**MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO**

Secretaria de Tecnologia da Informação

Departamento de Infraestrutura e Serviços de Tecnologia da Informação

*Este documento de Boas práticas, Orientações e Vedações tem força normativa legal, estando vinculado à Portaria MP/STI nº 20, de 14 de junho de 2016, na forma de anexo, tendo sido assinado, em sua última versão, pelo Secretário de Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão em 13/05/2016 e publicado na mesma data.*

# Boas práticas, orientações e vedações para contratação de Serviços de Computação em Nuvem

Considerando os avanços tecnológicos, a computação em nuvem se tornou uma realidade plenamente acessível às organizações, sendo mundialmente adotada por empresas e órgãos de governo. Dentre os benefícios da adoção deste modelo, destacam-se: redução de custos, elasticidade, redução da ociosidade dos recursos, agilidade na implantação de novos serviços, foco nas atividades finalísticas do negócio e uso mais inteligente da equipe de TI.

Em comparação aos proveitos da computação em nuvem, o uso de salas-cofre e salas seguras torna-se dispendioso, com perda de escala e eficiência, além de apresentar maior complexidade de operação e manutenção de equipamentos.

1. Fica vedada a contratação de salas-cofre e salas seguras por órgãos integrantes do SISP.
    i. Solicitações de excepcionalização ao disposto no caput deverão ser submetidas pelo órgão, com as devidas justificativas, à apreciação da STI.
2. Compete à autoridade máxima do 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 (TIC), no todo ou em parte, que possam comprometer a segurança nacional, conforme os requisitos de confidencialidade, integridade, disponibilidade e autenticidade das informações envolvidas, em conformidade com a IN Nº 01 GSI/PR/2008 e suas Normas Complementares, e considerando os princípios de acesso à informação e sua imprescindibilidade à segurança do Estado e da sociedade, dispostos pela Lei nº

12.527, de 18 de novembro de 2011, Decretos nº 7.724, de 16 de maio de 2012, e nº 7.845, de 14 de novembro de 2012, e outras legislações específicas.

3. Para os casos de serviços de TIC que não comprometam a segurança nacional, incluindo Serviços de TIC Próprios, recomenda-se aos órgãos contratar preferencialmente Nuvem Híbrida, como Modelo de Implantação, de fornecedor público ou privado. Com isso, é possível valer-se dos benefícios dos modelos de nuvem pública (elasticidade e agilidade) e privada (desempenho garantido devido ao recurso dedicado), e ao mesmo tempo minimizar os riscos e otimizar os custos advindos de cada modelo.
4. Os órgãos deverão exigir, no momento da contratação de serviços em nuvem de fornecedores privados, que o ambiente do serviço contratado esteja em conformidade com a norma ABNT NBR ISO/IEC 27001:2013, sem prejuízo de outras exigências, objetivando mitigar riscos relativos à segurança da informação.
5. Para os casos de serviços de TIC que possam comprometer a segurança nacional, os órgãos devem contratar serviços de computação em nuvem com os órgãos ou entidades da Administração Pública Federal ou podem realizar diretamente Serviços de TIC Próprios.
    i. No caso dos Serviços de TIC Próprios, quando comprometer a segurança nacional, sua operação não poderá ser compartilhada ou contratada de terceiros.
6. A contratação de serviços em nuvem deverá respeitar a seguinte ordem de prioridade, quanto a capacidade de serviços que possa atender as necessidades do contratante:
    i. Software como Serviço (SaaS);
    ii. Plataforma como Serviço (PaaS);
    iii. Infraestrutura como Serviço (IaaS).
7. Os órgãos que não possuem infraestrutura de TI própria ou que necessitem renová-la ou ampliá-la devem contratar Infraestrutura como Serviço (IaaS).

    i. A contratação direta de equipamentos de infraestrutura de TI, como por exemplo, servidores e *storages*, somente poderá ser feita mediante justificativa aprovada previamente pela autoridade máxima do órgão ou pelo Comitê de Governança Digital, ou equivalente, caso esse tenha delegação para tal.

8. Os órgãos deverão exigir, por meio de cláusulas contratuais, em conformidade com o disposto na NC 14/IN01/DSIC/GSIPR, que os dados e informações do contratante residam exclusivamente em território nacional, incluindo replicação e cópias de segurança (*backups*), de modo que o contratante disponha de todas as garantias da legislação brasileira enquanto tomador do serviço e responsável pela guarda das informações armazenadas em nuvem.

