MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais
Reitoria

PORTARIA Nº 5495/IFMG, DE 03 DE OUTUBRO DE 2025

Dispõe sobre a estratégia de uso de software e de serviços de computação em nuvem no âmbito do Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais (IFMG).

O **REITOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MINAS GERAIS**, no uso das atribuições que lhe são conferidas pelo Estatuto da Instituição, republicado com alterações no Diário Oficial da União do dia 08/05/2018, Seção 1, Páginas 09 e 10, e pelo Decreto de 11 de setembro de 2023, publicado no DOU de 12 de setembro de 2023, Seção 2, Edição nº 174, página 01

Considerando a deliberação do Comitê de Tecnologia da Informação e Comunicação (CTIC); e o que consta no Processo nº **23208.005307/2024-51**,

RESOLVE

Aprovar , na forma do Anexo Único desta Portaria, o Documento de Estratégia de Uso de Software e de Serviços de Computação em Nuvem do IFMG, em conformidade com a SGD/MGI nº 5.950, de 26 de outubro de 2023.

Art. 1º A área de TI do IFMG 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 órgão.
Art. 2º Esta Portaria entra em vigor na data de sua assinatura.

ANEXO ÚNICO

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

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º A estratégia de uso de software e de serviços de computação em nuvem, no âmbito do IFMG, visa assegurar a obtenção dos resultados esperados e a mitigação dos riscos associados à adoção de possíveis novas tecnologias ou novas formas de contratação.

Art. 2° Esta estratégia deve ser aplicada para novas contratações de software e de serviços de computação em nuvem no âmbito do IFMG.

CAPÍTULO II

DOS OBJETIVOS E COMPETÊNCIAS

Art. 3º São objetivos da desta estratégia:

I - Apoiar a tomada de decisão e os demais instrumentos relacionados à adoção de soluções de computação em nuvem;

II - Modernização da infraestrutura de TIC, por meio da adoção de tecnologias modernas e flexíveis para atender às demandas do IFMG;

III - Otimização de custos, através da redução dos gastos com infraestrutura, licenciamento de software e gerenciamento de TIC;

IV - Melhoria da eficiência operacional, com a automatização de processos, simplificação do acesso a recursos e aumento da produtividade;

V - Aprimoramento da segurança da informação, fortalecendo a proteção dos dados e sistemas do IFMG em ambiente de nuvem.

Art. 4º Possuem competências no âmbito dessa estratégia:

I - Comitê de Tecnologia da Informação e Comunicação (CTIC), responsável por aprovar a estratégia, supervisionar sua implementação e definir as diretrizes gerais;

II - Diretoria de Tecnologia da Informação (DTI), responsável por planejar, contratar, gerenciar e operar os serviços de nuvem;

III - Demais setores do IFMG, responsáveis por utilizar os serviços de nuvem de forma eficiente e segura, seguindo as diretrizes estabelecidas.

CAPÍTULO III

DOS CONCEITOS E DEFINIÇÕES

Art. 5° 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;

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;

XLVIII - Lift and Shift, ou "Rehosting": é uma estratégia de migração para a nuvem que consiste em mover aplicações, sistemas e dados de um ambiente local para a nuvem (pública ou privada) sem fazer alterações significativas em sua arquitetura ou código;

XLIX – Cloud first: é uma estratégia empresarial que prioriza o uso de soluções e serviços de computação em nuvem (cloud computing) como a primeira opção para novas iniciativas de TI, em vez de optar por infraestruturas locais (on-premises).

CAPÍTULO III

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

Art. 6° Um conjunto de diretrizes deverá ser observado pelo IFMG ao adotar soluções de computação em nuvem de forma segura, com o objetivo de possibilitar o alcance dos resultados esperados e minimizar os riscos envolvidos no uso dessa tecnologia.

Seção I

Da identificação das necessidades do negócio

Art. 7° O IFMG deve identificar e avaliar as necessidades de negócio antes da contratação de softwares ou serviços de computação em nuvem.

Parágrafo único. 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.

Seção II

Da seleção dos modelos adequados

Art. 8° O IFMG deve avaliar quais modelos de serviço (IaaS, PaaS, SaaS) e de implementação (nuvem pública, nuvem privada, nuvem híbrida e etc.) melhor se adequam aos requisitos de negócio.

