INMETRO

INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA

Boletim de SERVIÇO

EDIÇÃO ESPECIAL

Portaria nº 285, de 19 de maio de 2025

Data de Publicação:

20 de maio de 2025

BOLETIM DE SERVIÇO

EDIÇÃO ESPECIAL

Marcio Andre Oliveira Brito
Presidente do INMETRO

Gildásio Nascimento Rocha
Diretor de Administração e Finanças

Jorge Andre Moreira Medeiros Soares
Coordenador-Geral de Gestão de Pessoas

Rio de Janeiro,20 de maio de 2025.

Publicação eletrônica disponível na intranet produzida mensalmente pela COGEP – Coordenação-Geral de Gestão de Pessoas.

As matérias aqui publicadas deverão ser do conhecimento de todos os servidores de cada unidade do Inmetro.

O Boletim de Serviço impresso encontra-se disponível para consulta no Serviço de Documentação e Informação – Sedin.

Este boletim contém a seguinte seção:
1. Atos do Presidente

Neste número, foram publicadas as matérias encaminhadas Coordenação-Geral de Gestão de Pessoas - Cogep, até a data do fechamento do boletim.

SUMÁRIO

Portaria nº 285, de 19 de maio de 2025.....3-16

Serviço Público Federal

MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA, COMÉRCIO E SERVIÇOS
INSTITUTO NACIONAL DE METROLOGIA , QUALIDADE E TECNOLOGIA - INMETRO

Portaria nº 285, de 19 de maio de 2025.

Estabelece a Estratégia de uso de *software* e de serviços de computação em nuvem no âmbito do Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO)

O PRESIDENTE DO INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA - INMETRO, **SUBSTITUTO**, no exercício da competência que lhe foi outorgada pelo artigo 4º, § 2º, da Lei nº 5.966, de 11 de dezembro de 1973, combinado com o disposto no artigo 18, incisos II e III, do Decreto n.º 11.221, de 5 de outubro de 2022 e o art. 12, da Lei nº 9.784, de 29 de janeiro de 1999.

Considerando a **Portaria SGD/MGI nº 5.950**, de 26 de outubro de 2023, que 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.

Considerando o que consta no Processo nº 0052600.003137/2025-17, **resolve**:

Art. 1º Aprovar, na forma do anexo único desta Portaria, o Documento de Estratégia de Uso de Software e de Serviços de Computação em Nuvem no âmbito do Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO), em conformidade com a SGD/MGI nº 5.950, de 26 de outubro de 2023.

Art. 2º A Coordenação-Geral de Tecnologia da Informação (CTINF) da Diretoria de Inovação, Planejamento e Articulação Institucional (DPLAN) do Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO) deverá adotar, monitorar e garantir a aplicação das diretrizes estabelecidas na Estratégia de Uso de Software e de Serviços de Computação em Nuvem, visando garantir a qualidade e a conformidade na utilização dos recursos e nas contratações de software e dos serviços de nuvem de acordo com as necessidades de negócio do Inmetro.

Art. 3º Esta Portaria entra em vigor na data da sua publicação no Boletim de Serviço do Inmetro.

DOCUMENTO ASSINADO ELETRONICAMENTE COM FUNDAMENTO NO ART. 6º, § 1º, DO DECRETO Nº 8.539, DE 8 DE OUTUBRO DE 2015 EM 20/05/2025, ÀS 11:10, CONFORME HORÁRIO OFICIAL DE BRASÍLIA, POR

JOÃO NERY RODRIGUES FILHO

Presidente, Substituto

ANEXO ÚNICO

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

1. **DO ESCOPO**

1.1. A estratégia de uso de software e de serviços de computação em nuvem tem o objetivo de assegurar que o INMETRO obtenha os resultados esperados e mitigue os riscos associados à adoção de possíveis novas tecnologias ou novas formas de contratação no âmbito do INMETRO.