9. Os órgãos deverão adotar o foro brasileiro para dirimir quaisquer questões jurídicas relacionadas aos contratos firmados entre o contratante e o fornecedor do serviço.

10. Na contratação de serviços em nuvem com empresas privadas os órgãos deverão exigir disponibilidade de no mínimo, 99,741% para os data centers onde os serviços estarão hospedados, aceita a comprovação por meio de certificação TIA 942 TIER II.

11. Os órgãos deverão assegurar, por meio de cláusulas contratuais, que o serviço a ser contratado permita a portabilidade de dados e aplicativos e que as informações do órgão contratante estejam disponíveis para transferência de localização, em prazo adequado e sem custo adicional, de modo a garantir a continuidade do negócio e possibilitar a transição contratual.

12. Os órgãos deverão assegurar, quando aplicável e por meio de cláusulas contratuais, que as informações sob custódia do fornecedor serão tratadas como informações sigilosas, não podendo ser usadas por este fornecedor ou fornecidas a terceiros, sob nenhuma hipótese, sem autorização formal do contratante.

## Glossário

### Computação em Nuvem

Computação em Nuvem é um modelo que permite acesso ubíquo, conveniente e sob demanda, através da rede, a um conjunto compartilhado de recursos computacionais configuráveis (por exemplo: redes, servidores, armazenamento, aplicações e serviços), que podem ser rapidamente provisionados e disponibilizados com o mínimo de esforço de gerenciamento ou de interação com o provedor de serviços.

### Sala-cofre

A Sala Cofre é um sistema modular composto por painéis remontáveis, para proteção física de equipamentos de hardware, formando uma Sala dentro de Sala. Pode ser montada com o data center em funcionamento, sendo possível ampliá-la ou mudá-la para outro local, conforme a necessidade do cliente, o que preserva o investimento realizado. Para ser classificado como sala-cofre, o ambiente deve estar em conformidade com as normas ABNT NBR 15247 (teste de fogo, calor e umidade; teste de resistência a desmoronamentos).

### Sala segura

Possui todas as características de uma sala-cofre, exceto a certificação ABNT NBR 15247. No entanto, uma sala segura deve estar em conformidade com outras certificações internacionais equivalentes, como por exemplo, a EN 1363-1.

### Modelos de Implantação

Nuvem Pública

É uma infraestrutura de nuvem que está disponível para uso público e que reside nas instalações do provedor. Pode ser da própria organização ou operada por terceiros, ou uma combinação. A infraestrutura física é compartilhada. No entanto, há uma separação lógica por cliente.

Nuvem Privada

A infraestrutura de nuvem privada está alocada para uso exclusivo de um único cliente. Sua utilização, gerenciamento e operação podem ser feitos pelo cliente, em suas dependências ou nas do provedor. Além disso, a nuvem privada tem sua flexibilidade reduzida.

Nuvem Híbrida

Este tipo de nuvem é uma composição de duas infraestruturas de nuvem (privada e pública), interligadas por tecnologias apropriadas que permitem portabilidade de aplicações e de dados entre as nuvens.

É possível utilizar essa abordagem para valer-se dos principais benefícios dos modelos público (elasticidade) e privado (desempenho garantido devido ao recurso dedicado), e ao mesmo tempo minimizar os riscos e otimizar os custos advindos de cada modelo, sempre que existirem necessidades distintas associadas a determinados tipos de usuários ou de dados.

**Tipos de Capacidade (de acordo com a arquitetura dos serviços disponibilizados pela nuvem)**

Infraestrutura como Serviço - IaaS

É o provisionamento pelo fornecedor de processamento, armazenamento, comunicação de rede e outros recursos fundamentais de computação, nos quais o cliente pode instalar e executar softwares em geral, incluindo sistemas operacionais (que pode vir instalado) e aplicativos. O cliente não gerencia nem controla a infraestrutura subjacente da nuvem, mas tem controle sobre o espaço de armazenamento e aplicativos instalados.

Plataforma como Serviço – PaaS

Os recursos fornecidos são linguagens de programação, bibliotecas, serviços e ferramentas de suporte ao desenvolvimento de aplicações, para que o cliente possa implantar, na infraestrutura da nuvem, aplicativos criados ou adquiridos por ele. O cliente não gerencia nem controla a infraestrutura subjacente da nuvem que são fornecidos como IaaS (rede, servidores e armazenamento), mas tem controle sobre as aplicações implantadas e possivelmente sobre as configurações do ambiente que as hospeda.