§1º É recomendável dar preferência à adoção de uma abordagem estratégica de nuvem híbrida, caso não possua maturidade suficiente na contratação de serviços em nuvem ou possua impedimentos técnicos ou normativos para migração de algum recurso.

§2º Uma abordagem completa, incluindo as demandas de migração do ambiente on-premise para a nuvem, pode ser adotada caso o IFMG possua maturidade e já tenha concluído que a demanda prevista pode ser atendida integralmente por meio de serviços em nuvem.

§3º Ainda que adotada uma abordagem completa de migração para a nuvem, o IFMG deve manter um ambiente on-premise mínimo, conforme previsto no §3º do art. 21, para assegurar a possibilidade de retorno operacional em caso de interrupção dos serviços em nuvem. Além disso, devem ser consideradas previsões de contingenciamento no orçamento federal, de forma a garantir a continuidade dos serviços essenciais diante de eventuais limitações financeiras.

§4º A Diretoria de Tecnologia da Informação deverá, previamente à adoção de soluções de nuvem, realizar análise comparativa de custo e benefício

entre a contratação de serviços de co-location e a utilização de serviços em nuvem, considerando aspectos técnicos, financeiros e de continuidade de negócios.

§5º Essa análise deverá:

I – demonstrar a viabilidade econômica da solução escolhida, mediante comparação de custos diretos e indiretos;

II – avaliar os benefícios institucionais em termos de escalabilidade, disponibilidade, desempenho e segurança;

III – indicar, de forma justificada, se a contratação de nuvem representa vantagem em relação ao co-location, ou se este último é a alternativa mais adequada ao caso concreto.

§6º O resultado da análise deverá integrar os Estudos Técnicos Preliminares (ETP) e ser submetido à apreciação do Comitê de Tecnologia da Informação e Comunicação, quando se tratar de contratação de alta materialidade ou relevância.

Seção III

Da avaliação dos possíveis fornecedores

Art. 9º. Os estudos técnicos preliminares devem abranger o levantamento dos possíveis fornecedores aptos ao atendimento dos requisitos de negócio, de forma a garantir a competitividade e a conformidade com as normas aplicáveis.

Parágrafo único. A avaliação de fornecedores deverá considerar, no mínimo:

I – os fatores de segurança, conformidade, disponibilidade e suporte técnico, em consonância com a Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, a Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, e demais normativos aplicáveis;

II – localização dos datacenters em território nacional;

III – certificações de segurança e privacidade (ISO/IEC 27001, ISO/IEC 27701, SOC 2 ou equivalentes reconhecidos);

IV – aderência integral à LGPD e legislação nacional correlata;

V – comprovação de mecanismos de portabilidade e interoperabilidade, prevenindo dependência tecnológica excessiva (vendor lock-in);

VI – histórico e mecanismos de resposta a incidentes de segurança e indisponibilidade;

VII – política de suporte técnico, incluindo tempos de resposta e canais de atendimento compatíveis com as necessidades institucionais.

Seção IV

Da definição de requisitos de segurança

Art. 10. O IFMG deve determinar e exigir requisitos mínimos de segurança da informação para a contratação e uso de softwares e serviços em nuvem, de forma a proteger os dados institucionais e garantir a continuidade dos serviços.

§1º Os requisitos mínimos a serem exigidos dos fornecedores incluem:

I – criptografia de dados em repouso e em trânsito, com algoritmos reconhecidos pela ABNT e ITI;

II – autenticação multifator (MFA) para acessos administrativos e críticos;

III – geração e retenção de logs de auditoria imutáveis, com possibilidade de exportação para análise pelo IFMG;

IV – segregação lógica e física adequada em ambientes multi-tenant, garantindo isolamento de dados institucionais;

V – suporte a planos de continuidade e recuperação de desastres, com

RTO e RPO alinhados às necessidades do IFMG;

VI – comprovação de certificações em segurança da informação (ISO/IEC 27001, ISO/IEC 27701, SOC 2, ou equivalentes);

VII – aderência integral às exigências da Instrução Normativa GSI/PR nº 5, de 2021.

§2º A avaliação do atendimento a esses requisitos deve ocorrer nos Estudos Técnicos Preliminares e ser registrada no Termo de Referência e nos contratos.

§3º Exceções a requisitos de segurança somente poderão ser aceitas mediante aprovação expressa do Comitê de Tecnologia da Informação e Comunicação, com justificativa técnica e plano de mitigação.

