Ministério da Educação
Universidade Federal de Alfenas
Rua Gabriel Monteiro da Silva, 700 - Bairro centro, Alfenas/MG - CEP 37130-001
Telefone: (35) 3701-9000 - http://www.unifal-mg.edu.br

Resolução Nº 03/2024, DE 05 de novembro de 2024

Aprova as normas que estabelecem a Estratégia de Uso de Software e de Serviços de Computação em Nuvem e a Política de Uso Seguro de Computação em Nuvem para a Universidade Federal de Alfenas (UNIFAL-MG).

O Comitê de Governança Digital (CGD) da Universidade Federal de Alfenas – UNIFAL-MG, no uso de suas atribuições regimentais,

CONSIDERANDO o constante dos autos do processo nº 23087.017684/2024-57,

R E S O L V E :

Art. 1º Aprovar, na forma do anexo SEI Nº 1386334, a norma que estabelece a Estratégia de Uso de Software e de Serviços de Computação em Nuvem;

Art. 2º Aprovar, na forma do anexo SEI Nº 1386336, a norma de Política de Uso Seguro de Computação em Nuvem para a Universidade Federal de Alfenas (UNIFAL-MG);

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

Assinado Eletronicamente

SANDRO AMADEU CERVEIRA

Presidente do Comitê de Governança Digital

POLÍTICA DE USO SEGURO DE COMPUTAÇÃO EM NUVEM

CAPÍTULO I DO ESCOPO

Art. 1° A normativa sobre uso seguro da computação em nuvem tem a finalidade de estabelecer um conjunto de princípios, diretrizes e responsabilidades que visam garantir a segurança da informação no uso de softwares e serviços de computação em nuvem no âmbito da UNIFAL-MG.

Art. 2° Esta normativa visa garantir que os dados críticos estejam disponíveis e protegidos contra perdas, falhas de hardware, desastres naturais e ameaças cibernéticas.

Art. 3° As diretrizes estabelecidas neste documento se aplicam a todos os dados tratados em sistemas de informação, aplicações e serviços de Tecnologia da Informação em um serviço de nuvem computacional.

Art. 4° As determinações desta normativa aplicam-se a novas contratações de softwares e serviços em computação em nuvem realizadas a partir da data de publicação desta normativa e novos contratos com provedores de serviço de nuvem computacional.

Art. 5° Para garantir o nível de segurança da informação, privacidade e proteção de dados pessoais determinados pela legislação vigente são definidos os seguintes objetivos para esta normativa:

I. observar os requisitos da legislação competente para elevar o nível de proteção das informações no uso de softwares e serviços em nuvem computacional;
II. definir medidas que deverão ser observadas pelos servidores vinculados à UNIFAL-MG e por organizações fornecedoras de computação em nuvem; e
III. proteger informações de acesso não autorizado e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado, ou ilícito e considerar a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, assim como os princípios previstos em legislação pertinente.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 6° Para fins de compreensão dos termos utilizados neste documento serão utilizados os seguintes conceitos e definições:

I. agente responsável: servidor público ocupante de cargo efetivo incumbido de implementar procedimentos relativos ao uso seguro de tecnologias de computação em nuvem;
II. 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;
III. nuvem: recursos computacionais que podem ser utilizados de forma automatizada, dinâmica e sob demanda, disponibilizados por grandes servidores compartilhados e interligados por meio da Internet, possibilitando o acesso de qualquer lugar a qualquer hora;
IV. nuvem privada: infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos usuários, e

sua propriedade e seu gerenciamento podem ser da própria organização, de terceiros ou de ambos;

V. nuvem pública (ou externa): infraestrutura de nuvem dedicada para uso aberto de qualquer organização, e sua propriedade e seu gerenciamento podem ser de organizações públicas, privadas ou de ambas;