*Software* como Serviço - SaaS

Neste modelo, o cliente tem a possibilidade de utilizar aplicações do provedor de serviços na infraestrutura de nuvem, que são acessíveis de forma transparente independente de dispositivo (*desktops*, *tablets*, *smartphones*, etc.). Essencialmente, trata-se de uma forma de trabalho cuja aplicação é oferecida como serviço, eliminando-se a necessidade de se adquirir licenças de uso e infraestrutura de TI (fornecida como IaaS) para utilizá-la. O cliente gerencia apenas as configurações dos aplicativos, específicas do usuário;

**Portabilidade**

Capacidade que permite às aplicações e dados operarem em qualquer modelo de nuvem, ofertados por fornecedores distintos, sem a necessidade de reescrever códigos de aplicações, converter bancos de dados, alimentar os sistemas com informações dos usuários ou mesmo alterar características das aplicações.

**Elasticidade**

Permite aumentar ou reduzir de forma simples e dinâmica, sem interrupções e em tempo de execução, a quantidade de recursos computacionais utilizados, suprindo, desta forma, momentos de picos de demanda.

**Confidencialidade**

Propriedade que limita o acesso à informação somente às entidades autorizadas pelo proprietário da informação.

**Integridade**

Propriedade que assegura que a informação manipulada mantém todas as características originais estabelecidas pelo proprietário da informação.

**Disponibilidade**

Propriedade que garante que a informação esteja sempre disponível para o uso dos usuários autorizados pelo proprietário da informação.

**Autenticidade**

Propriedade que garante que a informação provém da fonte anunciada e que não foi alterada no decorrer de um processo.

**Serviços de TI Próprios**

Caracteriza-se Serviço de Tecnologia da Informação próprio quando o órgão realiza, diretamente e por meios próprios, a gestão e a administração desse serviço, visando garantir segurança e auditabilidade da informação e comunicação.

**Classificação de data centers em Tiers de acordo com a norma TIA 942**

A classificação Tier adotada em data centers foi desenvolvida pelo Uptime Institute, nos EUA, é usada desde 1995 e tem reconhecimento mundial. Os níveis de disponibilidade associados às classificações *Tier* foram determinados por meio de resultados de análises de disponibilidade de data centers reais.

Tier I

Data center básico que possui componentes internos não redundantes e uma rota de alimentação externa (energia e conexão de dados) não redundante servindo ao ambiente crítico. A infraestrutura Tier I inclui um espaço dedicado para os sistemas de TI; um sistema UPS (*no-break*) para lidar com falhas momentâneas no fornecimento de energia; um equipamento dedicado de refrigeração e um sistema gerador para proteger as funções de TI de falhas prolongadas no fornecimento de energia. A disponibilidade para o Tier I é de 99,671%.

Tier II

Data center Tier II possui componentes internos redundantes e uma rota de distribuição de alimentação externa (energia e conexão de dados) não redundante servindo ao ambiente crítico. Os componentes redundantes são: geradores, sistemas UPS (*no-break*), sistemas de refrigeração e tanques de combustível. Esses componentes podem ter seu funcionamento interrompido, seguindo um plano de manutenção, por exemplo, sem a necessidade de desligar qualquer um dos equipamentos críticos de TI. A disponibilidade para o Tier II é de 99,741%.

Tier III

Data center paralelamente sustentável que possui componentes de capacidade redundantes e múltiplas rotas independentes de distribuição (energia e conexão de dados) que servem o ambiente crítico. Apenas uma rota de distribuição é necessária para servir o ambiente crítico em qualquer momento. Qualquer componente nas rotas de distribuição pode ser interrompido sem impactar qualquer equipamento do ambiente crítico. A disponibilidade para o Tier III é de 99,982%.

Tier IV

Data center tolerante a falhas composto por vários sistemas fisicamente independentes e isolados, componentes redundantes e múltiplas rotas independentes de alimentação (energia e conexão de dados) ativas simultaneamente, servindo ao ambiente crítico. Sistemas complementares e rotas de distribuição devem estar fisicamente isolados um do outro (compartimentalizados) para prevenir qualquer tipo de incidente de impactar simultaneamente os sistemas ou as demais rotas de distribuição / alimentação. A disponibilidade para o Tier IV é de 99,99%.

**Fontes**

Acórdão 1739/2015-TCU-Plenário.

*National Institute of Standards and Technology* – NIST.

NC 14 14/IN01/DSIC/GSIPR

*Uptime Institute Professional Services – Data Center Site Infrastructure Tier Standard.*