1.2. Esta estratégia deve ser aplicada para novas contratações de *software* e de serviços de computação em nuvem no âmbito do INMETRO, tais como: (incluindo, mas não se limitando a)

I - software sob o modelo de licenciamento permanente de direitos de uso;

II - software sob o modelo de cessão temporária de direitos de uso;

III - software sob o modelo de subscrição ou como Serviço (SaaS);

IV - Infraestrutura como Serviço (IaaS);

V - Plataforma como Serviço (PaaS);

VI - suporte técnico para software e serviços de computação em nuvem;

VII - serviço de operação e gerenciamento de recursos em nuvem;

VIII - serviço de migração de recursos para ambiente de nuvem;

IX - integração de serviços de computação em nuvem; e

X - consultoria especializada em software e/ou serviços de computação em nuvem.

2. **DAS REFERÊNCIAS**

2.1. Para o desenvolvimento da estratégia de uso de software e de serviços de computação em nuvem, cabe ao INMETRO observar, sem prejuízo das demais normas em vigor:

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

II - Instrução Normativa GSI/PR 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;

III - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

IV - Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação;

V - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

VI - Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

VII - Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021 que dispõe sobre os processos relacionados à gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal;

VIII - Decreto nº 10.641, de 2 de março de 2021, que altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da Segurança da Informação, e altera o , que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional;

IX - Portaria SGD/MGI nº 852, de 28 de março de 2023, que dispõe o Programa de Privacidade e Segurança da Informação; e

X - demais leis, decretos, resoluções, portarias e instruções normativas relacionadas à Segurança da Informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República.

3. DOS CONCEITOS E DEFINIÇÕES

3.1. Para fins de compreensão dos termos utilizados nesta norma serão considerados os seguintes conceitos e definições:

I - **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;

II - **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;

III - **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;

IV - **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;

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

VI - **Computação em nuvem:** modelo que possibilita o provisionamento e a utilização sob 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;

VII - **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;

VIII - **Data center ou centro de dados:** Consiste em uma estrutura, ou grupo de estruturas, dedicada à acomodação centralizada, interconexão e operação dos equipamentos de tecnologia da informação e redes 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 para fornecer a disponibilidade de serviço desejada, conforme ABNT NBR ISO/IEC 22.237-1:2023;

IX - **Disponibilidade:** condição de um serviço ou recurso estar acessível e apto para desempenhar plenamente suas funções, em determinado momento ou durante um período acordado;

X - **Hosting:** locação de recursos computacionais localizados em infraestrutura física tradicional de data center pertencente a terceiros, sem o compartilhamento de recursos entre clientes, para a hospedagem de aplicações e soluções de TI;

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

XII - **Incidente de Segurança da Informação:** qualquer evento de Segurança da Informação indesejável e inesperado, seja único ou em série, que pode comprometer as operações de negócio e ameaçar a Segurança da Informação;

XIII - **IN GSI/PR nº 5, de 2021:** Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, que 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;

XIV - **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;

XV - **Instância de Computação:** componente 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;

XVI - **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 mais provedores de serviço de computação em nuvem. O *Cloud Broker* apoia o órgão ou entidade em descobrir, planejar, migrar, 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, como a ISO e a NIST e, no Brasil, a Associação Brasileira de Normas Técnicas - ABNT, para garantir que os serviços sejam oferecidos de forma segura, eficiente e confiável;

XVII - **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;

XVIII - **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;

XIX - **Licença por subscrição/assinatura:** permite aos usuários acessar 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;

XX - **Licença perpétua:** é uma licença que concede ao usuário o direito de usar o software por tempo indeterminado, bem como acesso a *updates* e suporte técnico por tempo determinado;

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

XXII - **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;

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

XXIV - **Modelo de Serviços em nuvem IaaS (*Infrastructure as a Service* – Infraestrutura como 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;

XXV - **Modelo de Serviços em nuvem PaaS (*Platform as a Service* – Plataforma 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;

XXVI - **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;

