DIÁRIO OFICIAL DA UNIÃO

Publicado em: 25/07/2025 | Edição: 139 | Seção: 1 | Página: 822

Órgão: Ministério da Saúde/Gabinete do Ministro

PORTARIA GM/MS Nº 7.678, DE 23 DE JULHO DE 2025

Institui a Estratégia de uso de software e de serviços de computação em nuvem no âmbito do Ministério da Saúde.

O MINISTRO DE ESTADO DA SAÚDE, no uso das atribuições que lhe confere o art. 87, parágrafo único, incisos I e II, da Constituição, resolve:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Estratégia de Uso de Software e de Serviços de Computação em Nuvem, que estabelece diretrizes, princípios e orientações para o uso de software e de serviços de computação em nuvem no âmbito do Ministério da Saúde, em atenção ao disposto na Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, e na Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021.

Art. 2º A estratégia de uso de software e de serviços de computação em nuvem tem como objetivos:

I - estruturar e orientar a adoção, implementação e governança responsável de serviços e soluções baseadas em nuvem, assegurando a integridade dos dados, a proteção da informação sensível e o atendimento às regulamentações vigentes de segurança da informação e privacidade;

II - estabelecer diretrizes para a utilização de soluções de computação em nuvem no Ministério da Saúde, com objetivo de garantir a segurança, integridade, confidencialidade e a disponibilidade dos dados do ambiente tecnológico de acordo com a Política de Segurança da Informação do Ministério da Saúde;

III - definir requisitos de segurança que devem ser atendidos pelos provedores de soluções de computação em nuvem, incluindo criptografia, autenticação forte, gerenciamento de identidade e acesso, auditorias regulares e monitoramento de segurança;

IV - estabelecer critérios claros para avaliar e selecionar provedores de soluções de computação em nuvem que atendam aos requisitos de segurança da informação e privacidade;

V - promover a modernização da infraestrutura de Tecnologia de Informação do Ministério de Saúde, aumentando a eficiência e a escalabilidade dos serviços;

VI - reduzir custos operacionais e otimizar a alocação de recursos tecnológicos por meio de modelos de consumo sob demanda;

VII - assegurar a conformidade com as normativas vigentes, incluindo a Lei Geral de Proteção de Dados e as diretrizes da Estratégia de Governo Digital;

VIII - aprimorar a interoperabilidade e a integração entre sistemas e serviços do Ministério da Saúde; e

IX - fortalecer a governança e a gestão dos serviços de computação em nuvem, estabelecendo métricas de monitoramento e avaliação contínua.

CAPÍTULO II

DAS COMPETÊNCIAS

Art. 3º Compete à Secretaria de Informação e Saúde Digital, apoiada pelo Departamento de Informação e Informática do Sistema Único de Saúde e demais áreas competentes, assegurar a utilização de tecnologias de computação em nuvem em conformidade com as orientações contidas nesta Portaria, e:

I - deliberar sobre os projetos novos que não ultrapassem o limite previsto no inciso III, do art. 4º desta Portaria;

II - deliberar sobre o aumento de recursos em projetos já existentes ou previamente aprovados, desde que eles não tenham impacto financeiro anual superior ao limite estabelecido no art. 75, inciso II, da Lei nº 14.133/2021; e

III - deliberar sobre o aumento de recursos em situações emergenciais ou excepcionais, ainda que ultrapasse os limites previstos no art. 75, inciso II, da Lei nº 14.133/2021, desde que:

a) a emergência esteja caracterizada por eventos imprevisíveis, falhas críticas que comprometam a continuidade dos serviços, inoperância de sistemas/projetos, riscos à segurança da informação ou à integridade de dados, ou outras situações de caráter urgente que exijam resposta imediata;

b) a solicitação de aumento seja acompanhada de justificativa técnica circunstanciada, com a descrição clara da emergência, da necessidade adicional de recursos, da relação direta com o projeto original e da estimativa de impacto financeiro;

c) haja ciência e aprovação da autoridade competente da Área de TIC;

d) seja elaborado relatório posterior, no prazo máximo de 30 (trinta) dias após a adoção da medida, detalhando os resultados alcançados, os custos envolvidos, e a avaliação quanto à necessidade de revisão da estratégia original de uso de recursos, que deverá ser submetido à ciência do CGD na primeira reunião posterior à sua elaboração; e

e) para fins de controle, as solicitações de aumento de recursos serão registradas e o registro conterá o histórico por projeto e por área demandante, verificando-se as reincidências, frequências e valores acumulados no exercício financeiro sendo vedada a fragmentação de solicitações.

