MINISTÉRIO DO MEIO AMBIENTE E MUDANÇA DO CLIMA

SUBSECRETARIA DE PLANEJAMENTO, ORÇAMENTO E ADMINISTRAÇÃO

MINUTA

NORMA OPERACIONAL Nº <XXX>/SPOA , DE XX DE MAIO DE 2025

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

Dispõe sobre a estratégia de uso de software e de serviços de computação em nuvem no âmbito do Ministério do Meio Ambiente e Mudança do Clima e define padrões, procedimentos e responsabilidades.

A GESTORA DE SEGURANÇA DA INFORMAÇÃO – GSIN DO MINISTÉRIO DO MEIO AMBIENTE E MUDANÇA DO CLIMA, no uso das competências que lhe confere PORTARIA GM/MMA Nº 510, DE 12 DE JUNHO DE 2023, e considerando a necessidade da definição da Estratégia de Uso de Software e de Serviços de Computação em Nuvem do MMA, com vista ao atendimento à Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023,

R E S O L V E :

Art. 1º Fica aprovado, na forma do Anexo Único desta Resolução, o Documento de Estratégia de Uso de Software e de Serviços de Computação em Nuvem do Ministério do Meio Ambiente e Mudança do Clima – MMA.

Art. 2º A área de TI do MMA 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 É autorizado o tratamento de dados em ambiente de nuvem pública para viabilizar a prestação de serviços públicos e a implementação de políticas públicas de competência do MMA.

Parágrafo único. No tratamento de informações em ambiente de nuvem pública deverão sempre ser observados os instrumentos legais, de governança e de segurança da informação presentes nesta Estratégia.

Art. 4º Esta Resolução entra em vigor na data de sua publicação.

ANA BEATRIZ DE OLIVEIRA

GESTORA DE SEGURANÇA DA INFORMAÇÃO – GSIN
SUBSECRETÁRIA DE PLANEJAMENTO, ORÇAMENTO E ADMINISTRAÇÃO

Documento assinado eletronicamente por **Jonas Jeske**, **Coordenador(a) - Geral**, em 16/05/2025, às 15:43, conforme horário oficial de Brasília, com fundamento no Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site http://sei.mma.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1976549** e o código CRC **BD71B39D**.

Referência: Processo nº 02000.005707/2025-02 SEI nº 1976549

MINISTÉRIO DO MEIO AMBIENTE E MUDANÇA DO CLIMA

SUBSECRETARIA DE PLANEJAMENTO, ORÇAMENTO E ADMINISTRAÇÃO

ANEXO ÚNICO

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

CAPÍTULO I

DO ESCOPO

Art. 1° Documento a respeito da **estratégia de uso de software e de serviços de computação em nuvem.**

Art. 2° O Documento tem o objetivo de assegurar que o MMA obtenha os resultados esperados e mitigue os riscos associados à adoção de possíveis novas tecnologias ou novas formas de contratação no âmbito do ministério.

Art. 3° Esta estratégia deve ser aplicada para novas contratações de software e de serviços de computação em nuvem no âmbito do MMA, tais como:

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

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

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

IV - Infraestrutura como Serviço (IaaS);

V - Plataforma como Serviço (PaaS);

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

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

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

IX - integração de serviços de computação em nuvem; e

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

CAPÍTULO II

DAS REFERÊNCIAS

Art. 4º Para o desenvolvimento da estratégia de uso de software e de serviços de computação em nuvem, cabe ao MMA observar, sem prejuízo das demais normas em vigor:

I - Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023 que estabelece modelo de contratação de software e de serviços de computação em nuvem, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

II - Instrução Normativa Nº 5, de 30 de agosto de 2021: dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;

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

IV - Resolução SE/GSI nº 1, de 11 de setembro de 2019, que aprova o Regimento Interno do Comitê Gestor de Segurança da Informação;

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

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

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

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

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

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

XI - Portaria GM/MMA Nº 510, DE 12 de junho de 2023, que institui a Política de Segurança da Informação - POSIN - no âmbito do Ministério do Meio Ambiente e Mudança do Clima; e