Seção V

Do estabelecimento de uma política de governança

Art. 11° A política de governança do IFMG deve abranger 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 IFMG.

Seção VI

Das diretrizes de uso seguro de software e de serviços de computação em nuvem

Art. 12° O IFMG deve definir políticas e normas que versam sobre segurança da informação e sobre o tratamento de informações em nuvem, bem

como identificar, sob essa perspectiva, quais os sistemas ou recursos 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.

Seção VII

Da avaliação quanto às condições mínimas de infraestrutura de TIC para utilização de serviços de computação em nuvem

Art. 13º O IFMG deve ter conexão estável com a Internet e com banda suficiente para gerenciar softwares e serviços de computação em nuvem.

§ 1º Devem ser avaliadas e mantidas as condições mínimas de infraestrutura de TIC que garantam o pleno funcionamento dos serviços em nuvem, incluindo a qualidade da conexão, largura de banda e disponibilidade de rede.

§ 2º O IFMG deve dispor de firewall, ou equipamento equivalente, com capacidade de estabelecer conexões VPN seguras, garantindo a integridade, confidencialidade e autenticidade dos dados no tráfego entre os ambientes locais e os serviços em nuvem.

§ 3º A infraestrutura de segurança de rede deve ser continuamente monitorada e atualizada, assegurando proteção contra acessos não autorizados, vazamentos de dados e outras ameaças cibernéticas associadas ao uso de serviços em nuvem.

Seção VIII

Da definição de diretrizes de governança para o uso da nuvem

Art. 14° O IFMG deve definir papéis e responsabilidades para as áreas de TI, de negócio e de nuvem.

Art. 15º É vedada a contratação direta de serviços de SaaS (software como serviço) pelas unidades descentralizadas do IFMG, sem a anuência do Comitê de Tecnologia da Informação e Comunicação.

Parágrafo único. Todas as demandas por SaaS deverão ser previamente submetidas à DTI, que realizará análise quanto a requisitos de segurança, conformidade normativa, custo-benefício e integração aos sistemas institucionais, observando o disposto nesta Estratégia e nos Estudos Técnicos Preliminares (ETP).

Seção IX

Do estabelecimento dos princípios norteadores da estratégia

Art. 16° O IFMG deve adotar os seguintes princípios norteadores da estratégia:

I - Adoção da filosofia Cloud-First sempre que for possível;

II - Uso da abordagem “Lift And Shift” como último recurso; e

III - Preferência pelo uso de broker multicloud

Seção X

Do alinhamento com outros documentos institucionais

Art. 17° Esta estratégia deve estar alinhada com os seguintes planos estratégicos e políticas:

I - Plano de Desenvolvimento Institucional (PDI);

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

III - Plano de Contratações Anual (PCA); e

IV - Política de Segurança da Informação (POSIN).

Seção XI

Do estabelecimento de linhas de base e metas de benefícios e resultados esperados

Art. 18° O IFMG deve definir linhas de base e metas de benefícios e resultados esperados, com o objetivo de promover maior agilidade, redução de custos, resiliência e segurança na adoção de softwares e serviços em nuvem.

§ 1º A definição das metas deve ter como ponto de partida o mapeamento do cenário atual (AS IS), identificando os ativos de TIC existentes, bem como suas limitações, riscos e oportunidades de melhoria.

§ 2º Os benefícios e resultados esperados com a adoção de soluções em nuvem devem ser comparados com os indicadores da estrutura atual on-premise, considerando aspectos como desempenho, custo, segurança e continuidade dos serviços.

§ 3º Essa comparação deve fundamentar tecnicamente as decisões de migração, permitindo que as escolhas estratégicas se baseiem em critérios objetivos e alinhados ao interesse institucional.

§4º O acompanhamento da execução desta Estratégia será realizado por meio de um painel de indicadores, que deve contemplar, no mínimo:

I – disponibilidade dos serviços em nuvem;

II – tempo médio de provisionamento de recursos;

III – custo total da nuvem em relação ao baseline on-premise;

IV – conformidade em requisitos de segurança e privacidade;

V – número e gravidade de incidentes de segurança relacionados à nuvem;

VI – percentual de serviços com backup externo validado;

VII – evolução da capacitação da equipe.