VI. 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.

VII. 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;

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

IX. usuários: pessoas que fazem uso de recursos, serviços e sistemas de informação disponibilizados pela área de TI;

X. broker: intermediário que facilita a gestão, integração e otimização de serviços de diferentes provedores de nuvem para uma empresa ou usuário, oferecendo uma camada adicional de controle e simplificação no uso de múltiplas plataformas de nuvem.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 7° A UNIFAL-MG deve observar, no mínimo, os seguintes princípios antes de adotar a tecnologia de computação em nuvem:

I. alinhamento com a Política de Segurança da Informação e suas normas internas complementares;

II. alinhamento com os planos institucionais;

III. alinhamento com as diretrizes do processo de gestão de continuidade de negócios;

IV. alinhamento com as diretrizes do processo de gestão de riscos de segurança da informação; e

V. alinhamento com a estratégia de uso de software e de serviços de computação em nuvem.

CAPÍTULO IV
DAS DIRETRIZES GERAIS

Art. 8° A UNIFAL-MG ao contratar ou implementar soluções de computação em nuvem, deve garantir que:

I. o ambiente de computação em nuvem, sua infraestrutura e canal de comunicação estejam aderentes às diretrizes das políticas e normas internas complementares de segurança da informação utilizadas pela UNIFAL-MG e à legislação vigente no âmbito da administração pública federal;

II. o contrato de prestação de serviço, quando for o caso, deve conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem computacional, em especial aquelas sob custódia e gerenciamento do prestador de serviço;

III. a UNIFAL-MG deve avaliar quais informações serão hospedadas na nuvem computacional, considerando:

A. o processo de classificação da informação segundo a legislação vigente;

B. o valor do ativo de informação;
C. os controles de acesso, físicos e lógicos, relativos à Segurança da Informação;
D. o modelo de serviço e de implementação de computação em nuvem a serem adotados; e
E. a localização geográfica onde as informações estarão fisicamente armazenadas.

Art. 9° Antes de transferir serviços ou informações para um provedor de serviço de computação em nuvem, a UNIFAL-MG deverá, no mínimo:

I. efetuar verificação de que o provedor de serviços esteja conforme a legislação brasileira e aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros as seguintes operações:
   A. de coleta, armazenamento, guarda e tratamento de registros de dados pessoais; e
   B. de comunicações realizada por provedores de conexão e de aplicações de internet, em que pelo menos um desses atos ocorra em território nacional quando aplicável;
II. realizar o gerenciamento de riscos, precedido por análise e relatório de impacto de dados pessoais, conforme a legislação, dos seguintes itens:
   A. o tipo de informação a ser migrada;
   B. o fluxo de tratamento dos dados que podem ser afetados com a adoção da solução;
   C. o valor dos ativos envolvidos; e
   D. os benefícios da adoção de uma solução de computação em nuvem em relação aos riscos de segurança e privacidade referentes à disponibilização de informações e serviços a um terceiro;
III. definir o modelo de serviço e de implementação de computação em nuvem que será adotado;
IV. avaliar quais informações serão hospedadas na nuvem, considerando:
   A. o processo de classificação da informação conforme a legislação;
   B. o valor do ativo de informação;
   C. os controles de acessos físico e lógico relativos à segurança da informação; e
   D. definir as medidas de mitigação de riscos e de custos para a implementação de solução de computação em nuvem e para possibilidade de crescimento dessa solução; e
   E. planejar custos de migração das informações e dos serviços, nos casos de ingresso e de saída do serviço de computação em nuvem.

Art. 10. Em função da capacidade de o provedor de serviço de computação em nuvem implementar atualizações relacionadas à segurança da informação em seus produtos e serviços, a UNIFAL-MG deverá, no mínimo:

I. definir os critérios e a periodicidade das atualizações dos procedimentos e dos recursos computacionais a serem observados pelo provedor de serviço de nuvem; e
II. revisar e atualizar sempre que necessário seus processos internos de gestão de riscos de segurança da informação.

Art. 11. O gerenciamento de identidades e de registros de logs deve seguir as políticas vigentes na UNIFAL-MG.

