



ANVISA

Agência Nacional de Vigilância Sanitária

Boletim de Serviço

Nº 37/2026

10 de agosto de 2026

Diretor-Presidente
Leandro Pinheiro Safatle
Adjunto: Diogo Penha Soares

Diretorias

Segunda Diretoria
Diretora: Daniela Marreco Cerqueira
Adjunto: Elkiane Macedo Rama

Terceira Diretoria
Diretor Substituto: Marcelo Mário Matos Moreira
Adjunto: Suzana Yumi Fujimoto

Quarta Diretoria
Diretor: Daniel Meirelles Fernandes Pereira
Adjunto: Leandro Rodrigues Pereira

Quinta Diretoria
Diretor: Thiago Lopes Cardoso Campos
Adjunto: Allan Nuno Alves de Sousa

Secretaria Geral da Diretoria Colegiada - SGcol
Kenia Hugo Lucas
Sgcol.publicacao@anvisa.gov.br
Equipe Técnica

Projeto e Design Gráfico
Assessoria de Divulgação e Comunicação Institucional – ASCOM
intravisa@anvisa.gov.br
copyright ANVISA 2025-10-06

SUMÁRIO

PORTARIAS:

PORTARIA Nº 87/GGGAF/ANVISA, DE 22 DE JULHO DE 2026	4
PORTARIA Nº 96/GGGAF/ANVISA, DE 03 DE AGOSTO DE 2026	5
PORTARIA Nº 404/GGPES/ANVISA, DE 30 DE JULHO DE 2026.....	6
PORTARIA Nº 407/GGPES/ANVISA, DE 30 DE JULHO DE 2026.....	18
PORTARIA Nº 408/GGPES/ANVISA, DE 31 DE JULHO DE 2026.....	19
PORTARIA Nº 419/GGPES/ANVISA, DE 03 DE AGOSTO DE 2025.....	24
PORTARIA Nº 420/GGPES/ANVISA, DE 04 DE AGOSTO DE 2026.....	25
PORTARIA Nº 421/GGPES/ANVISA, DE 04 DE AGOSTO DE 2026.....	26
PORTARIA Nº 422/GGPES/ANVISA, DE 04 DE AGOSTO DE 2026.....	27
PORTARIA Nº 423/GGPES/ANVISA, DE 05 DE AGOSTO DE 2026.....	28
PORTARIA Nº 424/GGPES/ANVISA, DE 05 DE AGOSTO DE 2026.....	29
PORTARIA Nº 425/GGPES/ANVISA, DE 05 DE AGOSTO DE 2026.....	30
PORTARIA Nº 426/GGPES/ANVISA, DE 05 DE AGOSTO DE 2026.....	31
PORTARIA Nº 427/GGPES/ANVISA, DE 05 DE AGOSTO DE 2026.....	32
PORTARIA Nº 428/GGPES/ANVISA, DE 06 DE AGOSTO DE 2026.....	33
PORTARIA Nº 429/GGPES/ANVISA, DE 06 DE AGOSTO DE 2026.....	34
PORTARIA Nº 430/GGPES/ANVISA, DE 07 DE AGOSTO DE 2026.....	35
PORTARIA Nº 431/GGPES/ANVISA, DE 07 DE AGOSTO DE 2026.....	36
PORTARIA Nº 432/GGPES/ANVISA, DE 07 DE AGOSTO DE 2026.....	37
PORTARIA Nº 433/GGPES/ANVISA, DE 07 DE AGOSTO DE 2026.....	38
PORTARIA Nº 888/ANVISA, DE 3 DE AGOSTO DE 2026	39
PORTARIA Nº 907/ANVISA, DE 5 DE AGOSTO DE 2026	40
PORTARIA Nº 911/ANVISA, DE 7 DE AGOSTO DE 2026	42
Institui a estratégia de uso de software e serviços de computação em nuvem da Agência Nacional de Vigilância Sanitária (Anvisa).....	42

ORIENTAÇÃO DE SERVIÇO:

ORIENTAÇÃO DE SERVIÇO Nº 02/COGER/ANVISA, DE 10 DE AGOSTO DE 2026..	55
ORIENTAÇÃO DE SERVIÇO Nº 03/COGER/ANVISA, DE 10 DE AGOSTO DE 2026..	59

SUPRIMENTO DE FUNDOS:

PUBLICAÇÃO DE SUPRIMENTO DE FUNDOS – ANVISA SEDE.....	60
PUBLICAÇÃO DE SUPRIMENTO DE FUNDOS – ANVISA SEDE.....	61

CONCESSÃO DE DIÁRIAS:

PROPOSTA DE CONCESSÃO DE DIÁRIAS-PCD-ANVISA/BRASÍLIA.....	62
---	----

PORTARIA Nº 911/ANVISA, DE 7 DE AGOSTO DE 2026

Institui a estratégia de uso de software e serviços de computação em nuvem da Agência Nacional de Vigilância Sanitária (Anvisa).

O DIRETOR-PRESIDENTE DA AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA, no uso das atribuições que lhe confere o art. 172, XII, aliado ao art. 203, III, § 3º do Regimento Interno aprovado pela Resolução da Diretoria Colegiada – RDC nº 585, de 10 de dezembro de 2021, resolve:

Art. 1º Fica instituída a estratégia de uso de software e serviços de computação em nuvem da Agência Nacional de Vigilância Sanitária (Anvisa).

TÍTULO I
DAS DISPOSIÇÕES INICIAIS
CAPÍTULO I
FINALIDADE

Art. 2º A Estratégia de Uso de Software e Serviços de Computação em Nuvem no âmbito da Agência Nacional de Vigilância Sanitária (Anvisa), elaborada em observância à Seção 5 do Anexo I da Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, estabelece as diretrizes institucionais para a adoção, contratação e utilização de software e serviços de computação em nuvem, considerando a natureza e a finalidade da Agência — a proteção da saúde da população mediante o controle sanitário da produção, da comercialização e do consumo de produtos e serviços submetidos à vigilância sanitária, inclusive os ambientes, processos, insumos e tecnologias a eles relacionados — e seu alinhamento ao planejamento estratégico institucional para as atividades de gestão da informação e disponibilização de serviços internos e externos.

Art. 3º Para os fins do disposto nesta Estratégia, a segurança da informação abrange:

- I - dos dados, dos ativos de informação e dos processos organizacionais;
- II - do ambiente físico e eletrônico que contenha ativos de informação; e
- III - do pessoal envolvido no ciclo de vida da informação.

Art. 4º A presente Estratégia aplica-se às novas contratações de software e serviços de computação em nuvem, bem como, quando aplicável, às prorrogações e alterações relevantes dos respectivos instrumentos contratuais, 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 ou serviços de computação em nuvem.

Parágrafo único. Os contratos vigentes poderão ser avaliados quanto à aderência às diretrizes desta Estratégia quando de sua prorrogação, revisão ou substituição, observadas a conveniência administrativa, a viabilidade técnica e as disposições legais e contratuais aplicáveis.

CAPÍTULO II

DOS CONCEITOS E DAS DEFINIÇÕES

Art. 5º Para os efeitos da Estratégia de Uso de Software e de Serviços de Computação em Nuvem, bem como da sua utilização em futuras contratações, adotam-se as seguintes definições:

I - atualização de versões: disponibilização, por parte do fabricante, de uma versão completa do software, ou parcial, mas com funcionalidades adicionais ou evoluções tecnológicas que compreendam uma nova versão estável do produto. Podem, também, incluir correções de comportamentos disfuncionais que não tenham sido corrigidos por manutenções anteriores do software, por critério do fabricante;

II - Catálogo de Serviços de Computação em Nuvem Padronizados: relação de serviços de computação em nuvem que um órgão ou entidade fornece aos seus usuários, elaborada de forma padronizada, de acordo com as necessidades do órgão ou entidade e conforme as orientações estabelecidas pela SGD;