§5º As linhas de base desses indicadores serão levantadas no diagnóstico previsto no §1º e homologadas pelo Comitê de Tecnologia da Informação e Comunicação.

§6º A Diretoria de Tecnologia da Informação será responsável por coletar e publicar mensalmente os indicadores, submetendo relatório analítico trimestral ao Comitê de Tecnologia da Informação e Comunicação.

§7º O não atingimento recorrente das metas deverá ensejar plano de ação corretivo, com prazos, responsáveis e evidências.

Seção XII

Das considerações sobre capacitação da equipe

Art. 19° O IFMG 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.

Parágrafo único: O treinamento deve ser contínuo e especializado, de modo a assegurar que a equipe permaneça atualizada quanto às melhores práticas de uso, aos avanços em segurança da informação e às tecnologias emergentes em computação em nuvem

Seção XIII

Das considerações sobre portabilidade e interoperabilidade entre sistemas, dados e serviços

Art. 20° O IFMG deve considerar a viabilidade de adoção de medidas para mitigar a dependência tecnológica ou aprisionamento ao provedor.

Seção XIV

Dos requisitos regulatórios e de conformidade

Art. 21 O IFMG deve assegurar que o uso e a contratação de softwares e serviços de computação em nuvem estejam em conformidade com os requisitos regulatórios e normativos aplicáveis à Administração Pública Federal.

§1º Devem ser observados, no mínimo:

I – a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD);

II – a Instrução Normativa GSI/PR nº 5/2021, que trata dos requisitos mínimos de segurança em nuvem;

III – a Portaria SGD/MGI nº 5.950/2023, no que se refere à estratégia e ao modelo de contratação de software e serviços de nuvem;

IV – as diretrizes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP;

V – os instrumentos de planejamento e governança do IFMG, como o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), o Plano de Contratações Anual (PCA) e a Política de Segurança da Informação (POSIN);

VI – requisitos normativos específicos aplicáveis ao setor público, como os emanados pelo MEC, CGU, TCU e ANPD.

§2º Os contratos firmados deverão conter cláusulas expressas que assegurem:

I – a localização e soberania dos dados, com armazenamento em território nacional, salvo exceções devidamente justificadas;

II – a definição clara das responsabilidades de segurança compartilhada entre provedor e IFMG;

III – a portabilidade e reversibilidade (exit strategy) dos serviços, inclusive cópias e backups externos ao ambiente do provedor;

IV – o direito de auditoria e fiscalização pelo IFMG e por órgãos de controle da Administração Pública;

V – a obrigatoriedade de notificação imediata de incidentes de segurança ou indisponibilidade que afetem os serviços do IFMG.

§3º A Diretoria de Tecnologia da Informação deverá assegurar que tais requisitos estejam devidamente refletidos nos Estudos Técnicos Preliminares, no Termo de Referência e nos contratos administrativos.

Seção XV

Da indicação da estratégia de saída

Art. 22° O IFMG deve considerar a análise de dependências e aspectos de portabilidade, incluindo rotinas de backup, redundância, contratos de apoio e viabilidade de retorno dos serviços à infraestrutura local.

§ 1º A estratégia de saída deve estar alinhada à Política Institucional de Backup vigente, assegurando que os procedimentos de cópia, retenção e restauração de dados sejam aplicados de forma padronizada e segura, inclusive nos ambientes de nuvem.

§ 2º É obrigatória a realização de backups externos ao ambiente de nuvem contratado, de modo a garantir a independência da instituição em situações de falha, encerramento contratual, descontinuidade ou abandono do serviço por parte do provedor.

§ 3º O IFMG deve manter um ambiente on-premise com infraestrutura mínima necessária para suportar o retorno das aplicações e dados essenciais, assegurando a continuidade dos serviços em caso de necessidade de transição emergencial.

Seção XVI

Da análise de riscos

Art. 23° O IFMG 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.

CAPÍTULO IV

DO USO SEGURO DE COMPUTAÇÃO EM NUVEM

Art. 24º O IFMG deverá observar requisitos de segurança da informação para a utilização segura de software e de serviços de computação em nuvem, conforme Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, que deverão estar em norma específica para esta finalidade.

CAPÍTULO V

DAS DISPOSIÇÕES FINAIS

Art. 25° Esta estratégia e 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 IFMG, ou quando uma revisão for considerada necessária pelo Comitê de Tecnologia da Informação e Comunicação.