Art. 12. Em relação à necessidade do uso de recursos criptográficos, a UNIFAL-MG deverá:

I. verificar se os dados da organização estão sendo tratados e armazenados conforme a legislação;
II. analisar a necessidade de criptografar dados com base nos requisitos legais, nos riscos, no nível de criticidade, nos custos e nos benefícios.

Art. 13. Em relação ao gerenciamento da nuvem, a UNIFAL-MG deverá, no mínimo:
I. capacitar a equipe responsável por esse gerenciamento nas tecnologias utilizadas pelo provedor de serviço de nuvem;
II. exigir que o provedor de serviço de nuvem documente e comunique seus recursos, papeis e responsabilidades de segurança da informação para o uso de seus serviços em nuvem;
III. elaborar uma matriz de responsabilidades que inclua obrigações e responsabilidades próprias; e
IV. elaborar um processo de tratamento de incidentes junto ao provedor de serviço de nuvem e comunicá-lo à equipe responsável pelo gerenciamento da nuvem.

Art. 14. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pela UNIFAL-MG, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro sempre que for legalmente exigido.

Parágrafo Único: A UNIFAL-MG, mediante justificativa, poderá estabelecer normas internas específicas que determinem a obrigatoriedade de hospedagem de determinados tipos de dados exclusivamente em território nacional.

Art. 15. O instrumento contratual a ser firmado com um provedor de serviço de nuvem para a prestação do serviço de computação em nuvem deve conter dispositivos que tratem dos requisitos estabelecidos nesta normativa e, no mínimo, os seguintes procedimentos de segurança:
I. termo de confidencialidade que impeça o provedor de serviço de nuvem de usar, transferir e liberar dados, sistemas, processos e informações do órgão ou da entidade para empresas nacionais, transnacionais, estrangeiras, países e governos estrangeiros;
II. garantia da exclusividade de direitos, por parte da UNIFAL-MG, sobre todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, tais como backups de segurança;
III. proibição do uso de informações da UNIFAL-MG pelo provedor de serviço de nuvem para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado;
IV. conformidade da política de segurança da informação do provedor de serviço de nuvem com a legislação brasileira;
V. devolução integral dos dados, informações e sistemas sob custódia do provedor de serviço de nuvem a UNIFAL-MG ao término do contrato;
VI. eliminação, por parte do provedor de serviço de nuvem, ao término do contrato, de qualquer dado, informação ou sistema da UNIFAL-MG sob sua custódia, observada a legislação que trata da obrigatoriedade de retenção de dados; e
VII. garantia do direito ao esquecimento para dados pessoais, conforme art. 16 da Lei nº 13.709, de 14 de agosto de 2018, LGPD.

Art. 16. Nas contratações de serviços em nuvem (IaaS, PaaS e SaaS) devem ser observados, no mínimo, além dos requisitos legais aplicáveis, os seguintes requisitos de privacidade e segurança da informação:
I. o provedor de nuvem deve possuir deve cumprir os requisitos de segurança da informação estabelecidos nos artigos 20 e 25 da Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021;
II. deve-se exigir, mediante justificativa prévia, que os provedores de serviços em

nuvem possuam, no momento da assinatura do contrato, certificações de normas de segurança da informação aplicáveis ao objeto da contratação, assim como outros requisitos que objetivem mitigar riscos relativos à segurança da informação;

III. devem ser predefinidos canais para comunicação, de maneira rápida e eficiente e, conforme os requisitos legais, regulatórios e contratuais, de eventos de segurança da informação;

IV. o contrato entre a UNIFAL-MG e o provedor/*broker* deve estabelecer direitos claros e exclusivos de propriedade do órgão ou da entidade contratante sobre todos os dados, informações e códigos tratados decorrentes do contrato, incluídas eventuais cópias, cópias de segurança, logs, além do acesso aos dados;

V. logs de auditoria do provedor, que registrem atividades de acesso de usuários privilegiados, tentativas de acessos autorizados e não autorizados, exceções do sistema e eventos de segurança da informação, devem ser mantidos conforme as políticas e regulamentos aplicáveis, e devem estar de acordo com as políticas do cliente;