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

XXVIII - **Nuvem comunitária:** modelo de implantação de nuvem em que os serviços de computação em nuvem são exclusivamente suportados e compartilhados por um grupo específico de órgãos e entidades de serviços de computação em nuvem que têm 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 — Part 1: Vocabulary*). 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;

XXIX - **Nuvem de governo:** infraestrutura de nuvem privada ou comunitária gerida exclusivamente por órgãos ou empresas públicas;

XXX - **Nuvem híbrida:** 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;

XXXI - **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 de empresas públicas com finalidade específica relacionada à tecnologia da informação, conforme ISO/IEC 22123-1:2023 (*Information technology — Cloud computing — Part 1: Vocabulary*). 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 empresas públicas, e não se configurando como uso de Nuvem Pública;

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

XXXIII - **Orquestração:** habilidade de coordenar e gerenciar recursos em diferentes provedores de nuvem públicas;

XXXIV - **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;

XXXV - **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;

XXXVI - **Região:** agrupamento de localizações geográficas específicas em que os recursos computacionais se encontram hospedados;

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

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

XXXIX - **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, além de outras atividades auxiliares comuns a todos os órgãos da Administração que, a critério do Poder Executivo, necessitem de coordenação central;

XL - **Software livre:** tipo de software de código aberto que pode ser usado, estudado, modificado e redistribuído gratuitamente. O software livre é publicado sob uma licença que permite aos usuários acessar os códigos-fonte e modificá-los para atender às suas necessidades;

XLI - **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 acessar o código-fonte, mas impõe certas limitações quanto a sua modificação ou personalização;

XLII - **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”;

XLIII - **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;

XLIV - **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;

XLV - **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;

XLVI - **Função como Serviço (FaaS)**: recursos fornecidos ao órgão e entidade para construir e gerenciar aplicativos de microserviços ou equivalentes, de forma escalável, conforme ISO 22123-2:2023; e

XLVII - **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.

4. **DOS PRINCÍPIOS**

4.1. Esta estratégia segue os seguintes princípios:

I - respeito aos princípios e diretrizes constitucionais, legais e regulamentares que regem a Administração Pública Federal;

II - garantia de integridade, autenticidade e disponibilidade da informação sob a custódia do INMETRO, com respeito ao princípio da transparência e atribuição de confidencialidade apenas nos casos expressamente previstos na legislação;

III - alinhamento estratégico da Política de Segurança da Informação com os demais planos institucionais;

IV - responsabilidade pelo cumprimento das normas pertinentes à Segurança da Informação vigentes; e

V - conscientização, educação e comunicação como alicerces fundamentais para o fomento da cultura em Segurança da Informação.

5. **DAS DISPOSIÇÕES GERAIS**

5.1. A Coordenação-Geral de Tecnologia da Informação (CTINF) da Diretoria de Inovação, Planejamento e Articulação Institucional (DPLAN) deve analisar e autorizar os softwares de uso corporativo da instituição;

5.2. Para a contratação de softwares, deve prever e tratar o risco de dependência tecnológica a um fornecedor (risco de *lockin*);

5.3. A CTINF deve manter atualizado o inventário de softwares da instituição.

6. **DAS DIRETRIZES PARA DEFINIÇÃO DA ESTRATÉGIA DE USO DE SOFTWARE E DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM**

6.1. As seguintes diretrizes deverão ser observadas pelo INMETRO ao adotar soluções de computação em nuvem de forma segura, com o objetivo de elevar o nível de proteção das informações no uso dessa tecnologia.

6.2. **Da identificação das necessidades do negócio**

6.2.1. O INMETRO deve identificar e avaliar as necessidades de negócio antes da contratação de software e de serviços de computação em nuvem;

6.2.1.1. Deve 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.

6.2.1.2. Deve avaliar, quando da concepção de novos serviços e sistemas, quanto à viabilidade de que os serviços sejam desenvolvidos para utilização em ambientes de nuvem ou não;

6.3. **Da seleção dos modelos adequados**

6.3.1. O INMETRO deve 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.

6.3.1.1. Caso o INMETRO 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.

6.3.1.2. Caso o INMETRO possua maturidade suficiente e já tenha concluído que a demanda prevista pode ser atendida integralmente por meio de serviços em nuvem, poderá ser adotada uma abordagem completa, contemplando inclusive as demandas de migração do ambiente *on-premises* para a nuvem.

