



**MINISTÉRIO DA EDUCAÇÃO  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO MARANHÃO  
Comitê de Governança Digital**

**RESOLUÇÃO Nº 1/2025 DE 9 DE MAIO DE 2025**

Aprovar a Estratégia de Uso de Software e de Serviços de Computação em Nuvem, do Instituto Federal de Educação, Ciência e Tecnologia do Maranhão - IFMA.

**O PRESIDENTE DO COMITÊ DE GOVERNANÇA DIGITAL DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO MARANHÃO**, no uso de suas atribuições, com base na Portaria 044 de 05 de janeiro de 2021 e, considerando as disposições da Resolução CONSUP/IFMA Nº 020, de 10 de fevereiro de 2020.

considerando a decisão do plenário deste Comitê de Governança Digital na 4ª Reunião Ordinária de 02 de maio de 2025; e,

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

considerando a Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023.

**RESOLVE**

**Art. 1º** APROVAR a **Estratégia de Uso de Software e de Serviços de Computação em Nuvem** do Instituto Federal de Educação, Ciência e Tecnologia do Maranhão- IFMA.

**Art. 2º.** Esta Resolução entra em vigor na data de sua assinatura.

*(assinado eletronicamente)*

**CARLOS CESAR TEIXEIRA FERREIRA**  
Presidente do Comitê de Governança Digital

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

### CAPÍTULO I

#### DO ESCOPO

**Art. 1º** Esta normativa estabelece princípios, diretrizes e responsabilidades para o uso estratégico e seguro de software e serviços de computação em nuvem no Instituto Federal do Maranhão (IFMA).

**Art. 2º** Aplica-se a novas contratações e contratos vigentes relacionados a:

- I - Licenciamento permanente ou temporário de software;
- II - Software como Serviço (SaaS);
- III - Infraestrutura como Serviço (IaaS);
- IV - Plataforma como Serviço (PaaS);
- V - Suporte técnico para computação em nuvem;
- VI - Operação e gerenciamento em nuvem;
- VII - Migração e integração de recursos para nuvem;
- VIII - Consultoria especializada em computação em nuvem.

**Art. 3º** Esta normativa aplica-se aos dados tratados por sistemas, aplicações e serviços de Tecnologia da Informação e Comunicação (TIC) em nuvem.

### CAPÍTULO II

#### DOS OBJETIVOS

**Art. 4º** São objetivos desta normativa:

- I - Apoiar decisões relacionadas à computação em nuvem;
- II - Modernizar a infraestrutura tecnológica do IFMA;
- III - Otimizar custos e melhorar eficiência operacional;
- IV - Proteger informações contra ameaças, perdas e desastres;
- V - Garantir conformidade com a legislação vigente;
- VI - Definir responsabilidades claras aos servidores e fornecedores;
- VII - Assegurar a proteção e disponibilidade de dados críticos.

### CAPÍTULO III

#### DAS DEFINIÇÕES

**Art. 6º** Para fins de compreensão dos termos utilizados nesta normativa, serão considerados os seguintes conceitos, adotadas as definições constantes no Glossário de Segurança da Informação do Governo Federal e normas específicas correlatas:

**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.

**Ativos de informação:** os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

**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.

**Carga de trabalho (workload):** conjunto de recursos que compõem uma arquitetura técnica destinada a suportar um ou mais serviços de TIC.

**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.

**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.

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

**Computação em nuvem:** modelo que possibilita o provisionamento e a utilização 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.

**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.

**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.

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

**Função como Serviço (FaaS):** recursos fornecidos ao órgão e entidade para construir e gerenciar aplicativos de micros serviços ou equivalentes, de forma escalável.

**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.

**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.

**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 .

**Instância de Computação:** componente de computação em nuvem composto de máquina virtual e serviços agregados.

**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 .

**Licença de software:** documento que fornece diretrizes legalmente vinculantes para o uso e a distribuição de determinado software.

**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.

**Licença por subscrição/assinatura:** permite aos usuários acessarem o software por meio de serviços online, em vez de adquirir uma licença de uso único.

**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.

**Manutenção de software (correção de erros):** é o processo de fornecer suporte técnico, atualizações e melhorias para um determinado software.

**Marketplace:** loja virtual operada por um provedor de nuvem que oferece acesso a software e serviços que são

desenvolvidos, se integram ou complementam as soluções disponibilizadas pelo provedor de nuvem.

**Modelos de implantação de nuvem:** representam como a computação em nuvem pode ser organizada, com base no controle e no compartilhamento de recursos físicos ou virtuais<sup>21</sup>. Incluem: nuvem pública, nuvem privada, nuvem comunitária e nuvem híbrida.

**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.

**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.

**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.

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

**Nuvem:** recursos computacionais que podem ser utilizados de forma automatizada, dinâmica e sob demanda, disponibilizados através de grandes servidores compartilhados e interligados por meio da Internet, possibilitando o acesso de qualquer lugar a qualquer hora.