Art. 26° 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.

Art. 27° Esta estratégia e seus documentos complementares devem ser divulgados a todos os usuários e partes interessadas a fim de promover sua

observância e conhecimento.

Art. 28° Os casos omissos não abordados neste documento serão tratados pelo Comitê de Tecnologia da Informação e Comunicação.

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 do IFMG, em conformidade com a SGD/MGI nº 5.950, de 26 de outubro de 2023.

Art. 2º A área de TI do IFMG 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 órgão.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

ANEXO ÚNICO

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

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º A estratégia de uso de software e de serviços de computação em nuvem, no âmbito do IFMG, visa assegurar a obtenção dos resultados esperados e a mitigação dos riscos associados à adoção de possíveis novas

tecnologias ou novas formas de contratação.

Art. 2° Esta estratégia deve ser aplicada para novas contratações de software e de serviços de computação em nuvem no âmbito do IFMG.

CAPÍTULO II

DOS OBJETIVOS E COMPETÊNCIAS

Art. 3º São objetivos da desta estratégia:

I - Apoiar a tomada de decisão e os demais instrumentos relacionados à adoção de soluções de computação em nuvem;

II - Modernização da infraestrutura de TIC, por meio da adoção de tecnologias modernas e flexíveis para atender às demandas do IFMG;

III - Otimização de custos, através da redução dos gastos com infraestrutura, licenciamento de software e gerenciamento de TIC;

IV - Melhoria da eficiência operacional, com a automatização de processos, simplificação do acesso a recursos e aumento da produtividade;

V - Aprimoramento da segurança da informação, fortalecendo a proteção dos dados e sistemas do IFMG em ambiente de nuvem.

Art. 4º Possuem competências no âmbito dessa estratégia:

I - Comitê de Tecnologia da Informação e Comunicação (CTIC), responsável por aprovar a estratégia, supervisionar sua implementação e definir as diretrizes gerais;

II - Diretoria de Tecnologia da Informação (DTI), responsável por planejar, contratar, gerenciar e operar os serviços de nuvem;

III - Demais setores do IFMG, responsáveis por utilizar os serviços de nuvem de forma eficiente e segura, seguindo as diretrizes estabelecidas.

CAPÍTULO III

DOS CONCEITOS E DEFINIÇÕES

Art. 5° 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;

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;

XLVIII - Lift and Shift, ou "Rehosting": é uma estratégia de migração para a nuvem que consiste em mover aplicações, sistemas e dados de um ambiente local para a nuvem (pública ou privada) sem fazer alterações

significativas em sua arquitetura ou código;

XLIX – Cloud first: é uma estratégia empresarial que prioriza o uso de soluções e serviços de computação em nuvem (cloud computing) como a primeira opção para novas iniciativas de TI, em vez de optar por infraestruturas locais (on-premises).

CAPÍTULO III

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

Art. 6° Um conjunto de diretrizes deverá ser observado pelo IFMG ao adotar soluções de computação em nuvem de forma segura, com o objetivo de possibilitar o alcance dos resultados esperados e minimizar os riscos envolvidos no uso dessa tecnologia.

Seção I

Da identificação das necessidades do negócio

Art. 7° O IFMG deve identificar e avaliar as necessidades de negócio antes da contratação de softwares ou serviços de computação em nuvem.

Parágrafo único. 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.

Seção II

Da seleção dos modelos adequados

Art. 8° O IFMG deve avaliar quais modelos de serviço (IaaS, PaaS, SaaS) e de implementação (nuvem pública, nuvem privada, nuvem híbrida e etc.) melhor se adequam aos requisitos de negócio.

§1º É recomendável dar preferência à adoção de uma abordagem estratégica de nuvem híbrida, caso não possua maturidade suficiente na contratação de serviços em nuvem ou possua impedimentos técnicos ou normativos para migração de algum recurso.

§2º Uma abordagem completa, incluindo as demandas de migração do ambiente on-premise para a nuvem, pode ser adotada caso o IFMG possua maturidade e já tenha concluído que a demanda prevista pode ser atendida integralmente por meio de serviços em nuvem.

§3º Ainda que adotada uma abordagem completa de migração para a nuvem, o IFMG deve manter um ambiente on-premise mínimo, conforme previsto no §3º do art. 21, para assegurar a possibilidade de retorno operacional em caso de interrupção dos serviços em nuvem. Além disso, devem ser consideradas previsões de contingenciamento no orçamento federal, de forma a garantir a continuidade dos serviços essenciais diante de eventuais limitações financeiras.

