MINISTÉRIO DA AGRICULTURA E PECUÁRIA
COORDENAÇÃO DE GESTÃO DE REDES, DATACENTERS E COMPUTAÇÃO EM CLOUD

DOCUMENTO DE ESTRATÉGIA DE USO DE SOFTWARE E DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM

DOCUMENTO DE ESTRATÉGIA DE USO DE SOFTWARE E DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM

Dispõe sobre as estratégias de contratação de serviços de computação em nuvem no âmbito do Ministério da Agricultura e Pecuária, órgãos e entidades integrantes do MAPA.

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art.1º Estabelecer as diretrizes das contratações de serviços de computação em nuvem que deverão ser realizadas observando-se o processo de contratação de soluções de tecnologia da informação e comunicação e o seu uso seguro; disposto pela Instrução Normativa SGD/ME nº 94, de dezembro de 2022 regida pela Lei nº 14133, de 2021; Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023.

Devem-se observar as seguintes orientações:

a) avaliar a viabilidade de utilização de modelos já adotados na Administração, pois aumenta o nível de padronização nas contratações no âmbito do SISP;

b) não utilizar métrica de remuneração cuja medição não seja passível de verificação, nos termos da Súmula TCU 269;

c) avaliar a economicidade dos preços estimados e contratados, realizando a análise crítica da composição de preços unitários e do custo total estimado da contratação; e

d) abster-se de criar unidades de medida de forma unilateral, sem prévia avaliação técnica, econômica e de padronização.

CAPÍTULO II

DEFINIÇÃO DOS SERVIÇOS

Art. 2º Os modelos descritos nesta Portaria preveem a contratação de:

I - Serviços de computação em nuvem: disponibilização de grupo escalável e elástico de recursos físicos ou virtuais, compartilháveis, acessados via rede, com provisionamento via autoatendimento e administração sob

demanda; e

II - Serviços de operação e gerenciamento de serviços de computação em nuvem: gerenciamento, monitoramento, interoperabilidade, portabilidade, continuidade e suporte à gestão de custos de computação em nuvem.

Art.3º Termos e Definições

Atualização de versões: disponibilização, por parte do fabricante, de uma versão completa do software, ou parcial, mas com funcionalidades adicionais ou evoluções tecnológicas que compreendam uma nova versão estável do produto. Podem também, incluir correções de comportamentos disfuncionais que não tenham sido corrigidos por manutenções anteriores do software, por critério do fabricante.

Catálogo de Serviços de Computação em Nuvem Padronizados: relação de serviços de computação em nuvem que um órgão ou entidade fornece aos seus usuários, elaborada de forma padronizada, de acordo com as necessidades do órgão ou entidade e conforme as orientações estabelecidas pela SGD.

Catálogo de Soluções de TIC com condições padronizadas: relação de soluções de TIC ofertadas pelo mercado que possuem condições padrões definidas pelo Órgão Central do SISP, podendo incluir o nome da solução, descrição, níveis de serviço. Preço Máximo de Compra de Item de TIC – PMC –TIC, entre outros;

Carga de trabalho (workload): conjunto de recursos que compõem uma arquitetura técnica destinada a suportar um ou mais serviços de TIC. As cargas de trabalho podem requerer uma combinação de recursos computacionais e de serviços técnicos para agregar valor ao negócio por meio de serviços de TIC;

Co-location em nuvem: locação de infraestrutura de data center pertencente a terceiros para hospedar equipamentos computacionais de uma organização;

Computação em nuvem: modelo que possibilita o provisionamento e a utilização sobre demanda de recursos e serviços computacionais de qualquer lugar e a qualquer momento, de maneira conveniente, com acesso por meio de rede a recursos configuráveis (ex.: redes, segurança, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente provisionados, utilizados e liberados com o mínimo de esforço em gerenciamento ou interatividade com o provedor de serviços em nuvem;

Consultoria especializada em software: serviços especializados de configuração, customização, instalação, otimização e manutenção em software cujos padrões de desempenho e qualidade podem ser objetivamente definidos no Termo de Referência. Esses serviços não se confundem com os serviços técnicos especializados de natureza predominantemente intelectual, dispostos no inciso XVIII do art.6º da Lei nº 14.133, de 1º de abril de 2021.

Data center ou centro de dados: Consiste em uma estrutura, ou grupo de estruturas, dedicadas a acomodação centralizada, interconexão e operação dos equipamento de tecnologia da informação e rede de telecomunicações que fornece serviços de armazenamento de dados, processamento e transporte em conjunto a todas as instalações e infraestruturas de distribuição de energia e controle ambiental, juntamente com os níveis necessários de recuperação e segurança requeridos par a fornecer a disponibilidade de serviço desejada, conforme ABNT NBR ISO/IEC 22.237-1:2023.

Disponibilidade: condição de um serviço ou recurso estar acessível e apto para desempenhar plenamente suas funções, determinado momento ou

durante um período acordado;

Hosting: locação de recursos computacionais localizados em infraestrutura física tradicional de data center pertencente a terceiros, sem o compartilhamento de recursos entre clientes, pa a hospedagem de aplicações e soluções de TIC;

Incidente: qualquer acontecimento não planejado que cause redução na qualidade do serviço ou interrupção do serviço em parte ou como um todo, ou evento ainda não impactou o serviço do usuário;

Incidente de Segurança da Informação: qualquer evento de segurança da informação indesejável e inesperado, seja único ou em serie, que pode comprometer as operações de negócio e ameaçar a segurança da informação;

IN GSI/PR nº 5, de 2021: Instrução Normativa GSI/PR nº 5, de evento de segurança da informação indesejável e inesperado, seja único ou em série, que pode comprometer as operações de e ameaçar a segurança da informação;

IN SGD/ME nº 94, de 2022: Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, que 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;

Instancia de Computação: Componentes de computação em nuvem composto de máquina virtual e serviços agregados, como armazenamento, dispositivos de rede e demais serviços necessários para manter essa máquina virtual em operação.

Integrador de Serviços em Nuvem (Cloud Broker): realiza a integração dos serviços de computação em nuvem com agregação de valor entre o órgão ou a entidade e dois ou provedores de serviço de computação em nuvem. O Cloud Broker apoia o órgão ou entidade em descobri, planejar, migra, configurar, utilizar, gerenciar e evoluir os serviços de computação em nuvem de forma segura e eficiente, os serviços prestados pelo Cloud Broker são orientados de acordo com os padrões internacionais relevantes, com ISO e NIST e, no Brasil, a Associação Brasileira de Normas Técnicas – ABNT, para garantir que os serviços sejam oferecidos de forma segura, eficiente e confiável;

Licença de software: documento que fornece diretrizes legalmente vinculantes para o uso e a distribuição de determinado software, A Licença de software geralmente fornece aos usuários finais o direito a uma ou mais cópias do software sem incorrer em violação de direitos autorais. Também define as responsabilidades das partes envolvidas no contrato de licença. Além disso, pode impor restrições sobre como o software pode ser usado. Os termos e condições de licenciamento de software geralmente incluem o uso justo do software, as limitações de responsabilidade, garantias e isenções de responsabilidade e proteções se o software ou seu uso infringirem os direitos de propriedade intelectual de terceiros;

Licença de uso: instrumento que estabelece o direito de usar o software sem haver a transferência da sua propriedade entre o licenciante e o licenciado, e inclui, entre outros direitos, o serviço de correção de erros, sem ônus ao licenciado;

Licença por subscrição/assinatura: permite aos usuários acessarem o software por meio de serviços online, em vez de adquirir uma licença de uso único. As licenças por assinatura também podem fornecer aos usuários acesso a atualizações de software, suporte técnico e outros serviços;

Licença perpétua: é uma licença que concede ao usuário o direto de usar

o software por tempo indeterminado, vem como acesso a updates e suporte técnico por tempo determinado:

Manutenção de software (correção de erros): é o processo de fornecer suporte técnico, atualizações e melhorias para determinados softwares. É um processo contínuo que garante que o software se mantenha atualizado e funcione corretamente;

Marketplace: Loja virtual operada por um provedor de nuvem que oferece acesso a software e serviços que são desenvolvidos, se integram ou complementam as soluções disponibilizadas pelo provedor de nuvem;

Modelos de implantação de nuvem: representam como a computação em nuvem pode ser organizada, com base no controle e no compartilhamento de recursos físico ou virtuais. Os modelos de implantação em nuvem incluem; nuvem pública, nuvem privada, nuvem comunitária e nuvem hibrida;

Modelo de Serviços em nuvem IaaS (Infrastructure as a Service – Infraestrutura com Serviço): capacidade fornecida ao cliente para provisionar processamento, armazenamento, comunicação de rede e outros recursos de computação fundamentais, nos quais o cliente pode instalar e executar software em geral, incluindo sistemas operacionais e aplicativos. O cliente não gerencia nem controla a infraestrutura na nuvem subjacente, mas tem controle sobre os sistemas operacionais, armazenamento e aplicativos instalados e, possivelmente, um controle limitado de alguns componentes de rede;

Modelo de Serviços em nuvem PaaS (platform as a Service – Software como Serviço):capacidade fornecida ao cliente para provisionar na infraestrutura de nuvem aplicações adquiridas ou criadas para o cliente, desenvolvidas com linguagens de programação, bibliotecas, serviços e ferramentas suportados pelo provedor de serviços em nuvem. O cliente não gerencia nem controla a infraestrutura na nuvem subjacente, incluindo rede, servidores, sistema operacional ou armazenamento, mas tem controle sobre as aplicações instaladas e possivelmente sobre as configurações do ambiente de hospedagem de aplicações;