**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.

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

**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.

**Nuvem privada ou interna:** infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas.

**Nuvem pública ou externa:** infraestrutura de nuvem dedicada para uso aberto de qualquer organização.

**Orquestração:** habilidade de coordenar e gerenciar recursos em diferentes provedores de nuvem públicas.

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

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

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

**Relatório de impacto à proteção de dados pessoais (RIPD):** documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

**Responsável pelo serviço:** servidor responsável pela operação de serviços ou equipamentos da área de TI, bem como pela realização dos testes de restore.

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

**Serviços agregados:** são serviços adicionais providos pelo fornecedor da solução que oferecem aos usuários acesso a recursos adicionais relacionados ao objeto principal.

**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.

**Software livre:** tipo de software de código aberto que pode ser usado, estudado, modificado e redistribuído gratuitamente.

**Software open source (ou de código aberto):** tipo de software de código aberto que pode ser usado, estudado, modificado e redistribuído gratuitamente.

**Software pronto para uso:** software disponibilizado (pago ou não) com um conjunto de funcionalidades pré-concebidas.

**Suporte técnico:** serviço provido pelo fornecedor para auxiliar os usuários com problemas relacionados ao serviço contratado.

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

**Recursos reservados:** são aqueles recursos tecnológicos que possuem planos pré-definidos de consumo por determinado período mediante a aplicação de desconto.

**Usuários:** pessoas que fazem uso de recursos, serviços e sistemas de informação disponibilizados pela área de TI.

## **CAPÍTULO IV**

### **DOS PRINCÍPIOS**

**Art. 6º** Os princípios norteadores são:

- I. Conformidade com a legislação e normativas institucionais;
- II. Garantia de integridade, autenticidade, confidencialidade e disponibilidade das informações;
- III. Alinhamento com políticas e planos institucionais;
- IV. Promoção da cultura de segurança da informação;
- V. Adoção do uso de serviços de computação em nuvem na implementação de soluções tecnológicas, sempre que possível e viável, antes de considerar alternativas tradicionais (Cloud-First) ;
- VI. Migrar aplicações legadas para a nuvem sem redesenho, reescrita ou reengenharia, mantendo a lógica, a configuração e os componentes praticamente inalterados, somente como último recurso (Lift and Shift);
- VII. Preferência pelo uso de função, serviço ou arquitetura intermediária cuja responsabilidade é intermediar, gerenciar, integrar e orquestrar o uso de múltiplos provedores de serviços em nuvem, de maneira unificada e estratégica. (Broker multicloud);

## **CAPÍTULO V**

### **DAS DIRETRIZES GERAIS**

**Art. 7º** Ao contratar serviços em nuvem, o IFMA deverá:

- a. Garantir a aderência à legislação vigente;
- b. Assegurar que os contratos incluam cláusulas específicas sobre segurança da informação;
- c. Avaliar previamente as informações a serem armazenadas em nuvem.

## **CAPÍTULO VI**

### **DA IDENTIFICAÇÃO DAS NECESSIDADES DO NEGÓCIO**

**Art. 8º** O IFMA deverá 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.

## **CAPÍTULO VII**

### **DA SELEÇÃO DOS MODELOS ADEQUADOS**

**Art. 9º** O IFMA 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.

§1º Caso as unidades do IFMA não possuam maturidade suficiente na contratação de serviços em nuvem ou possuam impedimentos técnicos ou normativos para migração de alguns workloads, é recomendável sempre dar preferência à adoção de uma abordagem estratégica de nuvem híbrida.

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

## **CAPÍTULO VIII**

### **DA AVALIAÇÃO DOS FORNECEDORES**

**Art. 10º** 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.

**Parágrafo único:** Fatores como segurança, conformidade, disponibilidade e suporte técnico devem ser considerados nessa avaliação.

## **CAPÍTULO IX**

### **DOS REQUISITOS DE SEGURANÇA**

**Art. 11º** Deverão ser definidos claramente os requisitos de segurança mandatórios, com avaliação constante da capacidade dos fornecedores em atendê-los.

## **CAPÍTULO X**

### **DA POLÍTICA DE GOVERNANÇA**

**Art. 12º** A política de governança do IFMA 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 IFMA.

**Art. 13º** Esta estratégia deve estar alinhada com os seguintes planos estratégicos e políticas do IFMA:

- a. Plano de Desenvolvimento Institucional (PDI);
- b. Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC);
- c. Plano de Contratações Anual (PCA);
- d. Política de Segurança da Informação e Comunicação (Posic).

## **CAPÍTULO XI**

### **DO USO SEGURO DA COMPUTAÇÃO EM NUVEM**

**Art. 14º** O IFMA 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 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.

## **CAPÍTULO XII**

### **DA INFRAESTRUTURA DE TIC**

**Art. 15º** O IFMA deverá assegurar infraestrutura adequada de conectividade e estabilidade para uso efetivo dos serviços em nuvem.

## **CAPÍTULO XIII**

### **DA CAPACITAÇÃO DA EQUIPE**

**Art. 16º** O IFMA deverá promover capacitação constante dos servidores responsáveis pela gestão e operação dos serviços em nuvem.