§4º A Diretoria de Tecnologia da Informação deverá, previamente à adoção de soluções de nuvem, realizar análise comparativa de custo e benefício entre a contratação de serviços de co-location e a utilização de serviços em nuvem, considerando aspectos técnicos, financeiros e de continuidade de negócios.

§5º Essa análise deverá:

I – demonstrar a viabilidade econômica da solução escolhida, mediante comparação de custos diretos e indiretos;

II – avaliar os benefícios institucionais em termos de escalabilidade, disponibilidade, desempenho e segurança;

III – indicar, de forma justificada, se a contratação de nuvem representa vantagem em relação ao co-location, ou se este último é a alternativa mais adequada ao caso concreto.

§6º O resultado da análise deverá integrar os Estudos Técnicos Preliminares (ETP) e ser submetido à apreciação do Comitê de Tecnologia da

Informação e Comunicação, quando se tratar de contratação de alta materialidade ou relevância.

Seção III

Da avaliação dos possíveis fornecedores

Art. 9º. Os estudos técnicos preliminares devem abranger o levantamento dos possíveis fornecedores aptos ao atendimento dos requisitos de negócio, de forma a garantir a competitividade e a conformidade com as normas aplicáveis.

Parágrafo único. A avaliação de fornecedores deverá considerar, no mínimo:

I – os fatores de segurança, conformidade, disponibilidade e suporte técnico, em consonância com a Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, a Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, e demais normativos aplicáveis;

II – localização dos datacenters em território nacional;

III – certificações de segurança e privacidade (ISO/IEC 27001, ISO/IEC 27701, SOC 2 ou equivalentes reconhecidos);

IV – aderência integral à LGPD e legislação nacional correlata;

V – comprovação de mecanismos de portabilidade e interoperabilidade, prevenindo dependência tecnológica excessiva (vendor lock-in);

VI – histórico e mecanismos de resposta a incidentes de segurança e indisponibilidade;

VII – política de suporte técnico, incluindo tempos de resposta e canais de atendimento compatíveis com as necessidades institucionais.

Seção IV

Da definição de requisitos de segurança

Art. 10. O IFMG deve determinar e exigir requisitos mínimos de segurança da informação para a contratação e uso de softwares e serviços em nuvem, de forma a proteger os dados institucionais e garantir a continuidade dos serviços.

§1º Os requisitos mínimos a serem exigidos dos fornecedores incluem:

I – criptografia de dados em repouso e em trânsito, com algoritmos reconhecidos pela ABNT e ITI;

II – autenticação multifator (MFA) para acessos administrativos e críticos;

III – geração e retenção de logs de auditoria imutáveis, com possibilidade de exportação para análise pelo IFMG;

IV – segregação lógica e física adequada em ambientes multi-tenant, garantindo isolamento de dados institucionais;

V – suporte a planos de continuidade e recuperação de desastres, com RTO e RPO alinhados às necessidades do IFMG;

VI – comprovação de certificações em segurança da informação (ISO/IEC 27001, ISO/IEC 27701, SOC 2, ou equivalentes);

VII – aderência integral às exigências da Instrução Normativa GSI/PR nº 5, de 2021.

§2º A avaliação do atendimento a esses requisitos deve ocorrer nos Estudos Técnicos Preliminares e ser registrada no Termo de Referência e nos contratos.

§3º Exceções a requisitos de segurança somente poderão ser aceitas mediante aprovação expressa do Comitê de Tecnologia da Informação e Comunicação, com justificativa técnica e plano de mitigação.

Seção V

Do estabelecimento de uma política de governança

Art. 11° A política de governança do IFMG deve abranger 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 IFMG.

Seção VI

Das diretrizes de uso seguro de software e de serviços de computação em nuvem

Art. 12° O IFMG deve definir políticas e normas que versam sobre segurança da informação e sobre o tratamento de informações em nuvem, bem como identificar, sob essa perspectiva, quais os sistemas ou recursos 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.

Seção VII

Da avaliação quanto às condições mínimas de infraestrutura de TIC para utilização de serviços de computação em nuvem

Art. 13º O IFMG deve ter conexão estável com a Internet e com banda suficiente para gerenciar softwares e serviços de computação em nuvem.