6.3.1.3. Para definição do modelo de implementação a ser adotado, devem ser consideradas as características específicas de cada carga de trabalho (*workload*) e a respectiva necessidade de negócio que a originou.

6.3.1.4. Quando houver previsão de implementação de soluções totalmente em nuvem, o processo de aquisição deverá incluir um plano de recuperação dos serviços, a ser acionado em caso de descontinuidade do instrumento contratual por fatores externos.

6.3.2. O modelo de fornecimento dos softwares deverá ser compatível com as disponibilidades orçamentárias do Inmetro.

6.3.3. A natureza e a criticidade das informações deverão ser consideradas na seleção do modelo de fornecimento do software.

6.4. **Da avaliação dos possíveis fornecedores**

6.4.1. Deve ampliar a participação de fornecedores, assegurando os critérios mínimos de qualidade necessários.

6.4.2. Os critérios de seleção de fornecedores devem considerar as diretrizes da Instrução Normativa GSI/PR nº 5, 30 de agosto de 2021, da Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023 e outras condições necessárias para atendimento à necessidade de negócio.

6.4.3. 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.

6.5. **Da definição de requisitos de segurança**

6.5.1. O INMETRO deve observar 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.

6.6. **Das condições mínimas de infraestrutura de TIC para utilizar serviços de computação em nuvem**

6.6.1. O INMETRO deve realizar a avaliação das condições mínimas de infraestrutura de TIC necessárias para a utilização de serviços de computação em nuvem, como, por exemplo, a disponibilidade de conexão estável com a Internet e a largura de banda adequada.

6.7. **Do estabelecimento de uma política de governança**

6.7.1. O INMETRO deve garantir que as contratações apresentem claramente as diretrizes e os papéis e responsabilidades dos atores organizacionais (da TI, das áreas de negócio e da nuvem), observando as práticas e orientações fornecidas pela Secretaria de Governo Digital - SGD em seus manuais e normativos relacionados a contratações de softwares e serviços em nuvem.

6.7.2. A CTINF deve possuir especialistas em computação em nuvem para auxiliar a gestão e operação dos serviços.

6.8. **Do estabelecimento dos princípios norteadores da estratégia**

6.8.1. O INMETRO deve adotar os seguintes princípios norteadores da estratégia:

6.8.2. ***Cloud First*;**

6.8.2.1. **Prioridade para a nuvem:** Deve priorizar a adoção de serviços e soluções em nuvem sempre que possível, considerando fatores como custo, agilidade, escalabilidade e segurança.

6.8.2.2. **Avaliação de benefícios:** Deve avaliar continuamente os benefícios de usar a nuvem em comparação com soluções *on-premises*, garantindo que a nuvem seja a primeira opção viável.

6.8.3. ***Lift-and-Shift* como último recurso;**

6.8.3.1. **Otimização e modernização:** Antes de optar pelo *lift-and-shift* (migrar aplicações e dados para a nuvem sem modificações), deve avaliar a possibilidade de otimização e modernização das aplicações para tirar o máximo proveito dos recursos e benefícios da nuvem.

6.8.3.2. **Uso racional:** Para utilizar o *lift-and-shift*, deve assegurar que outras abordagens mais otimizadas não são viáveis, garantindo eficiência e economia de recursos.

6.8.4. **Uso de *broker multicloud;***

6.8.4.1. **Gestão *multicloud*:** Deve implementar um *broker multicloud* para gerenciar, integrar e otimizar o uso de múltiplas plataformas de nuvem, facilitando a interoperabilidade e a portabilidade entre diferentes provedores de serviços em nuvem.