Seção I

Do Comitê de Governança Digital do Ministério da Saúde - CGD/MS

Art. 4º Compete ao Comitê de Governança Digital - CGD, nos termos dispostos no Capítulo II do Título VII da Portaria de Consolidação GM/MS nº 1, de 28 de setembro de 2017:

I - aprovar as diretrizes e decisões relacionadas à contratação de software e de serviços de computação de nuvem que sejam de alta relevância para a continuidade dos serviços finalísticos da organização pública;

II - deliberar sobre aspectos críticos de segurança, compliance e continuidade dos serviços; e

III - deliberar sobre os projetos cujo consumo monetário estimado anual para implementação em ambiente de nuvem seja superior ao limite estabelecido no art. 75, inciso II, da Lei nº 14.133/2021, exceto os projetos contemplados na respectiva contratação, circunstância na qual fica dispensada a aprovação, devendo ser submetido à ciência do CGD na primeira reunião posterior à deliberação.

Parágrafo único - Entende-se por serviços de alta relevância, aqueles que possuem potencial de paralisação ou de causar prejuízo à continuidade dos serviços finalísticos da organização pública.

Seção II

Do Comitê Gestor de Segurança da Informação - CGSI

Art. 5º As competências do Comitê Gestor de Segurança da Informação - CGSI estão previstas no art. 254-E da Portaria de Consolidação GM/MS nº 1, de 28 de setembro de 2017.

CAPÍTULO III

DOS REQUISITOS PARA CONTRATAÇÃO DE SOFTWARE E DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM

Art. 6º As contratações e inclusão de projetos em ambiente de nuvem deverão estar alinhadas com o Plano Diretor de Tecnologia da Informação Comunicação e com a Estratégia Federal de Governo Digital.

Art. 7º As arquiteturas das soluções de nuvem deverão considerar custos e os princípios de segurança by design.

Art. 8º As soluções de nuvem e software serão preferencialmente diagnósticas e deverão considerar estratégias de saída.

Art. 9º As contratações e inclusão de projetos em ambiente de nuvem devem identificar e avaliar previamente:

I - as necessidades de negócio antes da contratação de software e de serviços de computação em nuvem, sendo necessária a determinação de 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; e

II - quais modelos de serviço e de implementação melhor se adequam aos requisitos de negócio, nos casos de contratação.

Art. 10. 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, considerando segurança, conformidade, disponibilidade e suporte técnico devem ser considerados nessa avaliação.

Art. 11. No planejamento das contratações de softwares e de serviços de computação em nuvem, deve-se elaborar análise de riscos, considerando as diretrizes de gerenciamento de riscos constantes no modelo definido na Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023.

Art. 12. As soluções devem sempre considerar critérios de interoperabilidade dos dados e transparência, planejando a possibilidade da necessidade de abertura dos dados e informações.

Art. 13. Os estudos de adoção de projetos e soluções de nuvem e software deverão sempre considerar a possibilidade de cenários e alternativas, inclusive entre diferente fornecedores e provedores.

Art. 14. As soluções de nuvem e de software devem sempre observar requisitos de soberania e residência de dados, com a devida classificação da informação a ser armazenada.

Art. 15. A inclusão de novos projetos no ambiente de nuvem ficarão condicionados à análise do impacto no saldo contratual e no andamento dos projetos existentes, bem como os riscos associados.

Art. 16. As migrações de cargas de trabalho e aplicações para nuvem deverão sempre considerar a possibilidade de refatoração, utilizando-se de técnicas de lift-and-shift como último recurso.

Art. 17. As decisões entre o uso da nuvem ou do ambiente on premises devem ser pautadas por análise de custo benefício, soberania, riscos, residência de dados e recursos disponíveis.

Art. 18. As soluções de nuvem e de software devem sempre considerar em sua arquitetura os princípios de alta-disponibilidade, resiliência, recuperação de dados, desacoplamento, observabilidade e rastreamento das cargas de trabalho, bem como seguir as normas de segurança da informação publicadas pelo Ministério da Saúde e outros órgãos competentes.

Art. 19. Os ambientes de nuvem serão sempre inventariados e monitorados com o objetivo de encontrar possibilidades de redução de custos e de desperdícios.

Art. 20. As decisões de arquitetura devem condizer aos requisitos de negócio e avaliar a aplicação dos serviços e modelos adequados para obtenção destes objetivos.

Art. 21. No caso de contratações de software como Software e Service - SaaS em ambientes de nuvem, a empresa prestadora do serviço deverá observar os critérios de segurança e os requisitos de sigilo e confidencialidade indicados pelo Ministério da Saúde.

CAPÍTULO IV

DOS REQUISITOS PARA USO SEGURO DE COMPUTAÇÃO EM NUVEM

Art. 22. Na transferência de serviços para um provedor de serviço de nuvem, o Ministério da Saúde deverá:

I - garantir que estejam alinhadas à 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) coleta, armazenamento, guarda e tratamento de registros de dados pessoais; e

b) comunicações realizadas por provedores de conexão e de aplicações de internet, em que pelo menos um desses atos ocorra em território nacional.