VI. deve-se prever cópia dos logs fornecidos pelo provedor, conforme a política de retenção da UNIFAL-MG;

VII. deve-se implementar controle de acesso lógico apropriado ao grau de confidencialidade dos dados armazenados na nuvem e controles para transferência de dados;

VIII. o provedor deve garantir controles eficazes e compatíveis com as políticas e procedimentos da UNIFAL-MG para gerenciamento de identidades de usuários e controle de acessos;

IX. devem ser estabelecidas políticas e procedimentos para o uso de criptografia, incluindo gerenciamento de chaves criptográficas, que devem ser seguidos pela UNIFAL-MG e pelo provedor;

X. devem ser estabelecidos os limites do acesso do provedor aos dados da UNIFAL-MG e a responsabilidade do provedor em garantir o isolamento de recursos e dados contra acesso indevido por outros clientes;

XI. devem ser definidos os países e as regiões em cada país onde os serviços poderão ser prestados e onde os dados poderão ser armazenados, processados e gerenciados, tendo o provedor que assegurar que dados sujeitos a limites geográficos não sejam migrados para além de fronteiras definidas em contrato;

XII. a utilização de termo de confidencialidade, que deverá conter cláusula que impeça o integrador ou provedor de serviço de nuvem de usar, transferir e liberar dados, sistemas, processos e informações da UNIFAL-MG para terceiros, como: empresas nacionais, transnacionais, estrangeiras, países e governos estrangeiros, além de incluir a proibição do uso de informações da UNIFAL-MG para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não autorizado;

XIII. deve-se avaliar a previsão de mecanismos de proteção de aplicações e de proteção de vulnerabilidade de código;

XIV. deve-se exigir que o *cloud broker* disponibilize uma estrutura exclusiva de contas nos provedores de nuvem em nome da UNIFAL-MG, por meio das quais os serviços serão provisionados; e

XV. deve-se prever responsabilidade por parte do *cloud broker* para as atividades de migração de contas entre *cloud brokers* ou outras ações necessárias à prestação e à continuidade dos serviços.

CAPÍTULO VI
DOS REQUISITOS DO PROVEDOR DE SERVIÇO DE NUVEM

Art. 17. Para estar habilitado a prestar serviços de computação em nuvem para a UNIFAL-MG, o provedor de serviço de nuvem deverá cumprir, no mínimo, os

seguintes requisitos:

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

II. implementar práticas de fortalecimento dos mecanismos de virtualização, que devem incluir, no mínimo, os seguintes procedimentos:
   A. desabilitar ou remover todas as interfaces, portas, dispositivos ou serviços desnecessários executados pelo sistema operacional;
   B. configurar com segurança todas as interfaces de rede e áreas de armazenamento virtuais;
   C. estabelecer limites para a utilização dos recursos de máquina virtual (Virtual Machine VM);
   D. manter todos os sistemas operacionais e as aplicações em execução na máquina virtual em suas versões mais atuais;
   E. possuir controles que permitam aos usuários autorizados da UNIFAL-MG acessarem os registros de acesso administrativo do monitor de máquina virtual;
   F. suportar o uso de máquinas virtuais confiáveis (Trusted VM) fornecidas pela UNIFAL-MG, que estejam conforme as políticas e práticas de fortalecimento de redes exigidas ao provedor de serviço de nuvem.