6.8.4.2. **Agregação de valor:** Deve assegurar que o *broker multicloud* agrega valor ao facilitar a interoperabilidade, a portabilidade e a gestão de custos entre diferentes provedores de serviços em nuvem.

6.8.5. **Segurança e conformidade;**

6.8.5.1. **Segurança da informação:** Deve implementar medidas de segurança robustas, incluindo criptografia, controle de acesso, monitoramento contínuo e backups regulares, para garantir a proteção das informações tratadas em ambiente de nuvem.

6.8.5.2. **Conformidade regulatória:** Deve assegurar que todas as operações em nuvem estejam em conformidade com as normas e regulamentações aplicáveis, como a Instrução Normativa GSI/PR nº 5, de 2021, e a Instrução Normativa SGD/ME nº 94, de 2022.

6.8.6. **Monitoramento e governança;**

6.8.6.1. **Supervisão contínua:** Deve estabelecer mecanismos de monitoramento e governança contínua para garantir o cumprimento das políticas e procedimentos definidos, bem como a eficiência e a segurança dos serviços em nuvem.

6.8.6.2. **Comitê de Governança Digital:** As decisões estratégicas relacionadas ao uso da nuvem devem ser supervisionadas e aprovadas pelo Comitê de Governança Digital ou estrutura colegiada equivalente.

6.8.7. **Treinamento e capacitação;**

6.8.7.1. **Capacitação contínua:** Deve oferecer treinamento e capacitação contínua para os profissionais envolvidos na gestão e operação dos serviços em nuvem, garantindo que estejam atualizados com as melhores práticas e novas tecnologias.

6.8.8. **Gestão de riscos;**

6.8.8.1. **Identificação e mitigação de riscos:** Deve desenvolver estratégias para identificar e mitigar os riscos associados ao uso da nuvem, incluindo a elaboração de planos de resposta a incidentes e a implementação de medidas preventivas.

6.9. **Do alinhamento com outros planos estratégicos**

6.9.1. Esta estratégia deve estar alinhada com os seguintes planos estratégicos:

I - Plano Estratégico do Inmetro (PEI);

II - Plano Diretor de Tecnologia da Informação e Comunicação do Inmetro (PDTIC);

III - Plano de Contratações Anual (PCA);

IV - Política de Segurança da Informação do Inmetro (POSIN);

6.9.2. **Integração e sincronização**

6.9.2.1. **Harmonização de objetivos**: Deve assegurar que os objetivos dos diversos planos estratégicos estejam alinhados e contribuam para a estratégia global do Inmetro. Isso envolve a harmonização dos objetivos do PEI, PDTIC, PCA e POSIN.

6.9.2.2. **Coordenação de atividades**: Deve promover a coordenação entre as atividades planejadas nos diferentes planos para evitar sobreposições e conflitos.

6.9.3. **Coerência e consistência**

6.9.3.1. **Coerência das ações**: Deve garantir que as ações definidas nos planos estratégicos sejam coerentes entre si, evitando duplicidades e inconsistências.

6.9.3.2. **Consistência de metas**: Alinhar as metas e indicadores de desempenho dos planos estratégicos para que estejam em consonância com as metas institucionais.

6.9.4. **Planejamento participativo**

6.9.4.1. **Envolvimento das partes interessadas**: Deve envolver todas as partes interessadas, incluindo as áreas de negócio, a TI, e a Alta Administração, no processo de planejamento para assegurar a contribuição de diferentes perspectivas e necessidades.

6.9.4.2. **Feedback contínuo**: Deve implementar mecanismos de feedback contínuo para ajustar e alinhar os planos estratégicos conforme necessário.

6.9.5. **Monitoramento e avaliação**

6.9.5.1. **Mecanismos de monitoramento**: Deve estabelecer mecanismos de monitoramento contínuo para verificar o progresso dos planos estratégicos e assegurar que estejam sendo implementados conforme planejado.