Modelo de Serviços em nuvem SaaS (Software as a Service- Software como Serviço): capacidade de fornecer uma solução de software completa que pode ser contratada de um provedor de serviços em nuvem. Toda a infraestrutura subjacente, middleware, software de aplicativo e dados de aplicativo ficam no data center do provedor de serviços. O provedor de serviço gerencia hardware e software e garante a disponibilidade e a segurança do aplicativo e de seus dados;

Multinuvem (multicloud): uma estratégia de utilização dos serviços de computação em nuvem por meio de dois ou mais provedores de nuvem pública;

Nuvem comunitária: modelo de implantação de nuvem em que os serviços de computação em nuvem são exclusivamente suportados e compartilhados por um grupo especifico de órgãos e entidades de serviços de computação em nuvem que tem requisitos compartilhados e um relacionamento entre si, e onde os recursos são controlados por pelo menos um membro deste grupo, conforme ISO/IEC 22123-1:2023 (Information technology – Cloud computing) O modelo de nuvem comunitária admite o uso de recursos computacionais de provedores de nuvem pública somente se assegurado o isolamento lógico e físico desses recursos, no ambiente do próprio órgão ou de empresas públicas, e não se configurando como uso de Nuvem Pública;

Nuvem de governo: infraestrutura de nuvem privada ou comunitária gerida exclusivamente por órgãos ou empresa públicas;

Nuvem hibrida: 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;

Nuvem privada ou interna – infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos usuários, e sua propriedade pode ser do próprio órgão ou empresas públicas com finalidade específica relacionada à tecnologia da informação, conforme ISO/IEC 22234-1:2023 (Information technology – Cloud e computing). O modelo de nuvem privada admite o uso de recursos computacionais de provedores de nuvem pública somente se assegurado o isolamento lógico e físico desses recursos, no ambiente do próprio órgão ou de empresa públicas, e não configurando com9o uso de Nuvem Pública;

Nuvem pública ou externa – infraestrutura de nuvem dedicada para o uso aberto de qualquer organização, e sua propriedade e seu gerenciamento podem ser de órgãos públicos, empresas privadas ou de ambos;

Orquestração: habilidade de coordenar e gerenciar recursos em diferentes provedores de nuvem pública de nuvem públicas;

Plataforma de gerenciamento de serviços em nuvem (Cloud Management Platform – CMP); sistema capaz de realizar o provisionamento e orquestração, requisição de serviço, inventário e classificação, monitoramento e análise, gerenciamento de custos e otimização de carga de trabalho, migração em nuvem, backup e recuperação de desastres, gerenciamento de segurança, conformidade e identidade e deployment e implantação dos recursos nos provedores de nuvem ofertados;

Provedor de serviços em nuvem: empresa que possui infraestrutura de Tecnologia da Informação - TI destinada ao fornecimento de infraestrutura, plataformas e aplicativos baseados em computação em nuvem;

Região: agrupamento d4e localizações geográficas especificas em que os recursos computacionais se encontram hospedados;

Serviço: meio de entregar valor aos usuários internos ou externos à organização ao facilitar o alcance de resultados almejados;

Serviços agregados: são serviços adicionais providos pelo fornecedor da solução que oferecem aos usuários acesso a recurso adicionais relacionados ao objeto principal. Esses serviços podem incluir suporte técnico, treinamento, atualizações, implementação e outros serviços.

Sistemas estruturantes: são sistemas de informação desenvolvidos e mantidos para operacionalizar e sustentar as atividades de pessoal, orçamento, estatística, administração financeira, contabilidade e auditoria, e serviços gerais, alem de outras atividades auxiliares comuns a todos os órgãos da administração que, a critério do Poder Executivo, necessitem de coordenação central;

Software livre: tipo de software de código aberto que pode ser usado, estudado, modificado e redistribuído gratuitamente. O software open source é publicado sob uma licença que permite aos usuários acessarem o código-fonte, mas impõe certas limitações quanto a sua modificação ou personalização;

Software open source (ou de código aberto): tipo de software de código aberto que pode ser usado, estudado, modificado e redistribuído gratuitamente. O software open source é publicado sob uma licença que permite aos usuários acessarem o código-fonte, mas impõe certas limitações quanto a sua modificação ou personalização;

Software pronto para uso: software disponibilizado (pago ou não) com um conjunto de funcionalidades pré-concebidas, também conhecido como Ready to Use Software Product (RUSP) ou mais comumente como “software de prateleira”;

Suporte técnico: serviço provido pelo fornecedor para auxiliar os usuários com problemas relacionados ao serviço contratado. O suporte técnico pode incluir resolução de problemas, treinamento, atualizações implementação e instalação;

Tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

Recursos reservados: são aqueles recursos tecnológicos que possuem planos pré-definidos de consumo por determinado período mediante a aplicação de desconto, seja por meio de antecipação de pagamento, seja mediante pagamento mensal durante o período pré definido.

Função como Serviço (FaaS): recursos fornecidos ao órgão e entidade para construir e gerenciar aplicativos de micros serviços ou equivalente, de forma escalável, conforme ISO 22123-2:2023

Banco de Dados como Serviço (DBaaS): ambiente no qual o recurso usado pelo órgão ou entidade é um banco de dados disponibilizado e operado pelo provedor de serviços em nuvem, e suas funções são acessadas por APIs ou meios equivalentes, conforme ISO 22123-2:2023.

OBJETIVOS E COMPETÊNCIAS

Art.3º As referências contidas neste documento, além de objetivarem a realização de um planejamento da contratação adequado com a melhor utilização dos recursos públicos, estão alinhadas à Estratégia de Governo Digital e à Estratégia Brasileira para a Transformação Digital (E-Digital), Ciclo 2022 - 2026, conforme objetivo específico do eixo G “Cidadania e transformação digital do governo”: “Adotar tecnologia de processos e serviços governamentais em nuvem como parte da estrutura tecnológica dos serviços e setores da administração pública federal”.

Art.4º A identificação do modelo de implantação de nuvem deve considerar as características de cada carga de trabalho em relação ao nível de sigilo das informações armazenadas ou manipuladas pelos serviços de TIC mantidos por essas cargas de trabalho.

Art. 5º Admite-se a utilização em ambiente de nuvem (pública, privada, híbrida, comunitária ou de governo) das cargas de trabalho que tratem informações sem restrição de acesso, considerada a legislação de dados pessoais e os aspectos de segurança da informação. (Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, Anexo – Item 5.42)

Art.6º Devem ser mantidas em ambiente de nuvem de governo, exceto se expressamente determinado pelo Comitê de Governança Digital ou instância equivalente do órgão ou entidade, cargas de trabalho que tratem informação com restrição de acesso prevista na legislação, a exemplo de: sigilo fiscal, bancário, comercial, empresarial, contábil, de segredo industrial, de direito autoral, de propriedade intelectual, industrial, policial, processual civil, processual penal e disciplinar administrativa. (Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, Anexo – Item 5.43)

Art.7º Não poderão ser tratadas em ambiente de nuvem pública

informações e cargas de trabalho que tratem informações classificadas em grau de sigilo (reservadas, secretas e ultrassecretas), nos termos do Decreto nº 7.724, de 16 de maio de 2012, e documentos preparatórios que possam originar informação classificada em grau de sigilo.

Art.8º Os dados tratados em ambiente de nuvem devem ser armazenados em data centers localizados em território brasileiro, admitindo-se o tratamento de dados em data centers fora do território brasileiro somente nos casos em que haja cópia de segurança atualizada armazenada em data centers localizados em território brasileiro, respeitando-se os demais limites estabelecidos neste modelo.

Art.9º Vinculação a resultados: toda execução dos serviços deve estar orientada ao alcance de resultados previamente estabelecidos, de forma planejada e controlada.

I - Continuidade do serviço público: adoção de infraestrutura de tecnologia capaz de assegurar a continuidade, disponibilidade, segurança e integridade dos serviços públicos;

II - Segurança da informação: observância à legislação, normativos e orientações de órgãos de controle relacionados à segurança da informação;

III - Parcelamento da contratação: realização do parcelamento da solução de TIC a ser contratada, em tantos itens quanto se comprovarem tecnicamente viáveis e economicamente vantajosos, avaliando sempre que possível a necessidade de licitações e contratações separadas para os itens que, devido a sua natureza, possam ser divididos.

IV - Padronização dos tipos de remuneração: aderência às modalidades de remuneração previstas neste documento;

V - Diretrizes para a seleção da modalidade de contratação: adoção de métricas padronizadas para cada modalidade de contratação;

VI - Utilização de catálogos padronizados: orientações para o uso de catálogos padronizados no planejamento das contratações;

VII - Definição de níveis mínimos de serviços: estabelecimento de padrões de níveis mínimos de serviço que devem servir de referência às contratações; e

VIII - Gerenciamento de riscos: adoção de processos e estudos abrangentes para a análise dos riscos, atentando para os possíveis impactos financeiros e não financeiros decorrentes desses riscos.

XIX - A adoção pelo órgão ou entidade deve pautar-se nos requisitos de negócio, e nos resultados pretendidos e na segurança da informação e privacidade, levando em consideração as especificidades de cada carga de trabalho.

XX - Deve-se submeter os dados a classificação previa da informação, nos termos do Decreto nº 7.724, de 16 de maio de 2012, de forma a assegurar que não haja restrições normativas ou legais para o tratamento da informação em ambiente de nuvem.