III. em relação ao gerenciamento de identidades e registros:
   A. possuir procedimentos de controle de acesso que abordem a transição entre as funções, os limites e controles dos privilégios dos usuários e os controles de utilização das contas de usuários;
   B. impor mecanismo de autenticação que exija tamanho mínimo, complexidade, duração e histórico de senhas de acesso;
   C. suportar tecnologia single sign-on para autenticação;
   D. suportar mecanismos de autenticação multi-fator ou outra alternativa que aumente o grau de segurança no processo de autenticação de usuários;
   E. permitir que a UNIFAL-MG gerencie as suas credenciais de acesso ao ambiente de gerenciamento fornecido pelo provedor de serviço de nuvem, incluindo a criação, atualização, exclusão e suspensão de credenciais; e
   F. atender aos requisitos legais, às melhores práticas de segurança e a outros critérios exigidos pela UNIFAL-MG em seus processos de autenticação, controle de acesso, contabilidade e de registro (formato, retenção e acesso).

IV. em relação à segurança de aplicações web disponibilizadas no ambiente de nuvem:
   A. utilizar firewalls especializados na proteção de sistemas e aplicações;
   B. desenvolver código web conforme as melhores práticas de desenvolvimento seguro e com os normativos existentes;
   C. utilizar melhores práticas de segurança de sistemas operacionais e de aplicações;
   D. realizar periodicamente testes de penetração de redes e de aplicações;
   E. possuir um programa de correção de vulnerabilidades;

V. possuir processos de gestão de continuidade de negócios e de gestão de mudanças, conforme os normativos existentes e com as melhores práticas;

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

VII. estabelecer um canal de comunicação seguro utilizando, no mínimo, Secure Sockets Layer/Transport Layer Security (SSL/TLS);

VIII. utilizar um padrão de encriptação seguro, conforme padrão internacional reconhecidamente aceito, que possa ser implementado com chaves de encriptação geradas e armazenadas pela UNIFAL-MG;

IX. disponibilizar facilidades que possibilitem a aplicação de uma proteção

criptográfica própria da UNIFAL-MG.

X. em relação à segregação de dados:
   A. isolar, utilizando separação lógica, todos os dados e serviços da UNIFAL-MG de outros clientes de serviço em nuvem;
   B. segregar o tráfego de gerenciamento do tráfego de dados da UNIFAL-MG; e
   C. implementar dispositivos de segurança entre zonas.

XI. possuir procedimentos em relação ao descarte de ativos de informação e de dados, que assegurem:
   A. sanitizar ou destruir, de modo seguro, os dados existentes nos dispositivos descartados por meio da utilização de métodos que estejam conforme os padrões estabelecidos para a conduta e as melhores práticas;
   B. destruir, de modo seguro, ativo de informação no fim do ciclo de vida ou considerado inservível, com o fornecimento de um Certificado de Destruição de Equipamento Eletrônico (Certificate of Electronic Equipment Destruction CEED) e discriminar os ativos reciclados, bem como o peso e os tipos de materiais obtidos em virtude do processo de destruição; e
   C. armazenar, de modo seguro, ativos de informação a serem descartados, em ambiente com acesso físico controlado, com registro de toda movimentação de entrada e de saída de dispositivos.

XII. notificar, imediatamente, a UNIFAL-MG sobre quaisquer incidentes de segurança da informação e comunicação ocorridos contra os serviços ou dados sob sua custódia;

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

XIV. demonstrar estar em conformidade com os padrões de segurança de nuvem, por meio de auditoria anual Service and Organization Controls 2 (SOC 2), conduzida por um auditor independente, com a apresentação dos relatórios de tipo I e tipo II.

CAPÍTULO VII
DA UTILIZAÇÃO DE CLOUD BROKERS

Art. 18. O *cloud broker* deverá atuar como integrador dos serviços de computação em nuvem entre a UNIFAL-MG e dois ou mais provedores de serviço de nuvem.

Art. 19. Caso a UNIFAL-MG contrate, por meio do *cloud broker*, plataforma de gestão multi nuvem para realizar procedimentos de provisionamento e orquestração do ambiente, é necessário que a ferramenta possua, no mínimo:

I. em relação às funcionalidades de provisionamento e orquestração de multi-nuvem:
   A. um único portal integrado de provisionamentos;
   B. utilização de modelos de provisionamento;
   C. automação segura de provisionamento simultâneo e utilização, no que couber, de ferramentas de código aberto e interoperáveis;
   D. fluxos de trabalho de orquestração baseada em eventos; e
   E. soluções seguras integradas de criação de infraestrutura por código IaaC;

II. em relação às funcionalidades de monitoramento e análise em multi-nuvem:
   A. relatórios de monitoramento de desempenho de recursos na nuvem;
   B. coleta e monitoramento de registros; e
   C. procedimentos de monitoramento de alertas.