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

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 completado 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 (Tecnologia da Informação e Comunicações) 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 - 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;

VI - 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;

VII - 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;

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

IX - 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;

X - 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;

XI - 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;

XII - 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;

XIII - 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;

XIV - 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;

XV - Licença de software: documento que fornece diretrizes legalmente vinculantes para ouso 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;

XVI - 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;

XVII - 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;

XVIII - 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;

XIX - 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;

XX - 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;

XXI - 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;

XXII - 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;

XXIII - 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;

XXIV - 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;

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

XXVI - 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;

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

XXVIII - 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;

XXIX - 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;

XXX - 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;

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

XXXII - 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;

XXXIII - 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;

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

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

XXXVI - 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;

XXXVII - 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;

XXXVIII - 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;

XXXIX - 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;

XL - 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”;

XLI - 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;

XLII - 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;

XLIII - 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;

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

XLV - 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.

CAPÍTULO IV

DOS PRINCÍPIOS

Art. 6° Esta estratégia segue os seguintes princípios:

I - respeito aos princípios e diretrizes constitucionais, legais e regulamentares que regem a administração pública federal;

II - garantia de integridade, autenticidade e disponibilidade da informação sob a custódia do MMA, 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.

CAPÍTULO V

DAS DISPOSIÇÕES GERAIS

Art. 7° A apresentação dos relatórios de tipo I e tipo II da auditoria SOC 2, comprovada a conformidade com os padrões de segurança em nuvem, é condição essencial, tanto para habilitar a participação em processo licitatório, como para renovar o contrato de prestação de serviço em nuvem com órgãos ou entidades da administração pública federal.

§ 1º. Na hipótese de utilização de cloud broker, esse será o responsável por apresentar os relatórios de tipo I e tipo II da auditoria SOC 2 de todos os provedores de serviço de nuvem que ele representa.

§ 2º. Cabe ao MMA buscar a contratação prevista no caput desse artigo de forma a se habilitar para poder participar de qualquer processo licitatório que envolva a contratação de serviços em nuvem.

CAPÍTULO VI

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

Art. 8° Diretrizes deverão ser observadas pelo MMA ao adotar soluções de computação em nuvem de forma segura, com o objetivo de elevar o nível de proteção das informações no uso dessa tecnologia.

Seção I

Da identificação das necessidades do negócio

Art. 9° O MMA deve identificar e avaliar as necessidades de negócio antes da contratação de software e de serviços de computação em nuvem.

§ 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. 10 O MMA 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.

§Único. Como as unidades do MMA não possuem maturidade suficiente na contratação de serviços exclusivamente em nuvem ou possua impedimentos técnicos ou normativos para migração de alguns workloads, o MMA deve começar o seu processo de migração para a nuvem utilizando-se de uma abordagem estratégica de nuvem híbrida, aproveitando a estrutura e investimentos realizados ao longo dos anos em sua sala cofre e transferindo paulatinamente os serviços de nuvem com um planejamento aprovado pelo Comitê responsável.

Seção III

Da avaliação dos possíveis fornecedores

Art. 11 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.

§ 1º. Como o MMA não tem maturidade suficiente para adotar um processo de contratação exclusiva de fornecedores de serviço em nuvem, deve-se optar em participar de IRPs de outros órgãos que já possuam maior expertise no tema.

§ 2º. Fatores como segurança, conformidade, disponibilidade e suporte técnico devem ser considerados nessa avaliação, de forma a identificar se os patrocinadores da IRPs atentaram para esses fatores.

Seção IV

Da definição de requisitos de segurança

Art. 12 O MMA deve determinar quais requisitos de segurança são importantes ou mandatórios para o negócio e deve ser avaliado, quando for o caso, como cada possível fabricante ou fornecedor atende a esses requisitos.

§ Único. Os requisitos de segurança devem ser os mesmos, tanto em relação aos serviços “on Premises” (realizados internamente na sala cofre) como os eventualmente contratados de terceiros.

Seção V

Do estabelecimento de uma política de governança

Art. 13 A política de governança 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 MMA, independentemente de serem serviços realizados internamente ou externamente.