DIRETRIZES PARA DEFINIÇÃO DA ESTRATÉGIA DE USO DE SOFTWARE E DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM

Art.10º Os seguintes aspectos podem ser considerados na definição das diretrizes de uma estratégia para o uso de software e de serviços de computação

em nuvem:

a) Identificação das necessidades do negócio: é necessário identificar e avaliar as necessidades de negócio antes da contratação de software e de serviços de computação em nuvem. Deve-se determinar quais sistemas, aplicações, dados e serviços precisam ser movidos para a nuvem, como eles serão acessados e quais recursos computacionais e de armazenamento serão necessários;

b) Seleção dos modelos adequados: é necessário avaliar quais modelos de serviço (IaaS, PaaS, SaaS) e de implementação (nuvem pública, nuvem privada, nuvem híbrida etc.) melhor se adequam aos requisitos de negócio. Caso o órgão ou entidade não possua maturidade suficiente na contratação de serviços em nuvem ou possua impedimentos técnicos ou normativos para migração de alguns workloads, é recomendável sempre dar preferência à adoção de uma abordagem estratégica de nuvem híbrida. Caso o órgão possua maturidade e já tenha concluído que a demanda prevista pode ser atendida integralmente por meio de serviços em nuvem, uma abordagem completa, incluindo as demandas de migração do ambiente on-premises para a nuvem pode ser adotada;

c) Avaliação dos possíveis fornecedores: os estudos técnicos preliminares devem abranger o levantamento dos possíveis fornecedores aptos ao atendimento dos requisitos de negócio, de forma a garantir que exista uma quantidade mínima de fornecedores com experiência e que atendam aos requisitos necessários ao atendimento da demanda. Fatores como segurança, conformidade, disponibilidade e suporte técnico devem ser considerados nessa avaliação;

d) Definição de requisitos de segurança: deve-se determinar quais requisitos de segurança são importantes ou mandatórios para o negócio e deve ser avaliado, quando for o caso, como cada possível fabricante ou fornecedor atende a esses requisitos;

e) Estabelecimento de uma política de governança: deve-se assegurar que a política de governança do órgão ou entidade abranja a identificação e classificação de dados, controle de acesso, gerenciamento de configuração e, quando for o caso, monitoramento das atividades em nuvem, de modo a garantir que os serviços a serem contratados sejam executados em conformidade com os padrões adotados pelo órgão ou entidade;

f) Diretrizes de uso seguro de software e de serviços de computação em nuvem: o órgão ou entidade deve conhecer os normativos que versam sobre segurança da informação e sobre o tratamento de informações em nuvem, bem como identificar, sob essa perspectiva, quais os sistemas ou workloads que podem ser migrados, assim como as medidas de gerenciamento de risco a serem adotadas para resguardar as informações sigilosas que eventualmente serão tratadas em ambiente de nuvem;

g) Avaliação quanto às condições mínimas de infraestrutura de TIC do órgão ou entidade para utilizar serviços de computação em nuvem, a exemplo de conexão estável com a Internet e com banda suficiente;

h) Definição de diretrizes de governança para o uso da nuvem, com papéis e responsabilidades dos atores organizacionais (da TI, das áreas de negócio e da nuvem);

i) Estabelecimento dos princípios norteadores da estratégia (ex.: cloud first, liftand-shift como último recurso, uso de broker multicloud etc.);

j) Alinhamento com outros planos estratégicos, a exemplo do Plano Estratégico Institucional (PEI), Plano Estratégico de TI (PETI), Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), Plano de Contratações Anual (PCA), Planos de Segurança da Informação etc.;

k) Estabelecimento de linhas de base e metas de benefícios/resultados esperados, a exemplo de mapeamento “AS IS” e “TO BE”, objetivando maior agilidade, redução de custos, resiliência, mais segurança etc.);

l) Considerações sobre capacitação da equipe do órgão ou entidade que gerenciará, operará ou utilizará os recursos de software e de computação de serviços em nuvem, identificando as capacidades e habilidades necessárias;

m) Considerações sobre portabilidade e interoperabilidade entre sistemas, dados e serviços, bem como a viabilidade de adoção de medidas para mitigar a dependência tecnológica ou aprisionamento ao provedor;

n) Requisitos regulatórios e de conformidade;

- Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023

Estabelece modelo de contratação de software e de serviços de computação em nuvem, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

- Instrução Normativa nº 5, DE 30 DE AGOSTO DE 2021 - Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.

o) Indicação da Estratégia de Saída, considerando a análise de dependências e aspectos de portabilidade, (backup, redundância, contratos de apoio, retorno para a infraestrutura local etc.); e

p) Análise de riscos, considerando as diretrizes de gerenciamento de riscos constantes deste modelo.

DO ESCOPO

Art. 11º O Documento de Estratégia de uso e de Serviços de Computação em Nuvem abrange as diretrizes de contratação de:

I - Software como Serviço (SaaS);

II - Infraestrutura como Serviço (IaaS);

III - Plataforma como Serviço (PaaS);

IV - Suporte técnico para software e serviços de computação em nuvem;

V - Serviço de operação e gerenciamento de recursos em nuvem;

VI - Serviço de migração de recursos para ambiente de nuvem;

VII - Integração de serviços de computação em nuvem; e

VIII - Consultoria especializada em software e/ou serviços de computação em nuvem.

Art.12º A contratação dos serviços de que tratam os itens acima: I a VIII, podem ser realizadas com empresas cujo ramo de atividade seja compatível com o

objeto, mediante análise das habilitações jurídica, fiscal e social, nos termos da legislação pertinente, a exemplo da Classificação Nacional de Atividades Econômicas (CNAE), bem como das verificações do contrato social da empresa e do cadastro junto à fazenda Pública.

Art.13º Os documentos de planejamento da contratação, assim como as tabelas de identificação dos itens do objeto da contratação constante do Termo de Referência, as propostas comerciais das empresas licitantes e da empresa vencedora do certame e o Termo Contratual devem conter, sempre que possível, informações necessárias à identificação do software, serviço ou produto contratado, abrangendo, no mínimo, os seguintes elementos:

a) nome específico, nome oficial e/ou descrição;

b) categoria ou linha do software, serviço ou produto;

c) código de identificação unívoca do fabricante (part number, SKU etc.);

d) modelo de licenciamento;

e) métrica ou unidade;

f) tipo de software, serviço ou produto; e

g) quantidade estimada.

Art.14º A indicação de fabricante de software, marca ou provedor é justificável somente:

a) em decorrência da necessidade de padronização do objeto;

b) em decorrência da necessidade de manter a compatibilidade com plataformas e padrões já adotados pela Administração; e/ou

c) quando determinado provedor for o único capaz de atender às necessidades do contratante;

Art. 15º O MAPA deverá exigir das empresas licitantes declaração que ateste a não ocorrência do registro de oportunidade, de modo a garantir o princípio da competitividade, conforme o disposto no art. 5º da Lei nº 14.133, de 2021.

Art.16º As contratações de Software e Serviços de Computação em Nuvem deverão estar explicitamente previstas no Plano de Contratações Anual (PCA) do órgão e entidade para o exercício em que se dará a contratação.

Art.17º Os valores previstos para as iniciativas deverão possuir mesma ordem de grandeza dos valores estimados previstos no Termo de Referência.

Art. 18º Havendo necessidade de indicação de marca, fabricante, tipo de software ou provedor de nuvem, deve-se deixar explícitas tais informações na descrição da iniciativa a constar do Plano de Contratações Anual (PCA).

Art.19º É dever da equipe de planejamento da contratação zelar pelo alinhamento do planejamento da contratação ao Plano Anual de Contratação, realizando se necessário as devidas atualizações nas iniciativas previstas no Plano de Contratações Anual.

DIRETRIZES PARA A SELEÇÃO DA MODALIDADE DE REMUNERAÇÃO

Art.20º Na etapa de planejamento da contração devem ser avaliadas diferentes formas de provimento e remuneração do objeto a ser contratado.

Art.21º Há diferentes modalidades de remuneração de software e serviços de computação em nuvem, cada uma adequada ao atendimento de um cenário específico.

Art.22º Para identificar a modalidade de remuneração que melhor se adequa à necessidade do órgão ou entidade é preciso levar em consideração:

a) os requisitos de negócio;

b) as necessidades tecnológicas;

c) as tecnologias já adotadas;

d) a cultura organizacional;

e) os riscos de indisponibilidade de serviço;

f) os riscos de dependência tecnológica;

g) a disponibilidade orçamentária;

h) os requisitos ambientais;

i) os resultados pretendidos; e

j) outros fatores que possam afetar a efetividade na utilização dos recursos computacionais.

Art.23º São premissas que devem ser observadas na construção do Termo de Referência, independentemente da modalidade de remuneração adotada:

a) fixação dos critérios de aceitação dos serviços prestados;

b) definição dos níveis mínimos de serviço e de qualidade;

c) pagamento vinculado ao alcance de resultados;

d) escolha do modelo adequado de precificação ou pagamento pelo serviço e os devidos controles, com vistas a mitigar riscos;

e) clareza quanto à definição do escopo dos serviços e seus entregáveis;

f) previsão de faixas de valores de ajustes nas metas dos indicadores de níveis de serviço;

g) adoção dos mecanismos adequados de penalidades, objetivando punir falhas de disponibilidade dos serviços contratados;

h) utilização de Termo de Confidencialidade ou Termo de Compromisso de Manutenção de Sigilo;

i) observância da legislação brasileira quanto à segurança da informação, proteção de dados pessoais e privacidade, em especial à Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709, de 14 de agosto de 2018);

j) respeito ao direito de propriedade intelectual e direitos autorais da contratante sobre o conteúdo hospedado, tratado, criado e alterado no ambiente de nuvem objeto do contrato; e

k) observância às disposições contidas na Lei de Acesso à Informação - LAI (Lei nº 12.527, de 18 de novembro de 2011).