III. em relação às funcionalidades de inventário e classificação em multi-nuvem:
   A. inventário de recursos na nuvem;

B. procedimentos de segurança para configuração de recursos na plataforma de gestão multi-nuvem; e
C. detecção de recursos sem etiqueta.

IV. em relação às funcionalidades de gerenciamento de segurança, conformidade e identidade:
A. mecanismos de single sign-on e de autenticação multi-fator das plataformas em nuvem;
B. gerenciamento seguro de usuários e de grupos de usuários;
C. gerenciamento de segurança dos recursos;
D. notificações de eventos de alerta multicanal;
E. gerenciamento de identidade e acesso IAM; e
F. registros de atividade da plataforma em nuvem.

V. Parágrafo único: O *cloud broker* poderá utilizar ferramentas de Software as a Service (SaaS) comum de mercado, desde que não haja risco de dependência tecnológica para disponibilizar essa plataforma.

Art. 20. O *cloud broker* é o responsável por garantir que os provedores de serviço de nuvem que ele representa:

I. cumpram todos os requisitos previstos nesta normativa e na legislação brasileira; e
II. operem conforme as melhores práticas de segurança.

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

CAPÍTULO VIII
DAS RESPONSABILIDADES

Art. 21. Compete à alta administração da UNIFAL-MG:

I. assegurar a utilização de tecnologias de computação em nuvem conforme as orientações contidas neste documento; e
II. disponibilizar recursos (humanos, tecnológicos e financeiros) para a implementação desta normativa.

Art. 22. Compete ao Comitê de Governança Digital:

I. aprovar as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de computação em nuvem e divulgá-las às partes interessadas.
II. estabelecer os países nos quais dados e informações custodiados pela UNIFAL-MG poderão ser armazenados em soluções de computação em nuvem, quando necessário.
III. avaliar e aprovar, com justificativa, a contratação de serviço de nuvem, em especial do tipo “contrato de adesão”, que não cumpra integralmente com o estabelecido na presente normativa.

CAPÍTULO X
DAS DISPOSIÇÕES FINAIS

Art. 23. Esta normativa bem como os documentos gerados a partir dela poderão ser revisados a qualquer tempo pelo CGD, quando houver mudanças significativas nos requisitos de segurança da informação que influenciem no uso seguro de

computação em nuvem, para assegurar sua continuidade, sustentabilidade, adequação e efetividade. Deverão ser revisados, aprovados e atualizados em função de alterações na legislação pertinente, de diretrizes políticas do governo federal, de alterações nas políticas e normas da UNIFAL-MG ou quando considerado necessário pelo Núcleo de Tecnologia de Informação.

Art. 24. A UNIFAL-MG adotará, preferencialmente e, sempre que possível, o foro brasileiro para dirimir quaisquer questões jurídicas relacionadas aos contratos firmados entre o contratante e o fornecedor do serviço.

Art. 25. Os casos omissos serão analisados pelo Comitê de Governança Digital.

Art. 26. Esta normativa entra em vigor a partir da data de sua publicação.

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

Art. 1° A estratégia de uso de software e de serviços de computação em nuvem tem o objetivo de assegurar que a UNIFAL-MG obtenha os resultados esperados e mitigue os riscos associados à adoção de possíveis novas tecnologias ou novas formas de contratação no âmbito da UNIFAL-MG.