Seção VI

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

Art. 14 O MMA 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.

Seção VII

Da avaliação quanto às condições mínimas de infraestrutura de TIC do MMA

para utilizar serviços de computação em nuvem

Art. 15 O MMA deve ter conexão estável com a Internet e com banda suficiente para gerenciar softwares e serviços de computação em nuvem.

Seção VIII

Da definição de diretrizes de governança para o uso da nuvem

Art. 16 O MMA deve definir papéis e responsabilidades para as áreas de TI, de negócio e da nuvem.

§ Único. Esses papéis e responsabilidade devem ser definidas antes de iniciar um processo de implementação do modelo Híbrido de Nuvem, ou seja, com a utilização dos recursos da sala cofre e de outro fornecedor externo.

Seção IX

Do estabelecimento dos princípios norteadores da estratégia

Art. 17 O MMA deve adotar os seguintes princípios norteadores da estratégia:

I – lift and shift; ou seja, migração de aplicativos e dados associados para a nuvem, a partir do desinvestimento na sala cofre, com o mínimo ou nenhuma alteração;

II - cloud first; ou seja, manter em mente a necessidade e importância do uso da nuvem como estratégia de negócio;

III - broker multicloud, quando o processo de migração estiver avançado.

Seção X

Do alinhamento com outros planos estratégicos

Art. 18 Esta estratégia deve estar alinhada com os seguintes planos estratégicos:

I - Plano de Desenvolvimento Institucional;

II - Plano Diretor de Tecnologia da Informação;

III - Plano de Contratações Anual; e

IV - Plano de Gestão de Segurança da Informação.

Seção XI

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

Art. 19 O MMA deve definir linhas de base e metas de benefícios/resultados esperados objetivando maior agilidade, redução de custos, resiliência, mais segurança etc.

Seção XII

Das considerações sobre capacitação da equipe

Art. 20 O MMA já utiliza de uma empresa para dar suporte aos serviços desenvolvidos na sala cofre, cuja capacitação é de responsabilidade da própria empresa.

§ Único. Quando do início do processo de migração, o MMA deve sinalizar à empresa de sustentação do ambiente, os novos requerimentos de conhecimentos para que a empresa possa capacitar a equipe que gerenciará, operará, utilizará ou integrará os recursos de software e de computação de serviços em nuvem, identificando as capacidades e habilidades necessárias.

Seção XIII

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

Art. 21 O MMA deve considerar a viabilidade de adoção de medidas para mitigar a dependência tecnológica ou aprisionamento ao provedor.

§ Único. O MMA deverá identificar os serviços que forem migrados para a nuvem e retirados do ambiente controlado da sala cofre, para a redução dos custos de sustentação do ambiente em relação à empresa atual.

Seção XIV

Dos requisitos regulatórios e de conformidade

Art. 22 O MMA deve considerar os requisitos regulatórios e de conformidade para o uso seguro de software e serviços de computação em nuvem no âmbito do MMA e da administração pública federal.

§ Único. Os sistemas estruturantes assim definidos pelo Governo Federal, somente serão migrados com a autorização do mesmo e para os ambiente de nuvem recomendados, estando desde já, vetada qualquer transferência que não obedeça aos critérios acima.

Seção XV

Da indicação da estratégia de saída

Art. 23 O MMA deve considerar a análise de dependências e aspectos de portabilidade (backup, redundância, contratos de apoio, retorno para a infraestrutura local etc.). Isso somente será feito após um ano da transferência do primeiro serviço migrado para a nuvem.