MECANISMOS DE GESTÃO

Art.24º A execução dos serviços está condicionada à emissão de ordem de serviço, contendo no mínimo:

a) as informações contidas no Art. 32 da Instrução Normativa SGD/ME nº 94, de 2022;

b) o objetivo da OS;

c) a descrição do que deve ser executado;

d) os produtos/resultados a serem entregues;

e) o prazo de atendimento e os requisitos não funcionais, a exemplo de critérios mínimos de desempenho operacional da solução, critérios de segurança da informação, critérios de identidade visual e usabilidade, entre outros identificados pela equipe da contratante;

f) a justificativa de necessidade da OS, seja um elemento pontual (e.g. alocação de uma máquina virtual) ou uma infraestrutura para um projeto;

g) a justificativa dos parâmetros utilizados na OS (tipos de recursos, modalidades de fornecimento, duração da alocação dos recursos, capacidade dos recursos);

h) a análise de custo-benefício da OS com o enfoque na justificativa da economicidade e efetividade da escolha.

Art.25º Será apurada mensalmente a quantidade de USNs efetivamente consumidas para fins de pagamento, respeitando-se o limite máximo estimado na ordem de serviço.

Art.26º O Termo de Referência deve prever que durante a execução dos serviços o cloud broker implemente as condições necessárias para gestão do consumo das USNs, de modo a observar os limites máximos previstos nas ordens de serviço.

Art.27º Admite-se a contratação de empresa especializada na realização de auditorias, com vistas a apoiar a fiscalização técnica do contrato.

Art.28º A verificação da adequação da prestação dos serviços deverá ser realizada com base em Níveis Mínimos de Serviço (NMS), capazes de aferir objetivamente os resultados pretendidos com a utilização dos serviços contratados.

Art.29º A equipe de fiscalização deverá implementar mecanismos próprios de controle dos volumes consumidos, evitando-se a aferição baseada exclusivamente em relatório ou outro artefato produzido pela própria contratada.

Art.30º O órgão ou entidade deve avaliar a utilização de mecanismos e instrumentos adicionais para assegurar a adequada verificação dos volumes consumidos, ou ainda a exigência, no instrumento convocatório, do fornecimento de evidências rastreáveis que comprovem a execução dos serviços.

Art.31º Deve-se prever no Termo de Referência que a emissão de Nota Fiscal por parte da contratada deve estar condicionada à autorização prévia por parte do gestor do contrato após a emissão do Termo de Recebimento Definitivo, nos termos da alínea “n” do Inciso I do art. 33 da IN SGD/ME nº 94, de 2022.

DIMENSIONAMENTO

Art.32º O dimensionamento do volume dos serviços consiste na identificação do quantitativo de serviços de computação em nuvem suficientes para

atender à demanda a ser suprida com a contratação pretendida.

São elementos que auxiliarão no dimensionamento:

a) a definição de uma estratégia para utilização de serviços em nuvem (totalmente cloud ou híbrida);

b) o mapeamento dos tipos de informações passíveis de serem transferidas para a nuvem;

c) a existência de equipe técnica com conhecimento em ambiente de nuvem; e

d) o histórico de consumo de recursos em ambiente de nuvem pública, privada, híbrida, comunitária ou de governo.

e) projetos em andamento ou com perspectiva de entrega durante a vigência do contrato; e

f) iniciativas previstas no PDTIC do órgão ou entidade.

GERENCIAMENTO DOS NÍVEIS DE SERVIÇO

ASPECTOS GERAIS SOBRE QUALIDADE DOS SERVIÇOS

Art.33º A verificação da qualidade constitui-se em procedimento indispensável para a fiscalização e a gestão de contratos de serviços da Administração Pública. Proporciona a devida verificação na medida em que o que está sendo entregue ao longo do contrato efetivamente corresponde ao resultado esperado (ou planejado). Nesse sentido, indicadores de níveis de serviços devem ser definidos para todo e qualquer contratação de serviços de computação em nuvem, observando-se o conjunto mínimo de indicadores capaz de assegurar a efetiva prestação de serviço com a qualidade esperada.

Art.34º O gerenciamento dos níveis mínimos de serviço consiste no monitoramento e controle da qualidade na execução dos serviços em função dos resultados pretendidos, por meio de um conjunto de procedimentos preestabelecidos pelo órgão ou entidade.

Art.35º Com vistas a assegurar a efetiva prestação dos serviços com a qualidade esperada, os indicadores de níveis de serviço devem adotar métricas associadas a resultado e abranger, no mínimo, as dimensões de qualidade, desempenho do produto e prazo de entrega.

Art.36º Os indicadores são instrumentos práticos de aferição do cumprimento do alcance dos níveis mínimos de serviço, evidenciando de maneira objetiva e mensurável o desempenho e as tendências de um serviço demandado. Devem ser objetivamente mensuráveis e compreensíveis, de preferência facilmente coletáveis, relevantes e adequados à natureza e características do serviço.

Art.37º Devem-se adotar cláusulas contratuais relacionadas a níveis de serviço que sejam alinhadas aos objetivos de negócio, observando as práticas adotadas pelo mercado, evitando estipular prazos para resolução de problemas que sejam inferiores àqueles definidos no modelo de comercialização do fabricante, salvo situações devidamente justificadas nos autos.

Art.38º Recomenda-se que o órgão realize a aferição dos indicadores de níveis de serviço por meio de ferramenta automatizada, que não esteja sob gestão da contratada, de modo a otimizar a rotina de fiscalização e a gestão do contrato.

Art.39º É vedada a aferição de indicadores de níveis de serviço baseada exclusivamente em dados fornecidos pela própria contratada.

Art.40º A definição dos indicadores de níveis de serviço deve considerar as necessidades de negócio, os riscos associados ao processo e a criticidade dos serviços.

DO GERENCIAMENTO DE CUSTOS DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM

Art.41º Os mecanismos de gerenciamento de custos de serviços de computação em nuvem são elementos fundamentais para assegurar a governança e a supervisão na gestão contratual em relação aos limites autorizados de execução dos recursos a serem previstos nas ordens de serviço.

O órgão ou entidade deve prever no Termo de Referência a estrita observância, para fins de pagamento, aos limites de recursos e serviços estabelecidos em cada ordem de serviço formalmente demandados pelo gestor do contrato.

O órgão ou entidade deve assegurar que cada carga de trabalho:

a) seja precedida de planejamento operacional compatível com os objetivos previstos na ordem de serviço;

b) possua cotas que limitem o consumo de determinado recurso de acordo com as necessidades da CONTRATANTE;

c) permita o gerenciamento de capacidade com antecedência com vistas a evitar a limitação inesperada do consumo de recursos conforme limites previamente estabelecidos na ordem de serviço; e

d) preveja mecanismos de controle de custos por meio de alertas relacionados a situações em que os gastos atingirem determinados limites previamente estabelecidos na ordem de serviço.

Art.42º O gerenciamento de custos deve ser responsabilidade da contratada, conforme diretrizes previamente estabelecidas nas ordens de serviço.

Art.43º O órgão ou entidade poderá avaliar durante o planejamento da contratação a necessidade da contratação de serviços especializados de auditoria técnica de serviços de computação em nuvem, com vista a assegurar a otimização dos recursos de computação em nuvem utilizados.

DA VIGÊNCIA DOS CONTRATOS

Art.44º O contrato a ser firmado poderá ter vigência de até 5 (cinco) anos, nas hipóteses de serviços e fornecimentos contínuos, podendo ser prorrogado, até o limite de 10 (dez) anos, conforme as regras e diretrizes estabelecidas nos arts. 105 a 107 da Lei nº 14.133, de 2021.

Art.45º A definição da vigência do contrato deve considerar aspectos técnicos e econômicos do objeto, devidamente registrados nos Estudos Técnicos Preliminares pela equipe de planejamento da contratação. As justificativas para o prazo de vigência adotado devem constar no Termo de Referência.

DA PREVISÃO DE ANTECIPAÇÃO DE PAGAMENTOS

Art.46º Excepcionalmente, admite-se o pagamento antecipado para remuneração por créditos se constatado que a solução propiciará sensível economia de recursos ou representará condição indispensável para a prestação do serviço, hipóteses que deverão ser previamente justificadas no estudo técnico preliminar por

meio de memória de cálculo específica e serem expressamente previstas no Termo de Referência.

Art.47º Entende-se por sensível economia, a redução no preço do recurso igual ou superior a 12% (doze por cento) ao ano em relação às demais modalidades comparadas, ou outro percentual definido pelo órgão, desde que demonstrada de forma clara a vantajosidade econômica. Por exemplo, a antecipação de pagamento de um recurso com vigência de 12 meses deve demandar a aplicação de um desconto mínimo de 12%, já a antecipação de um recurso com vigência de 36 meses deve demandar a aplicação de um desconto mínimo de 36%.

Art.48º O órgão ou entidade deverá avaliar, durante o planejamento da contratação, a necessidade de exigência da prestação de garantia adicional como condição para o pagamento antecipado, considerando os respectivos riscos identificados no mapa de gerenciamento de riscos da contratação.

Art.49º Deverão constar no Termo de Referência cláusulas que prevejam a devolução do valor antecipado caso o objeto não seja executado no prazo contratual.

Do Gerenciamento de Riscos

Art.50º O órgão ou entidade deve realizar um estudo abrangente para a análise dos riscos sobre os itens a serem licitados e sobre o contrato, contemplando, entre outras medidas, a identificação, a análise, a avaliação, o plano de tratamento e o monitoramento dos riscos identificados.

Art.51º Devem ser incluídos no escopo da análise de riscos as etapas de execução contratual, de negociação das prorrogações do contrato e de licitação para a substituição do fornecedor, aplicando, em cada etapa, as ações cabíveis previstas no referido plano de tratamento de riscos.