§ 1º Devem ser avaliadas e mantidas as condições mínimas de

infraestrutura de TIC que garantam o pleno funcionamento dos serviços em nuvem, incluindo a qualidade da conexão, largura de banda e disponibilidade de rede.

§ 2º O IFMG deve dispor de firewall, ou equipamento equivalente, com capacidade de estabelecer conexões VPN seguras, garantindo a integridade, confidencialidade e autenticidade dos dados no tráfego entre os ambientes locais e os serviços em nuvem.

§ 3º A infraestrutura de segurança de rede deve ser continuamente monitorada e atualizada, assegurando proteção contra acessos não autorizados, vazamentos de dados e outras ameaças cibernéticas associadas ao uso de serviços em nuvem.

Seção VIII

Da definição de diretrizes de governança para o uso da nuvem

Art. 14° O IFMG deve definir papéis e responsabilidades para as áreas de TI, de negócio e de nuvem.

Art. 15º É vedada a contratação direta de serviços de SaaS (software como serviço) pelas unidades descentralizadas do IFMG, sem a anuência do Comitê de Tecnologia da Informação e Comunicação.

Parágrafo único. Todas as demandas por SaaS deverão ser previamente submetidas à DTI, que realizará análise quanto a requisitos de segurança, conformidade normativa, custo-benefício e integração aos sistemas institucionais, observando o disposto nesta Estratégia e nos Estudos Técnicos Preliminares (ETP).

Seção IX

Do estabelecimento dos princípios norteadores da estratégia

Art. 16° O IFMG deve adotar os seguintes princípios norteadores da estratégia:

I - Adoção da filosofia Cloud-First sempre que for possível;

II - Uso da abordagem “Lift And Shift” como último recurso; e

III - Preferência pelo uso de broker multicloud

Seção X

Do alinhamento com outros documentos institucionais

Art. 17° Esta estratégia deve estar alinhada com os seguintes planos estratégicos e políticas:

I - Plano de Desenvolvimento Institucional (PDI);

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

III - Plano de Contratações Anual (PCA); e

IV - Política de Segurança da Informação (POSIN).

Seção XI

Do estabelecimento de linhas de base e metas de benefícios e resultados esperados

Art. 18° O IFMG deve definir linhas de base e metas de benefícios e resultados esperados, com o objetivo de promover maior agilidade, redução de custos, resiliência e segurança na adoção de softwares e serviços em nuvem.

§ 1º A definição das metas deve ter como ponto de partida o mapeamento do cenário atual (AS IS), identificando os ativos de TIC existentes, bem como suas limitações, riscos e oportunidades de melhoria.

§ 2º Os benefícios e resultados esperados com a adoção de soluções em

nuvem devem ser comparados com os indicadores da estrutura atual on-premise, considerando aspectos como desempenho, custo, segurança e continuidade dos serviços.

§ 3º Essa comparação deve fundamentar tecnicamente as decisões de migração, permitindo que as escolhas estratégicas se baseiem em critérios objetivos e alinhados ao interesse institucional.

§4º O acompanhamento da execução desta Estratégia será realizado por meio de um painel de indicadores, que deve contemplar, no mínimo:

I – disponibilidade dos serviços em nuvem;

II – tempo médio de provisionamento de recursos;

III – custo total da nuvem em relação ao baseline on-premise;

IV – conformidade em requisitos de segurança e privacidade;

V – número e gravidade de incidentes de segurança relacionados à nuvem;

VI – percentual de serviços com backup externo validado;

VII – evolução da capacitação da equipe.

§5º As linhas de base desses indicadores serão levantadas no diagnóstico previsto no §1º e homologadas pelo Comitê de Tecnologia da Informação e Comunicação.

§6º A Diretoria de Tecnologia da Informação será responsável por coletar e publicar mensalmente os indicadores, submetendo relatório analítico trimestral ao Comitê de Tecnologia da Informação e Comunicação.

§7º O não atingimento recorrente das metas deverá ensejar plano de ação corretivo, com prazos, responsáveis e evidências.

Seção XII

Das considerações sobre capacitação da equipe

Art. 19° O IFMG 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.