6.9.5.2. **Avaliação de resultados**: Deve realizar avaliações periódicas dos resultados alcançados em relação aos objetivos e metas estabelecidos nos planos estratégicos.

6.9.6. **Flexibilidade e adaptabilidade**

6.9.6.1. **Capacidade de adaptação**: Deve assegurar que os planos estratégicos sejam flexíveis e possam ser adaptados às mudanças no ambiente interno e externo.

6.9.6.2. **Revisão periódica**: Deve realizar revisões periódicas dos planos estratégicos para garantir que permaneçam relevantes e alinhados com as necessidades da organização.

6.9.7. **Diretrizes específicas**

6.9.7.1. **Plano Estratégico do Inmetro (PEI)**: Deve fornecer a visão geral e os objetivos de longo prazo da organização, orientando os demais planos estratégicos.

6.9.7.2. **Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC)**: Deve detalhar as iniciativas e projetos de TIC que apoiarão a execução do PEI.

6.9.7.3. **Plano de Contratações Anual (PCA)**: Deve refletir as necessidades de contratação de bens e serviços de TIC identificadas no PDTIC, assegurando que as contratações estejam alinhadas com a estratégia global da organização.

6.9.7.4. **Política de Segurança da Informação do Inmetro (POSIN):** Declaração formal acerca do compromisso com a proteção dos dados e informações de sua propriedade e/ou sob sua guarda no âmbito do Instituto Nacional de Metrologia Qualidade e Tecnologia - Inmetro;

6.10. **Do estabelecimento de linhas de base e metas de benefícios/resultados esperados**

6.10.1. O INMETRO deve adotar as seguintes linhas de base e metas de benefícios/resultados esperados:

6.10.1.1. **Identificar o estado atual (AS IS)**: Deve mapear o cenário atual, identificando pontos fortes, fraquezas, oportunidades e ameaças.

6.10.1.2. **Definir o estado futuro desejado (TO BE)**: Deve estabelecer metas claras e mensuráveis para alcançar um estado mais eficiente e seguro.

6.10.1.3. **Desenvolver um plano de ação**: Deve criar um plano detalhado para transição do estado atual para o estado futuro, incluindo etapas, recursos necessários e cronograma.

6.10.1.4. **Monitorar e ajustar**: Deve implementar um sistema de monitoramento contínuo para garantir que as metas estão sendo atingidas e fazer ajustes conforme necessário.

6.11. **Das considerações sobre capacitação da equipe**

6.11.1. O INMETRO deve capacitar a equipe que gerenciará, operará ou utilizará os recursos de software e de computação de serviços em nuvem, identificando as capacidades e habilidades necessárias.

6.11.2. **Identificação de capacidades e habilidades**: A equipe deve ter conhecimento técnico sobre a infraestrutura de nuvem, Segurança da Informação, gerenciamento de projetos e análise de dados.

6.11.3. **Treinamento contínuo**: Deve investir em treinamentos regulares para garantir que a equipe esteja atualizada com as melhores práticas e novas tecnologias.

6.11.4. **Certificações**: Deve incentivar a obtenção de certificações reconhecidas no mercado.

6.11.5. **Especialização**: Deve promover a especialização em áreas específicas, como segurança cibernética, desenvolvimento de aplicativos em nuvem e gerenciamento de desempenho.

6.11.6. **Colaboração e comunicação**: Deve fomentar uma cultura de colaboração e comunicação eficaz entre os membros da equipe para resolver problemas e melhorar processos.

6.12. **Das considerações sobre portabilidade e interoperabilidade entre sistemas, dados e serviços**

6.12.1. O INMETRO deve considerar a viabilidade de adoção de medidas para mitigar a dependência tecnológica ou aprisionamento ao provedor.

6.12.2. **Portabilidade de dados**: Deve assegurar que os dados possam ser transferidos de um sistema para outro sem perda de integridade ou qualidade.

6.12.3. **Interoperabilidade**: Deve garantir que diferentes sistemas possam trabalhar juntos de maneira eficiente, permitindo a troca de informações e serviços.