Seção XVI

Art. 24 O MMA 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 VII

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

Art. 25 Para que esteja habilitado a prestar serviços de computação em nuvem para o MMA, o provedor de serviço de nuvem deverá cumprir, no mínimo, os seguintes requisitos:

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

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

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

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

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

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

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

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

g) habilitar o registro completo do Hypervisor; e

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

III - em relação ao gerenciamento de identidades e registros:

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

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

c) suportar 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 do órgão ou da entidade no provedor de serviço de nuvem, de acordo com nível de criticidade da informação;

e) permitir ao MMA gerenciar as próprias identidades, inclusive criação, atualização, exclusão e

suspensão no ambiente fornecido pelo provedor de serviço de nuvem; e

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

IV - em relação à segurança de aplicações web disponibilizadas no ambiente de nuvem: a) utilizar firewalls especializados na proteção de sistemas e aplicações;

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

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

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

e) possuir um programa de correção de vulnerabilidades;

f) definir que os dados migrados para a nuvem, tenham no mínimo, as mesmas proteções, validações e segurança dos dados mantidos na sala cofre, enquanto for mantido o modelo híbrido de nuvem.

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

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

VII - estabelecer um canal de comunicação seguro utilizando, no mínimo, 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 pelo MMA;

IX - disponibilizar facilidades que possibilitem a aplicação de uma proteção criptográfica própria do MMA.

X - em relação à segregação de dados:

a) isolar, utilizando separação lógica, todos os dados e serviços do MMA ou da entidade de outros clientes de serviço em nuvem;

b) segregar o tráfego de gerenciamento do tráfego de dados do MMA; e

c) implementar dispositivos de segurança entre zonas.

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

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

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

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

XII - notificar, imediatamente, aos órgãos ou às entidades incidente cibernético contra os serviços ou dados sob sua custódia;

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

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

CAPÍTULO VIII

DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

Seção I

Da alta administração - SPOA

Art. 26 Compete à alta administração:

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

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

§ Único. Capacitar, no mínimo, um servidor do Ministério como especialista nas técnicas e boas práticas necessárias para a gestão de serviços de computação em nuvem.

Seção II

Da Alta Administração - Comitê de Segurança da Informação

Art. 27 Compete ao Comitê de Segurança da Informação:

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

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

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

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

Seção III

Do Gestor de Segurança da Informação

Art. 28 Compete ao Gestor de Segurança da Informação:

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

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

nuvem;

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

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

V - comunicar incidentes cibernéticos informados pelo provedor de serviço de nuvem aos órgãos competentes para os seus tratamentos, conforme a relevância dos incidentes previamente estabelecida;

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

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

Seção IV

Da Coordenação Geral de Tecnologia da Informação do MMA

Art. 29 Compete à Coordenação Geral de Tecnologia da Informação e demais setores de TI das unidades do MMA:

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

CAPÍTULO IX

DA REVISÃO E ATUALIZAÇÃO

Art. 30 Esta estratégia bem como os documentos gerados a partir dela devem ser revisados, aprovados e atualizados em função de alterações na legislação pertinente, de diretrizes políticas do governo federal, de alterações nas políticas e normas do MMA, quando considerada necessária pelo Comitê de Segurança da Informação.

Art. 31 Em função da capacidade de os provedores de serviço de computação em nuvem implementar atualizações relacionadas à segurança da informação em seus produtos e serviços, a presente estratégia deve ser revisada em até 2 (dois) anos para:
I - definir novos critérios e a periodicidade das atualizações dos procedimentos e dos recursos computacionais a serem observados pelo provedor de serviço de nuvem;
II - atualizar periodicamente os processos internos de gestão de riscos de segurança da informação;

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

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

CAPÍTULO X

DAS DISPOSIÇÕES FINAIS

Art. 32 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. 33 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. 34 A alta administração deve disponibilizar os recursos (humanos, tecnológicos e financeiros) necessários para a execução desta estratégia.

Art. 35 Os casos omissos não abordados neste documento serão analisados pelo Comitê de Segurança da Informação.

Art. 36 Esta norma após formalmente aprovada pelo Comitê de Segurança da Informação, e referendada pela Subsecretaria de Planejamento, Orçamento e Administração, entra em vigor a partir da data de sua publicação no Boletim Interno de Serviço.

Documento assinado eletronicamente por **Jonas Jeske**, **Coordenador(a) - Geral**, em 16/05/2025, às 15:43, conforme horário oficial de Brasília, com fundamento no Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site http://sei.mma.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1976594** e o código CRC **92930B91**.