Principais riscos a serem tratados

Art.52º Os riscos durante o processo de contratação de serviços de computação em nuvem devem ser tratados de acordo com a política de gestão de riscos de cada órgão ou entidade, embasando as decisões de tratamento do risco de acordo com a realidade da organização e levando-se em consideração o apetite de risco da alta administração, o limite de exposição a riscos, o impacto na política pública que pode ser afetada, os instrumentos de governança em vigor, as questões legais em curso, a dependência tecnológica do fornecedor, a dificuldade de substituição do fornecedor, a descontinuidade no fornecimento por eventos imprevistos ligados ao fornecedor, dentre outros, sempre atentando para os possíveis impactos decorrentes desses riscos.

Art.53º Independentemente da modalidade adotada, o órgão deve realizar o mapeamento de riscos da contratação, detalhando a identificação, a classificação e o tratamento dos riscos associados às contratações públicas. De forma complementar, deve-se considerar, no mínimo, os seguintes riscos, específicos para contratação de serviços de computação em nuvem:

a) Volumetria da contratação incompatível com a realidade do órgão ou entidade.

Descrição: Utilização de critérios não condizentes com a realidade do órgão ou entidade para elaboração da análise de custo total de propriedade (TCO), levando a um subdimensionamento ou superdimensionamento do quantitativo do objeto licitado, com consequente necessidade de aditivos ou novas contratações e com possibilidade de insuficiência de saldo contratual ou danos ao erário;

b) Não cumprimento dos níveis de serviços mínimos estabelecidos no Termo de Referência.
Descrição: Entrega de uma solução com características de qualidade inferiores às especificadas, levando ao não atendimento das necessidades de negócio, com consequente prejuízo às atividades finalísticas do órgão e ao alcance dos resultados pretendidos com a contratação;

c) Falhas na segurança da informação e privacidade da solução.
Descrição: Não observância dos padrões mínimos de segurança e privacidade da informação, levando a problemas de disponibilidade, integridade, confidencialidade e autenticidade, com consequente prejuízo às atividades finalísticas do órgão ou entidade e ao alcance dos resultados pretendidos com a contratação;

d) Contratação de modelo licenciamento de software, de implantação ou de prestação de serviços em nuvem que não atenda a necessidade do órgão ou entidade.
Descrição: Não observância dos requisitos de contratação, levando à escolha de um modelo incompatível com a necessidade, com consequente prejuízo às atividades finalísticas do órgão ou entidade, ao alcance dos resultados pretendidos com a contratação e dano ao erário;

e) Atraso na entrega dos serviços contratados.
Descrição: Demora pela contratada em entregar o produto ou serviço contratado, levando ao não atendimento das necessidades de negócio, com consequente prejuízo às atividades finalísticas do órgão ou entidade e ao alcance dos resultados pretendidos com a contratação;

f) Especificação incorreta dos modelos de licenciamento de software, de implantação ou de prestação de serviços em nuvem.
Descrição: Especificação dos modelos fora dos padrões técnicos apropriados, levando a um subdimensionamento ou superdimensionamento da capacidade dos serviços com consequente prejuízo às atividades finalísticas do órgão ou entidade, ao alcance dos resultados pretendidos com a contratação e dano ao erário;

g) Incompatibilidade do modelo de licenciamento de software, de implantação ou de prestação de serviços em nuvem escolhido com outras soluções de TIC existentes no órgão ou entidade.
Descrição: Contratação de um modelo de serviço sem levar em consideração possíveis impactos na infraestrutura de TIC atual do órgão, levando ao não atendimento das necessidades de negócio, com consequente prejuízo às atividades finalísticas do órgão ou entidade e ao alcance dos resultados pretendidos com a contratação; e

h) Encerramento de chamados de forma prematura.
Descrição: Falha no controle que permita que a contratada encerre chamados sem a efetiva finalização e comprovação de cumprimento dos níveis de serviço, levando a prejuízo às atividades finalísticas do órgão ou entidade, com consequente prejuízo ao alcance dos resultados pretendidos com a contratação e dano ao erário.

i) Não alinhamento da contratação às reais necessidades finalísticas do órgão ou entidade.
Descrição: Risco de não alinhamento dos produtos e serviços de software e nuvem a serem contratados às reais necessidades finalísticas do órgão ou entidade, levando a prejuízo às atividades finalísticas do órgão ou entidade, com consequente prejuízo ao alcance dos resultados pretendidos com a contratação

e dano ao erário.

j) Baixa Resiliência da infraestrutura de TIC.
Descrição: Adoção de infraestruturas de TIC vulneráveis ou com fragilidades estruturais ou de segurança que não observam as classes de disponibilidade e demais requisitos constantes da ABNT NBR ISO/IEC 22.237-1:2023, levando a indisponibilidades dos serviços mantidos pela infraestrutura, com consequente prejuízo aos serviços públicos prestados, à segurança e à integridade dos dados mantidos.

k) Dependência aos fornecedores de nuvem (riscos na saída). Descrição: Aumento da dependência dos recursos e serviços específicos de determinado provedor de serviços de computação em nuvem, levando à necessidade de prorrogações ou novas contratações específicas de determinado provedor com consequente prejuízo à economicidade das contratações ou à indisponibilidade dos serviços em eventual migração em um cenário de alta dependência tecnológica.

l) Ocorrência de sanções comerciais nos países em que se localizam as infraestruturas de TIC que mantêm os serviços de computação em nuvem ou subscrição de software.
Descrição: Eventual sanção comercial entre países em que se encontram as infraestruturas de TIC que sustentam os serviços de computação em nuvem ou as subscrições do software contratado levando à indisponibilidade dos dados mantidos ou dos serviços contratados, independentemente da aplicação das sanções contratuais previstas sobre a contratada, com consequente prejuízo à prestação dos serviços públicos.

m) Não observância de restrições legais quanto às informações sujeitas a sigilo.

Descrição: Manter informações sujeitas a diferentes tipos de sigilo com previsão legal em ambientes de TIC não autorizados legalmente, levanto à ofensa ao princípio da legalidade com consequente exposição de informações sigilosas a situações de vulnerabilidade a acesso não autorizado ou à indisponibilidade de acesso.

n) Perda do controle ou da governança sobre as informações mantidas em ambiente de nuvem.

Descrição: A dependência dos serviços de computação em nuvem ou de utilização de software sob o regime de subscrição pode resultar na perda do controle do órgão sobre as informações armazenadas no provedor de nuvem ou mantidas em software sob regime de subscrição, levando a um aumento da fragilidade na prestação dos serviços com consequente prejuízo à disponibilidade, integridade, segurança das informações mantidas em ambiente de nuvem ou em software sob subscrição.

o) Não padronização dos serviços em cenário de multicloud.

Descrição: A diferença entre produtos entre os provedores de serviços em nuvem pode dificultar a padronização dos serviços utilizados pela área de TIC do órgão ou entidade, levando a oscilações na qualidade dos serviços prestados e dificuldade de migração dos serviços entre provedores, com consequente queda na qualidade dos serviços públicos mantidos na infraestrutura de TIC.

p) Migração de aplicação para ambiente ou para provedor que não ofereça os recursos mais adequados à otimização do uso de recursos com a aplicação.

Descrição: Migrar aplicações para provedores que não possuam os recursos de otimização mais adequados à aplicação, levando a aumento do consumo ou redução do desempenho com consequente prejuízo ao erário e prejuízo à qualidade do serviço público.

q) Aumento de custos de cargas de trabalho não distribuídas entre provedores de forma eficiente e otimizada.

Descrição: Distribuição de cargas de trabalho não planejadas ou não otimizadas em termos de custos entre diferentes provedores levando a um consumo elevado de recursos com consequente gasto ineficiente de recursos públicos.

r) Redução da competitividade em longo prazo.

Descrição: Mudanças no mercado de provedores de computação em nuvem podem reduzir a competitividade, levando à dificuldade na continuidade da contração de determinados provedores com consequente necessidade de alteração constante, implicando em maior chance de indisponibilidade.

s) Redução ou ausência de recursos humanos especializados.

Descrição: Quantidade reduzidas de técnicos especializados em determinado provedor levando a aumento dos custos de gerenciamento e operação dos recursos em nuvem com consequente prejuízo ao erário.

t) Redução da quantidade de cloud brokers especializados em determinado provedor.

Descrição: A redução do marketshare de determinado provedor ou de sua penetração no mercado brasileiro pode implicar na redução da cadeia de revendas e na quantidade de cloud brokers levando à redução da competição e, por conseguinte, aumento dos custos e da dependência a grupo restrito de cloud brokers.

u) Descontinuidade dos serviços ou mudanças dos recursos tecnológicos a longo prazo. Descrição: Os recursos tecnológico remotos podem sofrer mudanças significativas ou até mesmo descontinuidade dos produtos levando a aumento de custos para migração ou adaptação às mudanças com consequente possibilidade de interrupção dos serviços e aumento não previstos de gastos.

DA TRANSIÇÃO E ENCERRAMENTO CONTRATUAL

Art.54º O órgão ou entidade deve estabelecer procedimento relacionado à transição e encerramento contratual, incluindo, no mínimo, a obrigação do integrador/provedor em efetuar a devolução dos dados, informações e sistemas à contratante, a eliminação de dados, a retenção de dados conforme legislação e a garantia ao direito ao esquecimento para os dados pessoais.

DA GOVERNANÇA DA CONTRATAÇÃO DOS SERVIÇOS DE COMPUTAÇÃO EM NUVEM

Art.55º Na contratação de serviços de computação em nuvem via integrador (cloud broker), deve-se assegurar que todo serviço de computação em nuvem seja fornecido com agregação de valor por parte do cloud broker, ou seja, a contratação via cloud broker pressupõe dois modelos de compartilhamento de responsabilidades:

a) totalmente gerenciado pelo cloud broker; e

b) parcialmente gerenciado pelo cloud broker.