6.12.4. **Mitigação da dependência tecnológica***:* Deve promover a adoção de medidas que reduzam a dependência de um único provedor, evitando o aprisionamento dos usuários.

6.12.5. **Adoção de tecnologias abertas**: Deve incentivar o uso de tecnologias e padrões abertos que facilitem a portabilidade e interoperabilidade.

6.12.6. **Transparência e segurança**: Deve assegurar que os processos de portabilidade e interoperabilidade sejam transparentes e seguros, protegendo a privacidade e a segurança dos dados.

6.13. **Dos requisitos regulatórios e de conformidade**

6.13.1. O INMETRO deve considerar os requisitos regulatórios e de conformidade para o uso seguro de software e serviços de computação em nuvem no âmbito do INMETRO e da Administração Pública Federal.

6.13.2. **Cumprimento legal**: Os dispositivos devem estar em conformidade com todas as leis e regulamentos aplicáveis, incluindo as normas internas da empresa.

6.13.3. **Conformidade e segurança**: Deve garantir que os dispositivos atendam aos padrões de segurança e conformidade exigidos, tanto a nível nacional quanto internacional.

6.13.4. **Documentação e procedimentos**: Deve manter uma documentação adequada e seguir procedimentos estabelecidos para assegurar a conformidade contínua.

6.13.5. **Auditorias e inspeções**: Deve realizar auditorias e inspeções regulares para verificar a conformidade e identificar áreas de melhoria.

6.13.6. **Treinamento e conscientização**: Deve implementar programas de treinamento e conscientização para garantir que todos os funcionários estejam cientes dos requisitos de conformidade e segurança.

6.14. **Da indicação da estratégia de saída**

6.14.1. O INMETRO deve considerar a análise de dependências e aspectos de portabilidade (backup, redundância, contratos de apoio, retorno para a infraestrutura local, etc.).

6.14.2. **Análise de dependências**: Deve realizar a avaliação das dependências tecnológicas e operacionais entre sistemas e serviços.

6.14.3. **Aspectos de portabilidade**: Deve ter em consideração a facilidade de transferência de dados e serviços para outras plataformas ou ambientes.

6.14.4. **Backup e redundância**: Deve implementar soluções de backup e redundância para garantir a continuidade dos serviços em caso de falhas.

6.14.5. **Contratos de apoio**: Deve estabelecer contratos de apoio técnico e administrativo para suporte contínuo.

6.14.6. **Retorno para a infraestrutura local**: Deve implementar um planejamento para o retorno dos serviços à infraestrutura local, caso necessário.

6.15. **Da análise de riscos**

6.15.1. O INMETRO deve considerar as diretrizes de gerenciamento de riscos constantes no modelo de contratação de software e de serviços de computação em nuvem estabelecidos na Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023 ou documento equivalente publicado posteriormente.

6.15.2. **Identificação de riscos**: Deve reconhecer e documentar todos os riscos potenciais associados às atividades da organização.

6.15.3. **Avaliação de riscos**: Deve analisar a probabilidade e a gravidade dos riscos identificados.

6.15.4. **Mitigação de riscos**: Deve implementar medidas para reduzir ou eliminar os riscos identificados.

6.15.5. **Monitoramento e revisão**: Deve monitorar continuamente os riscos e revisar as medidas de mitigação conforme necessário.

7. DA DEFINIÇÃO DOS REQUISITOS PARA O USO SEGURO DE COMPUTAÇÃO EM NUVEM

7.1. O INMETRO trata os requisitos para uso seguro de computação em nuvem em norma específica para esta finalidade.

8. DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

8.1. Da Alta Administração

8.1.1. Compete à Alta Administração:

I - aprovar as minutas de elaboração e de revisões do ato normativo sobre estratégia e o uso seguro de computação em nuvem e divulgá-las às partes interessadas;

II - assegurar a utilização de tecnologias de computação em nuvem em conformidade com as orientações contidas neste documento; e

III - disponibilizar recursos financeiros e humanos para a implementação desta estratégia.