Art. 2° Esta estratégia deve ser aplicada para novas contratações de serviços de computação em nuvem no âmbito da UNIFAL-MG, nos seguintes tipos de contratação:
I - Infraestrutura como Serviço (IaaS);
II - Plataforma como Serviço (PaaS);
III - suporte técnico para software e serviços de computação em nuvem;
IV - serviço de operação e gerenciamento de recursos em nuvem;
V - serviço de migração de recursos para ambiente de nuvem;
VI - integração de serviços de computação em nuvem; e
VII - consultoria especializada em software e/ou serviços de computação em nuvem.

Art. 3° A estratégia tem como objetivos principais:
I - Promover a modernização dos serviços de TI da UNIFAL-MG através da adoção de soluções em nuvem;
II - Garantir a segurança, privacidade e conformidade das operações na nuvem;
III - Otimizar custos e recursos, promovendo a eficiência operacional;
IV - Fomentar a inovação e a transformação digital dentro da instituição;

Art. 4° Esta estratégia segue os seguintes princípios:
I - respeito aos princípios e diretrizes constitucionais, legais e regulamentares que regem a administração pública federal;
II - garantia de integridade, autenticidade e disponibilidade da informação sob a custódia da UNIFAL-MG, com respeito ao princípio da transparência e atribuição de confidencialidade apenas nos casos expressamente previstos na legislação;
III - alinhamento estratégico da Política de Segurança da Informação com os demais planos institucionais;
IV - responsabilidade pelo cumprimento das normas pertinentes à segurança da informação vigentes; e

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

Art. 5° A adoção de soluções em nuvem na UNIFAL-MG deverá ser baseada na identificação clara das necessidades institucionais, alinhando-se às prioridades estratégicas estabelecidas no Plano de Desenvolvimento Institucional (PDI) e no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC). O Núcleo de Tecnologia de Informação (NTI) será responsável por sugerir quais sistemas, aplicações, dados e serviços devem ser migrados para a nuvem, determinando também como esses recursos serão acessados e quais capacidades computacionais e de armazenamento serão necessárias. Cabe ao Comitê Gestor de Desenvolvimento (CGD) definir os serviços críticos prioritários para migração, além de avaliar o custo-benefício de cada serviço, com base no Estudo Técnico Preliminar apresentado pelo NTI.

Art. 6° Com base nas necessidades identificadas, a UNIFAL-MG selecionará os modelos de serviços em nuvem mais adequados, avaliando quanto à sua capacidade de atender aos requisitos de desempenho, segurança, conformidade e custo-benefício:
I - SaaS (Software as a Service): Para soluções de software prontas, que possam substituir ou complementar sistemas legados com menores esforços de implementação.
II - PaaS (Platform as a Service): Para o desenvolvimento e hospedagem de aplicações específicas, proporcionando maior controle e customização.
III - IaaS (Infrastructure as a Service): Para necessidades de infraestrutura, como armazenamento, rede e computação, permitindo a escalabilidade e flexibilidade dos recursos.
Parágrafo Único. Caso o NTI da UNIFAL-MG não possua maturidade suficiente na contratação de serviços em nuvem ou possua impedimentos técnicos ou normativos para migração de serviços, é recomendável sempre dar preferência à adoção de uma abordagem estratégica de nuvem híbrida.

Art. 7° A seleção dos fornecedores de serviços em nuvem será baseada em uma avaliação criteriosa que considerará:
I - Reputação e Confiabilidade: Histórico do fornecedor em termos de disponibilidade, tempo de resposta e suporte técnico.
II - Conformidade Legal e Regulatória: Adesão às normas brasileiras, incluindo a LGPD e outras regulamentações específicas do setor público.
III - Segurança e Privacidade: Garantias oferecidas pelo fornecedor em relação à proteção de dados, políticas de backup e recuperação, e gestão de incidentes.

IV - Flexibilidade e Escalabilidade: Capacidade de adaptar os serviços às necessidades variáveis da UNIFAL-MG, com opções de expansão ou redução de recursos.
V - Custos e Condições Contratuais: Análise do custo total de propriedade (TCO), incluindo taxas de serviços, custos ocultos, e cláusulas contratuais que afetam a longo prazo.