Art.56º Os modelos de compartilhamento de responsabilidades não são excludentes entre si, pois a critério do órgão ou entidade, admite-se que determinadas cargas de trabalho operem em um modelo totalmente gerenciado, enquanto outras cargas de trabalho operem em um modelo parcialmente gerenciado.

Art.57º Nas contratações de serviços multinuvem o cloud broker deverá atuar como integrador dos serviços de computação em nuvem entre o órgão ou a entidade, conforme estabelecido no art. 21 da IN GSI/PR nº 5, de 2021.

Art.58º Para se definir os limites dos modelos de compartilhamento de responsabilidades, deve-se estabelecer no Termo de Referência uma matriz de responsabilidades capaz de identificar, controlar e assegurar as responsabilidades na relação entre o cloud broker e o órgão ou entidade contratante, identificando-se o ator e o respectivo papel ou função.

A matriz de responsabilidades, deve incluir um registro formal sobre o uso de serviços de computação em nuvem no órgão ou entidade, contendo, a exemplo, as seguintes informações:

a) a função na prestação dos serviços;

b) o responsável pelos serviços (órgão/entidade ou cloud broker); e

c) nível de responsabilidade.

Art.59º Deve-se prever no Termo de referência com condição necessária para assinatura do contrato, instrumento contratual acessório que assegure o regime de compartilhamento de responsabilidades entre broker e respectivo Provedor de Nuvem, a exemplo do modelo de Termo de Compartilhamento de responsabilidades de Serviços de Computação em nuvem.

DIRETRIZES PARA A GESTÃO DE CONTRATOS DE SOFTWARE E DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM

Art.60º Toda emissão de ordem de serviço deverá ser precedida de levantamento da demanda real dos volumes de bens ou serviços a constar da ordem de serviços, considerando as atuais necessidades de negócio e eventuais riscos inerentes à prestação dos serviços finalísticos do órgão ou entidade e observando os limites previstos no contrato.

Art.61º Os fiscais técnicos devem manter nos autos dos processos administrativos de fiscalização do contrato todas as evidências de modo a conter as informações suficientes que permitam a verificação posterior do que foi pago e do que foi utilizado.

Art.62º Os volumes de bens e serviços a constar de toda ordem de serviço devem ser precedidos de levantamentos, estimativas e cálculos que justifiquem a real demanda associada às cargas de trabalho a serem implementadas ou mantidas, considerando, sempre que possível, o padrão de atividade do negócio, eventuais picos de consumo ou sazonalidades relacionadas aos requisitos de negócio e riscos inerentes às atividades finalísticas associadas aos objetivos da ordem de serviço.

Art.63º Nas contratações de serviços de computação em nuvem, a equipe de fiscalização e o gestor do contrato devem assegurar que os períodos de reserva de recursos não excedam o período de vigência contratual.

Glosas e sanções

Art .64º As glosas e sanções devem ser proporcionais à relevância ou significância de cada indicador de Nível Mínimo de Serviço (NMS), de modo a assegurar o alcance da qualidade, segurança e tempestividade na contratação de software ou de serviços de computação em nuvem.

Art.65º Para a contratação de serviços de software, incluindo subscrição, e serviços de computação em nuvem, sempre que possível, a equipe de planejamento da contratação deve implementar um mecanismo gradual de aplicação de glosas proporcionais ao grau ou ao impacto do inadimplemento das condições previstas no Termo de Referência. Para a contratação ou aquisição de licenciamento de software quando for previsto pagamento à vista, a equipe de planejamento da contratação deve implementar um mecanismo gradual de aplicação de sanções, uma vez que somente cabe aplicação de glosas quando houver pagamento pendente.

Art.66º Há duas abordagens na definição dos mecanismos de glosas que podem ser adotadas:

a) Abordagem fixa, baseada na definição de faixas fixas de ajuste no pagamento, de forma independente entre os Níveis Mínimos de Serviço; e

b) Abordagem ponderada, baseada na definição de um valor máximo de desconto possível, em conjunto com a adoção de um mecanismo de ponderação de acordo com a relevância de cada Nível Mínimo de Serviço.

Art.67º Na abordagem fixa, a definição do nível de desconto para cada faixa de ajuste por nível de serviço deve ser dimensionada em função do risco associado ao descumprimento do NMS e o respectivo impacto para o alcance dos resultados, assegurando-se a proporcionalidade entre o ajuste e o impacto da ação ou comportamento que se deseja coibir.

Art.68º Na abordagem ponderada, devem-se atribuir pesos percentuais para cada NMS que, somados, não ultrapassem um valor situado no intervalo de 250 a 300%, além de se fixar um limite máximo de desconto. Assim, durante a aplicação de uma penalidade, se o limite aplicável de glosa sobre as faturas for de 30%, tem-se a seguinte fórmula: peso do NMS descumprido x 30%. Caso o somatório dos pesos dos NMS descumpridos ultrapasse 100%, aplica-se o desconto máximo previsto, a exemplo de 30%.

Art.69º As condições passíveis de aplicação de sanções devem ser apresentadas de forma detalhada em quadro específico, a exemplo do quadro constante no template de Termo de Referência para serviços de TIC, publicado pelo Órgão Central do SISP.

Da aprovação e acompanhamento pela alta administração

Art.70º As diretrizes e decisões relacionadas à contratação de software e de serviços de computação em nuvem que sejam de alta relevância para a continuidade dos serviços finalísticos da organização pública deve ser aprovadas previamente pelo Comitê de Governança Digital do órgão ou estrutura colegiada equivalente.

Art.71º A execução dos contratos de software e de serviços de computação em nuvem que sejam de alta relevância ou de alta materialidade para a continuidade dos serviços finalísticos da organização pública deve ser supervisionada pelo Comitê de Governança Digital do órgão ou estrutura colegiada

equivalente, que poderá determinar ajustes ou mudanças nos rumos estratégicos desses contratos.

Art.72º Entende-se por serviços de alta relevância, aqueles que possuem potencial de paralização ou de causar prejuízo à continuidade dos serviços finalísticos da organização pública.

Art.73º Entende-se por serviços de alta materialidade, aqueles que se enquadram nos limites estabelecidos pela Instrução Normativa SGD/MGI n° 6, de 2023.

DIRETRIZES SOBRE O USO SEGURO DE COMPUTAÇÃO EM NUVEM

Art. 74 As diretrizes sobre o uso seguro de computação em nuvem foram elaboradas com base nos requisitos mínimos apresentados a seguir:

I - Política de segurança da informação do Ministério da Agricultura e Pecuária e aos órgãos e instituições integrantes do MAPA – Portaria MAPA nº 136, de 25 de maio de 2021;

II - Deverá ser aprovado pela alta administração e divulgado a todas as partes interessadas;

III – As metas a serem alcançadas e os objetivos que regem o serviço de computação em nuvem - Plano Diretor de Tecnologia da Informação e Comunicação vigente e; Service Level Agreement – SLAs, definidos em contrato.

IV - Definir a equipe de fiscalização de serviços com funções e as responsabilidades dos agentes designados para o gerenciamento dos serviços de computação em nuvem; e

V - Estabelecer a periodicidade para sua revisão, a qual não deve exceder dois anos.

Parágrafo único. A revisão do ato normativo previsto no caput deverá ocorrer a qualquer tempo, quando houver mudanças significativas nos requisitos de segurança da informação que influenciem o uso seguro de computação em nuvem, de forma a assegurar sua continuidade, sustentabilidade, adequação e efetividade.

DAS RESPONSABILIDADES

Art. 75 Ao Coordenador Geral responsável pela Gestão de Segurança da Informação do MAPA compete:

I – Coordenar o planejamento, implementação e execução ou designar os responsáveis pela elaboração e revisões do ato normativo sobre uso seguro de computação em nuvem;

II - Supervisionar a aplicação do ato normativo sobre uso seguro de computação em nuvem;

III - assegurar a contínua efetividade da comunicação com o provedor de serviço de nuvem, que fornece tais serviços ao órgão ou à entidade, de forma a assegurar que os controles e os níveis de serviço acordados sejam cumpridos;

IV - Supervisionar a aplicação das medidas de correção pelo provedor de serviço de nuvem, em casos de eventuais desvios;

V - Comunicar incidentes cibernéticos informados pelo provedor de

serviço de nuvem aos órgãos competentes para os seus tratamentos, conforme a relevância dos incidentes previamente estabelecida; e

VI - Encaminhar para aprovação da alta administração as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de computação em nuvem.

VII – O coordenador geral poderá delegar tarefas e atribuir a execução de atividades a um colaborador.

Art. 76 Ao Comitê de Segurança da Informação ou à estrutura equivalente compete:

I - Estabelecer os países nos quais dados e informações custodiados pela administração pública federal poderão ser armazenados em soluções de computação em nuvem;

II - Definir os requisitos criptográficos mínimos para o armazenamento de dados e informações, custodiados pela administração pública federal, em soluções de computação em nuvem; e

III - Analisar, em caráter conclusivo, as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de computação em nuvem.

Art. 78 À alta administração do órgão ou da entidade compete aprovar as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de computação em nuvem e divulgá-las às partes interessadas.

DOS REQUISITOS PARA A ADOÇÃO SEGURA DE COMPUTAÇÃO EM NUVEM

Art. 77 . Deverão ser observados os requisitos mínimos deste Capítulo para que os órgãos ou as entidades adotem soluções de computação em nuvem de forma segura, com o objetivo de elevar o nível de proteção das informações no uso dessa tecnologia.