III - Catálogo de Soluções de TIC com condições padronizadas: relação de soluções de TIC ofertadas pelo mercado que possuem condições padrões definidas pelo Órgão Central do SISP, podendo incluir o nome da solução, descrição, níveis de serviço, Preço Máximo de Compra de Item de TIC - PMCTIC, entre outros;

IV - Carga de trabalho (workload): conjunto de recursos que compõem uma arquitetura técnica destinada a suportar um ou mais serviços de TIC. As cargas de trabalho podem requerer uma combinação de recursos computacionais e de serviços técnicos para agregar valor ao negócio por meio de serviços de TIC;

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

VI - Computação em nuvem: modelo que possibilita o provisionamento e a utilização sob demanda de recursos e serviços computacionais de qualquer lugar e a qualquer momento, de maneira conveniente, com acesso por meio de rede a recursos configuráveis (ex.: redes, segurança, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente provisionados, utilizados e liberados com o mínimo de esforço em gerenciamento ou interatividade com o provedor de serviços em nuvem;

VII - Consultoria especializada em software: serviços especializados de configuração, customização, instalação, otimização e manutenção em software cujos padrões de desempenho e qualidade podem ser objetivamente definidos no Termo de Referência. Esses serviços não se confundem com os serviços técnicos especializados de natureza predominantemente intelectual, dispostos no inciso XVIII do art. 6º da Lei nº 14.133, de 1º de abril de 2021;

VIII - Datacenter ou centro de dados: consiste em uma estrutura, ou grupo de estruturas, dedicada à acomodação centralizada, interconexão e operação dos equipamentos de tecnologia da informação e redes de telecomunicações que fornece serviços de armazenamento de dados, processamento e transporte, em conjunto a todas as instalações e infraestruturas de distribuição de energia e controle ambiental, juntamente com os níveis necessários de recuperação e segurança requeridos para fornecer a disponibilidade de serviço desejada, conforme ABNT NBR ISO/IEC 22.237-1:2023;

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

X - Hosting: locação de recursos computacionais localizados em infraestrutura física tradicional de data center pertencente a terceiros, sem o compartilhamento de recursos entre clientes, para a hospedagem de aplicações e soluções de TI;

XI - Incidente: qualquer acontecimento não planejado que cause redução na qualidade do serviço ou interrupção do serviço em parte ou como um todo, ou evento que ainda não impactou o serviço do usuário;

XII - Incidente de Segurança da Informação: qualquer evento de segurança da informação indesejável e inesperado, seja único ou em série, que pode comprometer as operações de negócio e ameaçar a segurança da informação;

XIII - IN GSI/PR nº 5, de 2021: Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;

XIV - IN SGD/ME nº 94, de 2022: Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

XV - Instância de Computação: componente de computação em nuvem composto de máquina virtual e serviços agregados, como armazenamento, dispositivos de rede e demais serviços necessários para manter essa máquina virtual em operação;

XVI - Integrador de Serviços em Nuvem (Cloud Broker): realiza a integração dos serviços de computação em nuvem com agregação de valor entre o órgão ou a entidade e dois ou mais provedores de serviço de computação em nuvem. O Cloud Broker apoia o órgão ou entidade em descobrir, planejar, migrar, configurar, utilizar, gerenciar e evoluir os serviços de computação em nuvem de forma segura e eficiente. Os serviços prestados pelo Cloud Broker são orientados de acordo com os padrões internacionais relevantes, como a ISO e a NIST e, no Brasil, a Associação Brasileira de Normas Técnicas - ABNT, para garantir que os serviços sejam oferecidos de forma segura, eficiente e confiável;

XVII - Licença de software: documento que fornece diretrizes legalmente vinculantes para o uso e a distribuição de determinado software. A licença de software geralmente fornece aos usuários finais o direito a uma ou mais cópias do software sem incorrer em violação de direitos autorais. Também define as responsabilidades das partes envolvidas no contrato de licença.