Art. 8° O NTI deve determinar através do Estudo Técnico Preliminar quais requisitos de segurança são importantes ou mandatórios para o negócio e deve ser avaliado, quando for o caso, como cada possível fabricante ou fornecedor atende a esses requisitos:
I - Criptografia de Dados: Todos os dados armazenados na nuvem deverão ser criptografados, tanto em repouso quanto em trânsito.
II - Autenticação Multi-Fator (MFA): Implementação de MFA para todas as contas que acessam recursos sensíveis.
III - Monitoramento e Logs de Atividades: Os serviços em nuvem deverão permitir a coleta e análise de logs detalhados para detecção de atividades suspeitas e auditorias.
IV - Conformidade com Padrões de Segurança: Exigir que os fornecedores estejam em conformidade com padrões reconhecidos.

Art. 9º Para assegurar o uso seguro e eficaz das soluções em nuvem, a governança do serviço deve abranger os seguintes aspectos:
I. Identificação e Classificação de Dados: A instituição deverá identificar e classificar os dados manipulados, determinando sua importância, sensibilidade e confidencialidade, a fim de estabelecer as medidas de segurança e proteção adequadas para cada categoria de dados.
II. Controle de Acesso: Serão estabelecidas regras rigorosas de controle de acesso, garantindo que apenas pessoas devidamente autorizadas tenham acesso aos dados e sistemas críticos, de modo a proteger as informações contra acessos não autorizados e violações de segurança.
III. Gerenciamento de Configuração: A UNIFAL-MG deverá monitorar e controlar as configurações dos sistemas e serviços em nuvem para assegurar que estejam em conformidade com as políticas e padrões de segurança da instituição, incluindo a manutenção das configurações sempre atualizadas e protegidas contra vulnerabilidades.
IV. Monitoramento das Atividades em Nuvem: Quando aplicável, será implementado um sistema de monitoramento contínuo das atividades realizadas em serviços de nuvem, a fim de garantir que estejam em conformidade com as políticas estabelecidas e permitir a detecção e resposta rápida a possíveis irregularidades ou violações.
V. Conformidade com Padrões: Todos os serviços em nuvem contratados pela instituição deverão ser executados em estrita conformidade com os padrões de segurança,

privacidade e operação definidos pela UNIFAL-MG, assegurando a integridade dos dados e a eficácia das operações.

Art. 10. Para garantir o uso seguro dos serviços de computação em nuvem, serão seguidas as seguintes diretrizes:
I - Educação e Treinamento: Todos os usuários e administradores dos serviços em nuvem deverão receber treinamento adequado sobre práticas seguras de uso.
II - Gestão de Identidades e Acessos (IAM): Controle rigoroso de acessos com base em perfis e necessidade de conhecimento, incluindo a aplicação de políticas de menor privilégio.
III - Gestão de Vulnerabilidades: Processos contínuos de identificação, avaliação e mitigação de vulnerabilidades nos serviços contratados.

Art. 11. Para adoção de serviços em nuvem, a infraestrutura de TIC da UNIFAL-MG deverá garantir que a capacidade de rede seja suficiente para suportar o tráfego adicional gerado pelo uso de serviços em nuvem, que as redes internas possuam mecanismos robustos de segurança para interagir com a nuvem de forma segura e que estejam disponíveis ferramentas adequadas para o gerenciamento e monitoramento dos serviços em nuvem.

Art. 12. A UNIFAL-MG 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.

Art. 13 A cada contratação, a UNIFAL-MG deve considerar a viabilidade de adoção de medidas para mitigar a dependência tecnológica ou aprisionamento ao provedor, devendo efetuar análise de dependências e aspectos de portabilidade (backup, redundância, contratos de apoio, retorno para a infraestrutura local etc.)

Art. 14. A UNIFAL-MG 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.

Art. 15. Os casos omissos serão analisados pelo Comitê de Governança Digital.

Art. 16. Esta norma entra em vigor a partir da data de sua publicação.