Art. 78 Antes de transferir serviços ou informações para um provedor de serviço de nuvem, os órgãos ou as entidades deverão, no mínimo:

I - Garantir que estejam alinhadas à legislação brasileira e aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros as seguintes operações:

a) de coleta, armazenamento, guarda e tratamento de registros de dados pessoais; e

b) de comunicações realizadas por provedores de conexão e de aplicações de internet, em que pelo menos um desses atos ocorra em território nacional;

II - Realizar o gerenciamento de riscos, precedido por análise e relatório de impacto de dados pessoais, em conformidade com a legislação, dos seguintes itens:

a) O tipo de informação a ser migrada;

b) O fluxo de tratamento dos dados que podem ser afetados com a adoção da solução;

c) O valor dos ativos envolvidos; e

d) Os benefícios da adoção de uma solução de computação em

nuvem, em relação aos riscos de segurança e privacidade referentes à disponibilização de informações e serviços a um terceiro;

III - Definir o modelo de serviço e de implementação de computação em nuvem que será adotado;

IV - Utilizar, para os sistemas estruturantes, somente os modelos de implementação de nuvem privada ou de nuvem comunitária, desde que restritas às infraestruturas de órgãos ou de entidades;

V - Avaliar quais informações serão hospedadas na nuvem, considerando:

a) O processo de classificação da informação de acordo com a legislação;

b) O valor do ativo de informação;

c) Os controles de acessos físico e lógico relativos à segurança da informação; e

d) O modelo de serviço e de implementação de computação em nuvem;

VI - Definir as medidas de mitigação de riscos e de custos para a implementação de solução de computação em nuvem e para possibilidade de crescimento dessa solução; e

VII - planejar custos de migração das informações e dos serviços, nos casos de ingresso e de saída do serviço de computação em nuvem.

Da capacidade do provedor de serviço de nuvem para implementar atualizações

Art.79 Em função da capacidade de o provedor de serviço de nuvem implementar atualizações relacionadas à segurança da informação em seus produtos e serviços, os provedores de serviço deverão, no mínimo:

I – disponibilizar sistemas operacionais atualizados pelos patchs de segurança mais recentes no momento da instalação ou da disponibilização de máquina virtual com o sistema operacional pré-instalado. As demais atualizações dos recursos computacionais deverão ser regidas pelas melhores práticas do mercado; e

II - Revisar e atualizar periodicamente seus processos internos de gestão de riscos de segurança da informação.

Do gerenciamento de identidades e de registros (logs)

Art.80 Em relação ao gerenciamento de identidades e de registros, o MAPA deverá, no mínimo:

I - Adotar um padrão de identidade federada para permitir quando possível o uso de tecnologia single sign-on no processo de autenticação de seus usuários no provedor de serviço de nuvem;

II - Negar ao provedor de serviço de nuvem permissão de uso e acesso direto ao ambiente de autenticação do MAPA;

III - adotar, de acordo com o nível de criticidade da informação, quando possivel, o uso da tecnologia, single sign-on, o qual deve ser acompanhado:

a) de autenticação multifator; adotar uma solução de 2FA contendo o OTP (Sigla de One True Pairing) como 2º fator.

Ou b) Implementação da gestão de ID com o conceito Many to one.

b) de uma alternativa que aumente o grau de segurança no processo de autenticação de seus usuários no provedor de serviço de nuvem;

IV – O Mapa deve exigir do provedor de serviço de nuvem que:

a) registre todos os acessos administrativos, incidentes e eventos cibernéticos, incluídas informações sobre sessões e transações; e

b) armazene, pelo período de um ano, todos os registros de que trata a alínea a;

V - Armazenar os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações, por cinco anos, no ambiente do provedor de serviço de nuvem ou em ambiente próprio controlado, à critério do órgão ou da entidade contratante;

VI - Manter em ambiente próprio controlado, pelo período de cinco anos, os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações recebidos do provedor de serviço de nuvem; e

VII - Capacitar a equipe de segurança para acessar e utilizar os registros gerados pelo provedor de serviço de nuvem.

Do uso de recursos criptográficos

Art.81 Em relação à necessidade do uso de recursos criptográficos pelo Ministérios da Agricultura e Pecuária, órgãos e entidades integrantes do MAPA, deverão, no mínimo:

I - Verificar se os dados da organização estão sendo tratados e armazenados de acordo com a legislação;

II – Os provedores de serviço em nuvem contratados pelo órgão deverão adotar o padrão criptográfico TLS 1.2 ou superior, no mínimo. O TLS (Transport Layer Security), como o SSL (Secure Sockets Layer), é um protocolo de criptografia destinado a manter os dados seguros ao ser transferido por uma rede).

III - utilizar, sempre que possível, chaves de encriptação baseadas em hardware.

Da segregação de dados e da separação lógica

Art.82 Em relação à segregação de dados e à separação lógica em ambientes de computação em nuvem, o provedor de serviço de nuvem, deverá adotar, no mínimo, os seguintes padrões:

I - Garantir que o ambiente contratado seja protegido de usuários externos do serviço em nuvem e de pessoas não autorizadas, implantar e

implementar controles de segurança da informação de forma a propiciar o isolamento adequado dos recursos utilizados pelos diferentes órgãos ou entidades da administração pública federal e por outros usuários do serviço em nuvem;

II - Adotar firewall de rede em conformidade com os padrões determinados pelo MAPA;

III - Possibilitar que seja aplicada segregação lógica apropriada dos dados das aplicações virtualizadas, dos sistemas operacionais, do armazenamento e da rede a fim de estabelecer a separação de recursos utilizados;

IV - Adotar firewall de aplicação em conformidade com os padrões estabelecidos pelo MAPA;

V - Possibilitar a separação de todos os recursos utilizados pelo Provedor de Serviço de Nuvem daqueles recursos utilizados pela administração interna do órgão ou da entidade; e

VI - Avaliar os riscos associados à execução de softwares proprietários a serem instalados no serviço de nuvem.

Do gerenciamento da nuvem

Art.83 Em relação ao gerenciamento da nuvem, o MAPA deverá, no mínimo:

I - Capacitar a equipe responsável por esse gerenciamento nas tecnologias utilizadas pelo provedor de serviço de nuvem;

II - Exigir que o provedor de serviço de nuvem documente e comunique seus recursos, papéis e responsabilidades de segurança da informação para o uso de seus serviços em nuvem;

III - Elaborar uma matriz de responsabilidades que inclua obrigações e responsabilidades próprias; e

IV - Elaborar um processo de tratamento de incidentes junto ao provedor de serviço de nuvem e comunicá-lo à equipe responsável pelo gerenciamento da nuvem.

Do tratamento da informação

Art.84 Em relação ao tratamento da informação em ambiente de computação em nuvem, o MAPA, além de cumprir as orientações contidas na legislação sobre proteção de dados pessoais, deve observar as seguintes diretrizes:

I - Informação sem restrição de acesso poderá ser tratada em ambiente de nuvem, considerada a legislação e os riscos de segurança da informação;

II - Informação classificada em grau de sigilo e documento preparatório que possa originar informação classificada não poderão ser tratados em ambiente de computação em nuvem; e

III - Poderão ser tratados em ambiente de computação em nuvem, observados os riscos de segurança da informação e a legislação vigente:

a) A informação com restrição de acesso prevista na legislação, conforme o Anexo a esta Instrução Normativa;

b) O material de acesso restrito regulado pelo próprio órgão ou pela entidade;

c) A informação pessoal relativa à intimidade, vida privada, honra e imagem; e

Art.85 Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo órgão ou pela entidade, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, observando-se as seguintes disposições:

I - Pelo menos uma cópia atualizada de segurança deve ser mantida em território brasileiro;

II - A informação sem restrição de acesso poderá possuir cópias atualizadas de segurança fora do território brasileiro, conforme legislação aplicável;

III - a informação com restrição de acesso prevista na legislação e o documento preparatório não previsto, bem como suas cópias atualizadas de segurança, não poderão ser tratados fora do território brasileiro, conforme legislação aplicável; e

IV - No caso de dados pessoais, deverão ser observadas as orientações previstas na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD, e demais legislações sobre o assunto.

Das cláusulas contratuais específicas

Art.86 O instrumento contratual a ser firmado com um provedor de serviço de nuvem para a prestação do serviço de computação em nuvem deve conter dispositivos que tratem dos requisitos estabelecidos nos itens 8 a itens 17 além de, no mínimo, os seguintes procedimentos de segurança:

I - Termo de confidencialidade que impeça o provedor de serviço de nuvem de usar, transferir e liberar dados, sistemas, processos e informações do órgão ou da entidade para empresas nacionais, transnacionais, estrangeiras, países e governos estrangeiros;

II - Garantia da exclusividade de direitos, por parte do órgão ou da entidade, sobre todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, tais como backups de segurança;

III - proibição do uso de informações do órgão ou da entidade pelo provedor de serviço de nuvem para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado;

IV - Conformidade da política de segurança da informação do provedor de serviço de nuvem com a legislação brasileira;

V - Devolução integral dos dados, informações e sistemas sob custódia do provedor de serviço de nuvem aos órgãos ou às entidades contratantes ao término do contrato;

VI - Eliminação, por parte do provedor de serviço de nuvem, ao término do contrato, de qualquer dado, informação ou sistema do órgão ou entidade sob sua custódia, observada a legislação que trata da obrigatoriedade de retenção de dados; e

VII - Garantia do direito ao esquecimento para dados pessoais, conforme art. 16 da Lei nº 13.709, de 14 de agosto de 2018 - LGPD.