II - realizar o gerenciamento de riscos, precedido por análise e relatório de impacto de dados pessoais, em conformidade com 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 - utilizar, para os sistemas estruturantes, preferencialmente modelos de implementação de nuvem privada;

V - avaliar quais informações serão hospedadas na nuvem, considerando:

a) o processo de classificação da informação de acordo com a legislação;

b) o valor do ativo de informação;

c) os controles de acessos físico e lógico relativos à segurança da informação; e

d) o modelo de serviço e de implementação de computação em nuvem.

VI - 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

VII - planejar custos de migração das informações e dos serviços, nos casos de ingresso e de saída dos serviços de computação em nuvem.

Art. 23. Na análise da capacidade do provedor de serviço de nuvem para implementar atualizações, o Ministério da Saúde deverá:

I- observar a periodicidade da revisão das atualizações dos procedimentos e dos recursos computacionais a serem cumpridas pelo provedor de serviço de nuvem, que será definida conforme criticidade ou relevância da atualização sugerida pelo provedor; e

II - revisar e atualizar periodicamente os processos internos de gestão de riscos de segurança da informação.

Art. 24. No gerenciamento de identidades e de registros (logs), o Ministério da Saúde deverá:

I - adotar um padrão de identidade federada para permitir o uso de tecnologia single sign-on no processo de autenticação de seus usuários no provedor de serviço de nuvem;

II - negar ao provedor de serviço de nuvem permissão de uso e acesso direto ao ambiente de autenticação do Ministério da Saúde;

III - exigir do cloud broker a proteção adequada ao usuário "root" das contas abertas junto aos provedores de nuvem, documentando quais são as proteções aplicadas; e

IV - adotar, de acordo com o nível de criticidade da informação, o uso da tecnologia single-sign-on, o qual deve ser acompanhado de autenticação multifator.

Art. 25. No uso de recursos criptográficos, o Ministério da Saúde deverá:

I - garantir que os dados do Ministério da Saúde estão sendo tratados e armazenados de acordo com a legislação; e

II - analisar a necessidade de criptografar dados com base nos requisitos legais, nos riscos, no nível de criticidade, nos custos e nos benefícios.

Art. 26. Na adoção de medidas de segregação de dados e da separação lógica, o provedor de nuvem deverá:

I - garantir que o ambiente contratado seja protegido de usuários externos do serviço em nuvem e de pessoas não autorizadas e implementar controles de segurança da informação de forma a propiciar o isolamento adequado dos recursos utilizados pelo Ministério da Saúde; e

II - avaliar os riscos associados à execução de softwares proprietários a serem instalados no serviço de nuvem.

CAPÍTULO V

DO TRATAMENTO DAS INFORMAÇÕES

Art. 27. O tratamento de informações em ambiente de computação em nuvem será permitida, desde que observados os riscos à segurança da informação e a legislação vigente, incluindo os seguintes tipos de conteúdo:

I- informação sem restrição de acesso;

II - informação com restrição de acesso prevista na legislação, conforme o Anexo à Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021;

III - material de acesso restrito regulado pelo Ministério da Saúde;

IV - informação pessoal relativa à intimidade, vida privada, honra e imagem; e

V - documento preparatório, com exceção do tipo previsto no art. 16 desta Portaria.

Art. 28. É vedado o tratamento, em ambiente de computação em nuvem, de informação classificada em grau de sigilo e documento preparatório que possa originar informação classificada, em conformidade com a Lei nº 12.527, de 18 de novembro de 2011, e a Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021.

Art. 29. O Ministério da Saúde deverá, em até cinco anos, mover suas cargas de trabalho que contenham informações previstas nos art. 27 e 28 para soluções on-premise ou de nuvem de governo, ou seja, onde haja garantia de que a soberania, gestão e residência destes dados estejam sob responsabilidade de um órgão ou entidade pública.

Art. 30. Os dados tratados em ambiente de nuvem devem ser armazenados em data centers localizados em território brasileiro, sendo admitido o tratamento de dados em data centers fora do território brasileiro somente nos casos em que haja cópia de segurança atualizada armazenada em data centers localizados em território brasileiro, respeitando-se os demais limites estabelecidos nesta Portaria.

CAPÍTULO VI

DO INVENTÁRIO DOS ATIVOS DE INFORMAÇÃO ARMAZENADOS EM NUVEM

Art. 31. O Ministério da Saúde deve realizar inventário de ativos dos serviços em nuvem que contabilize as informações e os ativos associados que estão armazenados no ambiente de computação em nuvem.

Parágrafo único. Os registros do inventário devem indicar onde o ativo é mantido e a identificação do serviço em nuvem.