## **CAPÍTULO XIV**

## DOS REQUISITOS REGULATÓRIOS E ESTRATÉGIA DE SAÍDA

**Art. 17º** O IFMA deverá observar requisitos regulatórios e definir claramente estratégias de saída dos serviços contratados em nuvem.

### CAPÍTULO XV

#### DO GERENCIAMENTO DE RISCOS

**Art. 18º** O IFMA deverá realizar periodicamente a análise e o gerenciamento dos riscos relacionados à computação em nuvem, incluindo relatórios de impacto de dados pessoais.

### CAPÍTULO XVI

#### DA UTILIZAÇÃO DE CLOUD BROKERS

**Art. 19º** O cloud broker deverá atuar como integrador dos serviços de computação em nuvem entre o IFMA e dois ou mais provedores de serviço de nuvem.

**Art. 20º** O cloud broker é o responsável por garantir que os provedores de serviço de nuvem que ele representa cumpram todos os requisitos previstos nesta normativa e na legislação brasileira e operem de acordo com as melhores práticas de segurança.

**Parágrafo único:** O IFMA deverá prever no instrumento contratual que o cloud broker poderá ser responsabilizado, civil e administrativamente, por qualquer desconformidade nos provedores que ele representa .

### CAPÍTULO XVII

#### DAS RESPONSABILIDADES

##### Seção I

##### Da Alta Administração

**Art. 21º** Cabe à Alta Administração aprovar e divulgar esta normativa e disponibilizar os recursos necessários para sua execução.

##### Seção II

##### Do Comitê de Segurança da Informação

**Art. 22º** Ao Comitê de Segurança da Informação cabe :

- a. Aprovar estratégias, analisar revisões da normativa e tratar casos omissos.
- b. Supervisionar a aplicação desta normativa;
- c. Assegurar a contínua efetividade da comunicação com o provedor de serviço de nuvem;
- d. Supervisionar a aplicação das medidas de correção pelo provedor de serviço de nuvem, em casos de eventuais desvios;
- e. Comunicar incidentes cibernéticos informados pelo provedor de serviço de nuvem aos órgãos competentes;
- f. Encaminhar para aprovação da alta administração as minutas de elaboração e de revisões desta normativa;
- g. 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.

##### Seção III

##### Da Diretoria de Gestão de Tecnologia da Informação (DIGTI)

**Art. 23º** Compete à Diretoria de Gestão de Tecnologia da Informação:

- a. Planejar, contratar, gerenciar e operar os serviços em nuvem.
- b. Ser responsável por planejar, contratar, gerenciar e operar os serviços de nuvem.
- c. Implementar os procedimentos relativos ao uso de tecnologias de computação em nuvem em conformidade com as orientações contidas nesta normativa e legislação pertinente.

### CAPÍTULO XVIII

## DA REVISÃO E ATUALIZAÇÃO

**Art. 24°** Esta normativa 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 IFMA, quando considerada necessária pelo Comitê de Segurança da Informação.

**Art. 25°** 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 normativa deve ser revisada periodicamente, não excedendo 2 (dois) anos para:

- a. Definir novos critérios e a periodicidade das atualizações dos procedimentos e dos recursos computacionais a serem observados pelo provedor de serviço de nuvem;
- b. Atualizar periodicamente os processos internos de gestão de riscos de segurança da informação;
- c. Quando ocorrerem eventos, fatores relevantes, novos requisitos tecnológicos, corporativos e/ ou legais que exijam sua revisão imediata;
- d. 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.

## CAPÍTULO X

### DAS DISPOSIÇÕES FINAIS

**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°** A apresentação dos relatórios de tipo I e tipo II da auditoria SOC 2, comprovada a conformidade com os padrões de segurança em nuvem, é condição essencial, tanto para habilitar a participação em processo licitatório, como para renovar o contrato de prestação de serviço em nuvem com o IFMA.

**Art. 28°** Esta normativa e seus documentos complementares devem ser divulgados a todos os usuários e partes interessadas a fim de promover sua observância e conhecimento.

**Art. 29°** A alta administração deve disponibilizar os recursos (humanos, tecnológicos e financeiros) necessários para a execução desta normativa.

**Art. 30°** Os casos omissos não abordados neste documento serão analisados pelo Comitê de Segurança da Informação.

**Art. 31°** O IFMA adotará o foro brasileiro para dirimir quaisquer questões jurídicas relacionadas aos contratos firmados entre o contratante e o fornecedor do serviço.

**Art. 32°** Esta norma entra em vigor a partir da data de sua publicação.

*(assinado eletronicamente)*

**CARLOS CESAR TEIXEIRA FERREIRA**

Presidente do Comitê de Governança Digital

Documento assinado eletronicamente por:

- **Carlos Cesar Teixeira Ferreira, REITOR(A) - CD1 - GAB-REIT**, em 09/05/2025 18:05:31.

Este documento foi emitido pelo SUAP em 09/05/2025. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse <https://suap.ifma.edu.br/autenticar-documento/> e forneça os dados abaixo:

**Código Verificador:** 1050630

**Código de Autenticação:** d7efa9b053