DOS REQUISITOS DO PROVEDOR DE SERVIÇO DE NUVEM

Art.87 Para que esteja habilitado a prestar serviços de computação em nuvem para os órgãos ou as entidades da administração pública federal, o provedor de serviço de nuvem deverá cumprir, no mínimo, os seguintes requisitos:

I - Possuir metodologia de gestão de riscos, elaborada em conformidade com as melhores práticas e com a legislação, bem como realizar o gerenciamento de riscos ;

II - Implementar práticas de fortalecimento dos mecanismos de virtualização, que devem incluir, no mínimo, os seguintes procedimentos:

a) Desabilitar ou remover todas as interfaces, portas, dispositivos ou serviços desnecessários executados pelo sistema operacional;

b) Configurar com segurança todas as interfaces de rede e áreas de armazenamento virtuais;

c) Estabelecer limites para a utilização dos recursos de máquina virtual (Virtual Machine - VM);

d) Manter todos os sistemas operacionais e as aplicações em execução na máquina virtual em suas versões mais atuais;

e) Validar a integridade das operações de gerenciamento de chaves criptográficas;

f) possuir controles que permitam aos usuários autorizados do órgão ou da entidade acessarem os registros de acesso administrativo do monitor de máquina virtual -Hypervisor;

g) habilitar o registro completo do Hypervisor; e

h) suportar o uso de máquinas virtuais confiáveis (Trusted VM) fornecidas pelo órgão ou pela entidade, que estejam em conformidade com as políticas e práticas de fortalecimento de redes exigidas ao provedor de serviço de nuvem;

III - em relação ao gerenciamento de identidades e registros:

a) possuir procedimentos de controle de acesso que abordem a transição entre as funções, os limites e controles dos privilégios dos usuários e os controles de utilização das contas de usuários;

b) impor mecanismo de autenticação que exija tamanho mínimo, complexidade, duração e histórico de senhas de acesso;

c) suportar, quando possível, a tecnologia single sign-on para autenticação;

d) suportar mecanismos de autenticação multifator ou outra alternativa que aumente o grau de segurança no processo de autenticação de usuários do órgão ou da entidade no provedor de serviço de nuvem, de acordo com nível de criticidade da informação;

e) permitir ao MAPA ou à entidade gerenciar as próprias identidades, inclusive criação, atualização, exclusão e suspensão no ambiente fornecido pelo provedor de serviço de nuvem; e

f) atender aos requisitos legais, às melhores práticas de segurança e a outros critérios exigidos pelo órgão ou pela entidade em seus processos de autenticação, controle de acesso, contabilidade e de registro (formato, retenção e acesso);

IV - Em relação à segurança de aplicações web disponibilizadas no ambiente de nuvem:

a) utilizar firewalls especializados na proteção de sistemas e aplicações;

b) desenvolver código web em conformidade com as melhores práticas de desenvolvimento seguro e com os normativos existentes;

c) utilizar melhores práticas de segurança de sistemas operacionais e de aplicações;

d) realizar periodicamente testes de penetração de redes e de aplicações; e

e) possuir um programa de correção de vulnerabilidades;

V - Possuir processos de gestão de continuidade de negócios e de gestão de mudanças, em conformidade com os normativos existentes e com as melhores práticas nessas áreas;

VI - Possuir um plano de recuperação de desastres que estabeleça procedimentos de recuperação e de restauração de plataforma, infraestrutura, aplicações e dados após incidentes de perda de dados;

VII -Estabelecer um canal de comunicação seguro utilizando, no mínimo, Transport Layer Security (/TLS);

VIII - utilizar um padrão de encriptação seguro, conforme padrão internacional reconhecidamente aceito, que possa ser implementado com chaves de encriptação geradas e armazenadas pelo órgão ou pela entidade;

IX - Disponibilizar facilidades que possibilitem a aplicação de uma proteção criptográfica própria do órgão ou da entidade;

X - Em relação à segregação de dados:

a) Isolar, utilizando separação lógica, todos os dados e serviços do MAPA de outros clientes de serviço em nuvem;

b) Segregar o tráfego de gerenciamento do tráfego de dados do MAPA; e

c) Implementar dispositivos de segurança entre zonas;

XI - Possuir procedimentos em relação ao descarte de ativos de informação e de dados, que assegurem:

a) Sanitizar ou destruir, de modo seguro, os dados existentes nos dispositivos descartados por meio da utilização de métodos que estejam em conformidade com os padrões estabelecidos para a conduta e as melhores práticas;

b) Destruir, de modo seguro, ativo de informação no fim do ciclo de vida ou considerado inservível, com o fornecimento de um Certificado de Destruição de Equipamento Eletrônico (Certificate of Electronic Equipment Destruction - CEED) e discriminar os ativos que foram reciclados, bem como o peso e os tipos de materiais obtidos em virtude do processo de destruição; e

c) Armazenar, de modo seguro, ativos de informação a serem descartados, em ambiente com acesso físico controlado, com registro de toda movimentação de entrada e de saída de dispositivos;

XII - Notificar, imediatamente, ao MAPA incidente cibernético contra os serviços ou dados sob sua custódia;

XIII - possuir procedimentos necessários para preservação de evidências, conforme legislação; e

XIV - demonstrar estar em conformidade com os padrões de segurança de nuvem, por meio de auditoria anual um relatório SOC 2 Tipo II concentra-se nos Critérios de Serviço de Confiança do Instituto Americano de Contadores Públicos Certificados (AICPA) (anteriormente Princípios de Serviço de Confiança). Ele examina os controles internos e sistemas de um provedor de serviços relacionados à segurança, disponibilidade, integridade de processamento, confidencialidade e privacidade de dados.

DA UTILIZAÇÃO DE CLOUD BROKERS

Art.88 O cloud broker deverá atuar como integrador dos serviços de computação em nuvem entre o MAPA, órgãos e institutos do ministério da agricultura e Pecuária, de dois ou mais provedores de serviço de nuvem.

Art.89 Caso o órgão ou a entidade contrate por meio do cloud broker plataforma de gestão multinuvem para realizar procedimentos de provisionamento e orquestração do ambiente, é necessário que a ferramenta possua, no mínimo:

I - Em relação às funcionalidades de provisionamento e orquestração de multinuvem:

a) Um único portal integrado de provisionamentos para o usuário final;

b) Utilização de modelos de provisionamento;

c) Automação segura de provisionamento simultâneo e utilização, no que couber, ferramentas de código aberto e interoperáveis;

d) Fluxos de trabalho de orquestração baseada em eventos; e

e) Soluções seguras integradas de criação de infraestrutura por código - IaaC;

II - Em relação às funcionalidades de monitoramento e análise em multinuvem:

a) relatórios de monitoramento de desempenho de recursos na nuvem;

b) coleta e monitoramento de registros; e

c) procedimentos de monitoramento de alertas;

III - Em relação às funcionalidades de inventário e classificação em multinuvem:

a) inventário de recursos na nuvem;

b) procedimentos de segurança para configuração de recursos na plataforma de gestão multinuvem; e

c) detecção de recursos sem etiqueta; e

IV - Em relação às funcionalidades de gerenciamento de

segurança, conformidade e identidade:

a) mecanismos, quando possivel, de single sign-on e de autenticação multifator das plataformas em nuvem;

b) gerenciamento seguro de usuários e de grupos de usuários;

c) gerenciamento de segurança dos recursos;

d) notificações de eventos de alerta multicanal;

e) gerenciamento de identidade e acesso - IAM; e

f) registros de atividade da plataforma em nuvem.

Parágrafo único. O cloud broker poderá utilizar ferramenta de

Software as a Service (SaaS)comum de mercado, desde que não haja risco de dependência tecnológica para disponibilizar essa plataforma.

Art.90 O cloud broker o responsável por garantir que os provedores de serviço de nuvem que ele representa:

I - Cumpram todos os requisitos previstos nesta Portaria e na legislação brasileira; e

II - Operem de acordo com as melhores práticas de segurança.

Parágrafo único. O órgão ou a entidade deverá prever no instrumento contratual que o cloud broker poderá ser responsabilizado, civil e administrativamente, por qualquer desconformidade nos provedores que ele representa.

Art.91 Para garantir a segurança de que trata esta portaria, os órgãos e as entidades poderão adotar outras diretrizes complementares, desde que não confrontem as previsões da legislação.

Art.92 A apresentação dos relatórios de tipo I e tipo II da auditoria SOC 2, comprovada a conformidade com os padrões de segurança em nuvem, é condição essencial, tanto para habilitar a participação em processo licitatório, como para renovar o contrato de prestação de serviço em nuvem com órgãos ou entidades da administração pública federal. (INSTRUÇÃO NORMATIVA Nº 5, DE 30 DE AGOSTO DE 2021, Art 25); https://www.aicpa.org/

Parágrafo único. Na hipótese de utilização de cloud broker, esse será o responsável por apresentar os relatórios de tipo I e tipo II da auditoria SOC 2 de todos os provedores de serviço de nuvem que ele representa.

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Orientações Gerais

Art.93º Este documento foi criado a partir de informações contidas nas seguintes referências:

I- Instrução Normativa SGD/ME nº 94, de dezembro de 2022 regida pela Lei nº 14133, de 2021;

II- Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023.

As dúvidas devem ser dirimidas através das referências acima ou em contato com a Secretaria do Governo Digital do Ministério da Gestão e da

Inovação em serviços Públicos.

Documento assinado eletronicamente por **MARCO ANTONIO BITTENCOURT SUCUPIRA**, **Coordenador Geral de Infraestrutura, Segurança e Serviços Digitais**, em 19/03/2025, às 17:28, conforme horário oficial de Brasília, com fundamento no art. 4º,§ 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **HIMALAYA HUDOLF TRINDADE CAMPOS**, **Coordenador de Gestão de Redes, Datacenters e Computação em Cloud**, em 19/03/2025, às 17:41, conforme horário oficial de Brasília, com fundamento no art. 4º,§ 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site: https://sei.agro.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **41305189** e o código CRC **D16701AF**.

Referência: Processo nº 21000.020699/2024-80 SEI nº 41305189