/pt-br/assuntos/noticias/2023/julho/gestao-abre-consulta-publica-sobre-modelo-de-contratacao-de-software-e-servicos-de-computacao-em-nuvem. Acesso em: 28 jul. 2023

[2] Segundo o texto em consulta para nova Portaria, o novo modelo irá substituir o Guia de Boas Práticas para Contratação de Serviços de Computação em Nuvem e deverá ser observado nos planejamentos da contratação iniciados após a respectiva publicação. No entanto, será facultativa a adoção da nova Portaria para os processos cujo planejamento da contratação tenha se iniciado antes de sua publicação ou para os casos de prorrogação de contratos anteriores.

[3] Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação (TIC) pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp) do Poder Executivo Federal.

[4] Aplica-se também a Instrução Normativa SGD/MGI nº 6, de 29 de março de 2023, que regulamenta os requisitos e procedimentos para aprovação de contratações ou de formação de atas de registro de preços, a serem efetuados por órgãos e entidades integrantes do SISP quanto a bens e serviços de TIC, tendo em vista o artigo 2º, da Lei nº 14.133, de 2021.

[5] No Anexo I, do Acórdão nº 1.739, do TCU, foram listados os riscos, os controles possíveis e os critérios de segurança analisados, tendo por base o tema da segurança da informação. Disponível em: https://pesquisa.apps. tcu.gov.br/redireciona/acordao-completo/%22ACORDAO-COMPLETO-1470754%22. Acesso em: 23 jul. 2023.

[6] Conforme os levantamentos realizados entre 2014 e 2015 pelo TCU, reunidos no referido Acórdão nº 1739, de 2015, o modelo de computação em nuvem poderia trazer benefícios como: maior agilidade na entrega e na atualização tecnológica de serviços públicos; ampliação do acesso e do uso de informações governamentais; suporte mais ágil a iniciativas de big data e dados abertos; atendimento de demanda sazonal de serviços pela Internet sem necessidade de alocar grande quantidade de recursos fixos de tecnologia da informação e que são subutilizados em momentos de pouco uso, redução de custos de infraestrutura e de serviços de Tecnologia da Informação notadamente frente aos ganhos de escala; otimização da produtividade das equipes de trabalho administrativo, de suporte e de tecnologia, aprimoramento do suporte de operações de missão crítica; a maior disponibilidade dos serviços de TI oferece melhor produtividade do usuário final; aumento da resistência a ataques contra a disponibilidade dos serviços; redução do tempo para implementação de novos serviços e ciclo mais rápido de inovação. In: BRASIL. Tribunal de Contas da União. Acórdão nº 1.739, 15 de julho de 2015, Plenário. Relator Ministro

Benjamin Zymler.

[7] O Decreto nº 9.637, de 26 de dezembro de 2018, instituiu a Política Nacional de Segurança da Informação (PNSI) para APF com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional.

[8] A afirmação não ignora o projeto "Expresso em Nuvem" lançado em dezembro de 2010 por duas empresas públicas brasileiras e visava oferecer uma solução em código aberto, com redução de gastos públicos, ampliar a independência tecnológica nacional, gerar investimentos na produção e compartilhamento de conhecimento no âmbito do serviço público com expansão a todos os poderes e camadas federativas. Isso porque se verificou que as contratações de solução de correio eletrônico corporativo demandavam investimentos robustos por parte das organizações. Pelo projeto Expresso em Nuvem, a Serpro e a Dataprev ofereciam uma suíte de comunicação completa, que agrega correio eletrônico, agenda, mensageria instantânea, serviços VoIP, workflow, diretório único de governo, sincronização de mensagens e agenda com dispositivos móveis (celular). O serviço foi considerado o primeiro serviço em nuvem do governo brasileiro. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-antigas/serpro-e-dataprev-lancam-expresso-em-nuvem. Acesso em: 23 jul. 2023.

