

## COMPUTAÇÃO EM NUVEM

A computação em nuvem (*cloud computing*) é um modelo que possibilita acesso universal e sob demanda a um conjunto compartilhado de recursos computacionais (por exemplo: servidores, armazenamento de dados, redes e aplicações), disponibilizados de forma a minimizar o esforço de gerenciamento e a interação com o provedor de serviços. Além disso, o modelo destaca-se pelas características essenciais de autoprovisionamento, alta disponibilidade, amplo acesso pela Internet, rápida elasticidade e serviços medidos por utilização.

A tecnologia pode ser utilizada de diferentes maneiras, dependendo das necessidades de uso e de negócio. Considerando as formas de implantação, existem basicamente quatro categorias de nuvem: pública, privada, comunitária e híbrida. Os serviços mais conhecidos e populares de nuvem estão em nuvens públicas, como correio eletrônico e armazenamento de arquivos.

Conforme a arquitetura dos serviços, existem três categorias: *software* como serviço (*software as a service* – SaaS), plataforma como serviço (*platform as a service* – PaaS) e infraestrutura como serviço (*infrastructure as a service* – IaaS). Na categoria SaaS, aplicações como ferramentas de produtividade de escritório e sistemas integrados de gestão são disponibilizadas para o cliente em infraestrutura de nuvem do próprio fornecedor; na PaaS, são fornecidos recursos como banco de dados, plataforma para desenvolvedores de aplicações e infraestrutura para execução de aplicações do próprio cliente; e na IaaS, são providos recursos de computação fundamentais (*hardware*, armazenamento e rede) nos quais o cliente pode instalar *softwares* em geral, incluindo sistemas operacionais e aplicativos.

### Objetivo do levantamento

Devido à crescente adoção dessa tecnologia, o TCU realizou, entre outubro de 2014 e fevereiro de 2015, levantamento com o objetivo principal de identificar os riscos mais relevantes em contratações pela Administração Pública Federal (APF) de serviços de computação em nuvem.

Para tanto, o trabalho abordou aspectos que vão desde conceitos e modelos de computação em nuvem, vantagens da adoção da tecnologia, modelos de comercialização de serviços, normas e padrões internacionais, quadro normativo brasileiro, até o panorama atual da contratação de serviços de computação em nuvem pela APF.

### Principais conclusões do TCU

O modelo de computação em nuvem pode trazer diversos benefícios, como: 1) redução de custos de infraestrutura e de serviços de Tecnologia da Informação (TI) devido a ganhos de escala; 2) otimização da produtividade da equipe de TI, melhorando o suporte de operações de missão crítica; 3) maior disponibilidade dos serviços de TI e conseqüente melhor produtividade do usuário final; 4) resistência a ataques contra a disponibilidade dos serviços; e 5) redução do tempo para implementação de novos serviços e ciclo mais rápido de inovação. Para a administração pública, a adoção de computação em nuvem traz ainda benefícios adicionais, 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; e
- atendimento de demanda sazonal de serviços pela Internet sem necessidade de alocar grande quantidade de recursos fixos de TI, que ficam subutilizados em momentos de pouco uso.

Entretanto, à época do trabalho, as iniciativas de uso de serviços de computação em nuvem ainda constituíam exceção no âmbito da APF. De maneira geral, os gestores continuavam cautelosos, em especial por causa de preocupação com riscos à segurança das informações, bem como por incerteza quanto a uma interpretação mais restritiva do Decreto 8.135/2013 de que a APF deveria contratar exclusivamente as empresas públicas de TI para serviços de computação em nuvem. Das empresas públicas que podem prestar esses serviços, a Dataprev ainda não tinha iniciado sua comercialização, e a oferta do Serpro era limitada.

Desse modo, um provável represamento de projetos dessa natureza, por causa de receio por parte dos gestores e de limitações de capacidade das empresas públicas de TI, poderia levar ao não aproveitamento de oportunidades geradas pela computação em nuvem.

Esse novo modelo, apesar de introduzir certos riscos, como os derivados da terceirização e do compartilhamento de recursos, mitiga uma série de outros problemas tão comuns à TI, como a falta de capacidade de expansão e a demora na implantação de ambientes ou sistemas. Há riscos relativos à segurança da informação que necessitam ser considerados pelo gestor, mas há de se ponderar também que as defesas baseadas em nuvem muitas vezes são mais robustas, escaláveis, eficientes e baratas se comparadas às soluções internas, em razão da especialização dos provedores e do ganho de escala.

As organizações devem analisar os riscos existentes e diversos fatores, econômicos e técnicos, para fundamentar a decisão de contratar ou não um serviço de computação em nuvem, bem como ajustar previamente a contratação. De todo modo, pode-se iniciar com aplicações contendo informações públicas e não críticas, com baixo risco de segurança da informação.

### Principais riscos identificados pelo TCU

Com a finalidade de facilitar a utilização tanto pelo gestor – quando do planejamento da contratação – como pelo auditor, foi estruturada uma tabela contendo possíveis controles associados aos riscos identificados, bem como referências de critérios (normas e boas práticas).

Os 43 riscos identificados foram agrupados em quinze categorias de risco, que, por sua vez, também foram agrupadas em quatro temas: “segurança da informação”, “governança e gestão de riscos”, “contratação e gestão contratual” e “infraestrutura de TI”.

No tocante a riscos inerentes à APF, destaca-se o risco de desconformidade com normativos brasileiros, como as normas do DSIC/GSI/PR, o Decreto 8.135/2013 e a Portaria Interministerial 141/2014.

Ademais, em razão da transformação de despesa de capital em despesa de custeio, há risco de estouro do orçamento disponível em razão de um consumo maior que o previsto, o que poderia acarretar a interrupção dos serviços por falta de recursos.

### Benefícios esperados

Este levantamento permitiu a identificação de oportunidades de atuação do controle externo na área de computação em nuvem. Além disso, foram elaboradas uma tabela de riscos e possíveis controles associados à contratação de serviços de computação em nuvem e também uma matriz de referência contendo questões, procedimentos e possíveis achados de auditoria, de modo a auxiliar os auditores do TCU em futuras fiscalizações.

Desse modo, as informações obtidas e os riscos identificados orientarão os gestores da APF e subsidiarão futuros trabalhos do TCU no campo da computação em nuvem, formato inovador no fornecimento de soluções e na prestação de serviços de TI.

### Acórdão

Acórdão: 1.739/2015-TCU-Plenário

Data da sessão: 15/7/2015

Relator: Ministro Benjamin Zymler

TC: 025.994/2014-0

Unidade técnica responsável: Secretaria de Fiscalização de Tecnologia da Informação (Sefti), com apoio da Secretaria de Infraestrutura de TI (Setic)