8.2. Do Comitê de Segurança da Informação

8.2.1. Compete ao Comitê de Segurança da Informação:

I - estabelecer os países nos quais dados e informações custodiados pela administração pública federal poderão ser armazenados em soluções de computação em nuvem (com apoio do Gestor de Segurança da Informação e da CTINF);

II - definir os requisitos criptográficos mínimos para o armazenamento de dados e informações, custodiados pela administração pública federal, em soluções de computação em nuvem (com apoio do Gestor de Segurança da Informação e da CTINF);

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

8.3. Do Gestor de Segurança da Informação

8.3.1. Compete ao Gestor de Segurança da Informação:

I - instituir e coordenar a equipe para elaboração e revisões do ato normativo sobre estratégia e o uso seguro de computação em nuvem;

II - supervisionar a aplicação do ato normativo sobre estratégia e o uso seguro de computação em nuvem;

III - assegurar a contínua efetividade da comunicação com o provedor de serviço de nuvem, de forma a assegurar que os controles e os níveis de serviço relacionados à Segurança da Informação acordados sejam cumpridos;

IV - supervisionar a aplicação das medidas de correção pelo provedor de serviço de nuvem, em casos de eventuais desvios relacionados à Segurança da Informação;

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, exceto se envolver dados pessoais, quando o Encarregado de dados será o responsável pela comunicação;

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; e

VII - propor ações de Segurança da Informação para a implementação ou a contratação, de tecnologias de computação em nuvem em conformidade com as orientações contidas neste documento.

8.4. **Da Coordenação-Geral de Tecnologia da Informação - CTINF**

8.4.1. Compete à Coordenação-Geral de Tecnologia da Informação - CTINF:

I - implementar os procedimentos relativos ao uso de tecnologias de computação em nuvem em conformidade com as orientações contidas neste documento e legislação pertinente.

9. DA REVISÃO E ATUALIZAÇÃO

9.1. Esta estratégia bem como os documentos gerados a partir dela devem ser revisados, aprovados e atualizados em função de alterações na legislação pertinente, de diretrizes políticas do Governo Federal, de alterações nas políticas e normas do INMETRO, quando considerada necessária pelo Comitê de Segurança da Informação.

9.2. Em função da capacidade de os provedores de serviço de computação em nuvem implementar atualizações relacionadas à Segurança da Informação em seus produtos e serviços, **a presente estratégia deve ser revisada em até 2 (dois) anos para**:

I - definir novos critérios e a periodicidade das atualizações dos procedimentos e dos recursos computacionais a serem observados pelo provedor de serviço de nuvem;

II - atualizar periodicamente os processos internos de gestão de riscos de Segurança da Informação;

III - quando ocorrerem eventos, fatores relevantes, novos requisitos tecnológicos, corporativos e/ ou legais que exijam sua revisão imediata; e

IV - assegurar a continuidade, sustentabilidade, adequação e efetividade quando houver mudanças significativas nos requisitos de Segurança da Informação que influenciem o uso seguro da computação em nuvem.

10. DAS DISPOSIÇÕES FINAIS

10.1. As novas contratações de software e serviços de computação em nuvem devem observar as diretrizes apresentadas neste documento, bem como o 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.

10.2. Esta estratégia e seus documentos complementares devem ser divulgados a todos os usuários e partes interessadas a fim de promover sua observância e conhecimento.

10.3. A alta administração deve disponibilizar os recursos (humanos, tecnológicos e financeiros) necessários para a execução desta estratégia.

10.4. Os casos omissos não abordados neste documento serão analisados pelo Comitê de Segurança da Informação.

10.5. Esta norma entra em vigor a partir da data de sua publicação.

Apresentação de Portaria do Inmetro - Rev.04 - Publicado Out/2011 - Responsabilidade: Profe - Referência NIG-Profe-001