Parágrafo único: O treinamento deve ser contínuo e especializado, de modo a assegurar que a equipe permaneça atualizada quanto às melhores práticas de uso, aos avanços em segurança da informação e às tecnologias emergentes em computação em nuvem

Seção XIII

Das considerações sobre portabilidade e interoperabilidade entre sistemas, dados e serviços

Art. 20° O IFMG deve considerar a viabilidade de adoção de medidas para mitigar a dependência tecnológica ou aprisionamento ao provedor.

Seção XIV

Dos requisitos regulatórios e de conformidade

Art. 21 O IFMG deve assegurar que o uso e a contratação de softwares e serviços de computação em nuvem estejam em conformidade com os requisitos regulatórios e normativos aplicáveis à Administração Pública Federal.

§1º Devem ser observados, no mínimo:

I – a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD);

II – a Instrução Normativa GSI/PR nº 5/2021, que trata dos requisitos mínimos de segurança em nuvem;

III – a Portaria SGD/MGI nº 5.950/2023, no que se refere à estratégia e

ao modelo de contratação de software e serviços de nuvem;

IV – as diretrizes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP;

V – os instrumentos de planejamento e governança do IFMG, como o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), o Plano de Contratações Anual (PCA) e a Política de Segurança da Informação (POSIN);

VI – requisitos normativos específicos aplicáveis ao setor público, como os emanados pelo MEC, CGU, TCU e ANPD.

§2º Os contratos firmados deverão conter cláusulas expressas que assegurem:

I – a localização e soberania dos dados, com armazenamento em território nacional, salvo exceções devidamente justificadas;

II – a definição clara das responsabilidades de segurança compartilhada entre provedor e IFMG;

III – a portabilidade e reversibilidade (exit strategy) dos serviços, inclusive cópias e backups externos ao ambiente do provedor;

IV – o direito de auditoria e fiscalização pelo IFMG e por órgãos de controle da Administração Pública;

V – a obrigatoriedade de notificação imediata de incidentes de segurança ou indisponibilidade que afetem os serviços do IFMG.

§3º A Diretoria de Tecnologia da Informação deverá assegurar que tais requisitos estejam devidamente refletidos nos Estudos Técnicos Preliminares, no Termo de Referência e nos contratos administrativos.

Seção XV

Da indicação da estratégia de saída

Art. 22° O IFMG deve considerar a análise de dependências e aspectos de portabilidade, incluindo rotinas de backup, redundância, contratos de apoio e viabilidade de retorno dos serviços à infraestrutura local.

§ 1º A estratégia de saída deve estar alinhada à Política Institucional de Backup vigente, assegurando que os procedimentos de cópia, retenção e restauração de dados sejam aplicados de forma padronizada e segura, inclusive nos ambientes de nuvem.

§ 2º É obrigatória a realização de backups externos ao ambiente de nuvem contratado, de modo a garantir a independência da instituição em situações de falha, encerramento contratual, descontinuidade ou abandono do serviço por parte do provedor.

§ 3º O IFMG deve manter um ambiente on-premise com infraestrutura mínima necessária para suportar o retorno das aplicações e dados essenciais, assegurando a continuidade dos serviços em caso de necessidade de transição emergencial.

Seção XVI

Da análise de riscos

Art. 23° O IFMG 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.

CAPÍTULO IV

DO USO SEGURO DE COMPUTAÇÃO EM NUVEM

Art. 24º O IFMG deverá observar requisitos de segurança da informação para a utilização segura de software e de serviços de computação em nuvem, conforme Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, que deverão estar em norma específica para esta finalidade.

CAPÍTULO V

DAS DISPOSIÇÕES FINAIS

Art. 25° Esta estratégia e 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 IFMG, ou quando uma revisão for considerada necessária pelo Comitê de Tecnologia da Informação e Comunicação.

Art. 26° 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.

Art. 27° Esta estratégia e seus documentos complementares devem ser divulgados a todos os usuários e partes interessadas a fim de promover sua observância e conhecimento.

Art. 28° Os casos omissos não abordados neste documento serão tratados pelo Comitê de Tecnologia da Informação e Comunicação.

Publicação: Transparência Ativa em 03 de outubro de 2025

Documento assinado eletronicamente sob fundamentação, por:
RAFAEL BASTOS TEIXEIRA | Reitor

Data da Assinatura:
03 de outubro de 2025 as 19:06 (America/Sao_Paulo)

Tipo de Documento:
Portaria

Autenticidade