[9] Importante referir que a IN nº 94, de 2022, considera como soluções de TIC "*os bens e/ou serviços que se adequam à definição de pelo menos*" uma das treze categorias constantes no Anexo II da IN para cada qual a INS também lista itens excluídos dentro de cada uma dessas categorias. São elas: materiais e equipamentos de TIC, desenvolvimento e sustentação de sistemas, hospedagem de sistemas; suporte e atendimento ao usuário de TIC, infraestrutura de TIC, comunicação de dados, *software* e aplicativos, impressão e digitalização, consultoria em TIC, computação em nuvem, internet das coisas (IoT), segurança da informação e privacidade e análise de dados, aprendizado de máquina e inteligência artificial. No caso da proteção de dados pessoais e da privacidade e da computação em nuvem a IN considera como recurso: a) na computação em nuvem recursos exemplificativos: a *Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Data Base as a Service (DBaaS), Device as a Service (DaaS), Containers as a Service (CaaS), Function as a Service (FaaS) e Big Data as a Service (BDaaS)*, serviços de orquestração de multi-nuvem, suporte e *brokerage* de nuvem e; b) na segurança da informação e privacidade: os serviços de avaliação e testes de segurança, gestão de vulnerabilidades e tratamento de incidentes, *Security as a Service* (SECaaS), segurança de redes, Serviço de Monitoria de eventos de segurança (SOC) e serviços técnicos de consultoria em segurança da informação e privacidade, com exclusão dos serviços e/ou equipamentos de segurança das informações que não estejam em suporte digital. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=29/12/2022&jornal=515&pagina=1. Acesso em: 23 jul. 2023.

[10] Por termo de referência são considerados os conceitos do artigo 6º, incisos XX e XXIII, da Lei nº 14.133, de 2021.

[11] A Portaria em consulta conceitua nuvem híbrida como a "*infraestrutura de nuvem composta por duas ou mais infraestruturas distintas (privadas, comunitárias ou públicas), que permanecem com suas próprias características, mas agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações*". Disponível em: https://www.gov.br/participamaisbrasil/modelo-de-contratacao-de-software-e-nuvem. Acesso em: 28 jul. 2023. Christopher Millard, Jatinder Singh e W. Kuan Hon analisam aspectos essenciais e introdutórios à computação em nuvem e apresentam como uma classificação amplamente utilizada a divisão em quatro modelos de implementação: a) nuvem privada, quando a infraestrutura relevante seja de propriedade de um único grande cliente ou de um grupo de entidades relacionadas; b) nuvem compartilhada (*community cloud*), quando a infraestrutura é de propriedade ou é operada e partilhada entre um grupo específico de clientes com interesses comuns, tais como agências governamentais ou instituições financeiras; c) nuvem pública, na qual a infraestrutura é compartilhada entre vários clientes usando o mesmo hardware e/ou software e; d) nuvem híbrida é a união ou mistura de nuvens e de suas funcionalidade de acordo com a finalidade pretendida pelo contratante. MILLARD, Christopher J. (ed.). *Cloud computing law.* 2. ed. Oxford: Oxford University Press, 2021.

[12] Compete à autoridade máxima de cada órgão, com apoio do Comitê de Governança Digital, do Comitê de Segurança da Informação e Comunicações e do Comitê Estratégico de Tecnologia da Informação, a definição dos serviços de Tecnologia da Informação e Comunicação, no todo ou em parte, que possam comprometer a segurança nacional, conforme os requisitos de confidencialidade, integridade, disponibilidade e autenticidade das informações envolvidas.

[13] SOLOVE, Daniel J.; HARTZOG, Woodrow. *Data Vu: why breaches involve the same stories again and again. scientific american. GWU Legal Studies Research Paper.* nº 2023-24, 2022. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4326723. Acesso em: 25 jul. 2023.

[14] Cabe referir que a Secretaria de Governo Digital (SGD) regulamentou o Programa de Privacidade e Segurança da Informação (PPSI), aplicável a 251 órgãos e entidades do governo federal integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), pela edição da Portaria SGD/MGI nº 852, de 28 de março de 2023, que dispõe sobre o Programa de Privacidade e Segurança da Informação (PPSI) e de um guia para sua implementação.

Fonte: https://conjur.jumps.com.br/2023-ago-11/tatiana-hahn-cloud-computing-administracao-publica-federal/