CAPÍTULO VII

DA GESTÃO DO AMBIENTE DE NUVEM

Art. 32. As novas propostas de projetos a serem incorporados na nuvem deverão conter:

I - esboço da arquitetura a ser implementada, inclusive apontando serviços e tecnologias, volumetria esperada e projeções de crescimento;

II - a projeção de custos mensais e anuais;

III - análise da área responsável pela gestão contratual do impacto deste novo projeto no saldo contratual e no andamento dos projetos atuais;

IV - parecer conclusivo sobre a possibilidade de implementação, sob a ótica de arquitetura segurança infraestrutura e banco de dados elaborado pelas respectivas aéreas responsáveis, por meio do Departamento de informação e Informática do Sistema Único de Saúde da secretaria de Informação e saúde Digital, e

V - aprovação da Comitê de Governança Digital do Ministério da Saúde, nos casos previstos do art. 4º, início III; ou do Departamento de Informação e Informática do Sistema Único de Saúde da Secretaria de Informação e Saúde Digital, nos demais casos

§ 1º Para os efeitos desta Portaria, consideram-se novas propostas de projetos aqueles já aprovados e que necessitem de transformações relevantes em sua arquitetura, independentemente de aprovação anterior.

§ 2º Ficam excluídos das disposições do caput os projetos já explicitamente mensurados e devidamente descritos nos instrumentos de planejamento da contratação dos serviços de nuvem e de software.

Art. 33. As ferramentas de marketplace (de terceiros) a serem contratadas nos ambientes de nuvem devem passar pelo mesmo processo de análise e aprovação dispostos no art. 32, e, adicionalmente, conter justificativa para o uso da ferramenta e o custo-benefício de seu uso nesta modalidade.

CAPÍTULO VIII

DA UTILIZAÇÃO DE CLOUD BROKERS

Art. 34. O cloud broker deverá atuar como integrador dos serviços de computação em nuvem entre o Ministério da Saúde e dois ou mais provedores de serviço de nuvem.

Parágrafo único. O cloud broker é o responsável por garantir que os provedores de serviço de nuvem que ele representa atendam aos requisitos previstos na legislação vigente, bem como operem de acordo com as melhores práticas de segurança.

Art. 35. O cloud broker poderá utilizar ferramenta de (SaaS) comum de mercado, desde que não haja risco de dependência tecnológica para disponibilizar essa plataforma.

Art. 36. O Ministério da Saúde deverá garantir que os serviços prestados pelo cloud broker agreguem valor, com a indicação de melhores práticas, tecnologias e preços, de forma a dar suporte à tomada de decisão de incorporação de processos na nuvem.

Art. 37. O Ministério da Saúde deverá prever no instrumento contratual que o cloud broker poderá ser responsabilizado, civil e administrativamente, por qualquer desconformidade nos provedores que ele representa.

CAPÍTULO IX

DAS DISPOSIÇÕES FINAIS

Art. 38. Deverão ser requisitos mínimos para contratação dos serviços de computação em nuvem:

I - capacitar a equipe responsável por esse gerenciamento nas tecnologias utilizadas pelo provedor de serviço de nuvem, com a inclusão da ação no Plano de Desenvolvimento de Capacitação do Ministério da Saúde;

II - exigir que nas cláusulas contratuais que as empresas prestadoras de serviços que executem ações no ambiente de nuvem comprovem capacitação adequada aos requisitos de nuvem;

III - exigir que o provedor de serviço de nuvem documente e comunique seus recursos, papéis e responsabilidades de segurança da informação para o uso de seus serviços em nuvem;

IV - elaborar um processo de tratamento de incidentes junto ao provedor de serviço de nuvem e ao cloud broker e comunicá-lo à equipe responsável pelo gerenciamento da nuvem;

V - criar uma política de etiquetagem padronizada para padronização da identificação dos recursos dentro do ambiente de nuvem;

VI - adotar técnicas de redução e contenção de custos, tais como definição de ciclo de vida dos dados, reservas de instâncias, identificação de recursos subutilizados, etc; e

VII - realizar a revisão periódica dos preços e serviços apresentados nos catálogos de serviços dos provedores de nuvem com a finalidade de redução de custos e adoção de novas tecnologias que possam trazer benefício.

Art. 39. O provedor de serviço de nuvem deve documentar e comunicar ao Ministério da Saúde seus recursos, papéis e responsabilidades de segurança da informação para o uso de seus serviços em nuvem.

Art. 40. O Departamento de Informação e Informática do Sistema Único de saúde da Secretaria de Informação e Saúde Digital do Ministério da saúde deverá adotar, 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 conformidades na utilização dos recursos e nas contratações de software e dos serviços de nuvem de acordo com as necessidades de negócio do Órgão.

Art. 41. Esta Portaria entra em vigor na data de sua publicação.

ALEXANDRE ROCHA SANTOS PADILHA