Além disso, pode impor restrições sobre como o software pode ser usado. Os termos e condições de licenciamento de software geralmente incluem o uso justo do software, as limitações de responsabilidade, garantias e isenções de responsabilidade e proteções se o software ou seu uso infringirem os direitos de propriedade intelectual de terceiros;

XVIII - Licença de uso: instrumento que estabelece o direito de usar o software sem haver a transferência da sua propriedade entre o licenciante e o licenciado, e inclui, entre outros direitos, o serviço de correção de erros, sem ônus ao licenciado;

XIX - Licença por subscrição/assinatura: permite aos usuários acessar o software por meio de serviços online, em vez de adquirir uma licença de uso único. As licenças por assinatura também podem fornecer aos usuários acesso a atualizações de software, suporte técnico e outros serviços;

XX - Licença perpétua: é uma licença que concede ao usuário o direito de usar o software por tempo indeterminado, bem como acesso a updates e suporte técnico por tempo determinado;

XXI - Manutenção de software (correção de erros): é o processo de fornecer suporte técnico, atualizações e melhorias para um determinado software. É um processo contínuo que garante que o software se mantenha atualizado e funcione corretamente;

XXII - Marketplace: loja virtual operada por um provedor de nuvem que oferece acesso a software e serviços que são desenvolvidos, se integram ou complementam as soluções disponibilizadas pelo provedor de nuvem;

XXIII - Modelos de implantação de nuvem: representam como a computação em nuvem pode ser organizada, com base no controle e no compartilhamento de recursos físicos ou virtuais. Os modelos de implantação em nuvem incluem: nuvem pública, nuvem privada, nuvem comunitária e nuvem híbrida;

XXIV - Modelo de Serviços em nuvem IaaS (Infrastructure as a Service - Infraestrutura como Serviço): capacidade fornecida ao cliente para provisionar processamento, armazenamento, comunicação de rede e outros recursos de computação fundamentais, nos quais o cliente pode instalar e executar software em geral, incluindo sistemas operacionais e aplicativos. O cliente não gerencia nem controla a infraestrutura na nuvem subjacente, mas tem controle sobre os sistemas operacionais, armazenamento e aplicativos instalados e, possivelmente, um controle limitado de alguns componentes de rede;

XXV - Modelo de Serviços em nuvem PaaS (Platform as a Service – Plataforma como Serviço): capacidade fornecida ao cliente para provisionar na infraestrutura de nuvem aplicações adquiridas ou criadas para o cliente, desenvolvidas com linguagens de programação, bibliotecas, serviços e ferramentas suportados pelo provedor de serviços em nuvem. O cliente não gerencia nem controla a infraestrutura na nuvem subjacente, incluindo rede, servidores, sistema operacional ou armazenamento, mas tem controle sobre as aplicações instaladas e possivelmente sobre as configurações do ambiente de hospedagem de aplicações;

XXVI - Modelo de Serviços em nuvem SaaS (Software as a Service – Software como Serviço): capacidade de fornecer uma solução de software completa que pode ser contratada de um provedor de serviços em nuvem. Toda a infraestrutura subjacente, middleware, software de aplicativo e dados de aplicativo ficam no data center do provedor de serviços. O provedor de serviço gerencia hardware e software e garante a disponibilidade e a segurança do aplicativo e de seus dados;

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

XXVIII - Nuvem comunitária: modelo de implantação de nuvem em que os serviços de computação em nuvem são exclusivamente suportados e compartilhados por um grupo específico de órgãos e entidades de serviços de computação em nuvem que têm requisitos compartilhados e um relacionamento entre si, e onde os recursos são controlados por pelo menos um membro deste grupo, conforme ISO/IEC 22123-1:2023 (Information technology — Cloud computing — Part 1: Vocabulary). O modelo de nuvem comunitária admite o uso de recursos computacionais de provedores de nuvem pública somente se assegurado o isolamento lógico e físico desses recursos, no ambiente do próprio órgão ou de empresas públicas, e não se configurando como uso de Nuvem Pública;

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

XXX - Nuvem híbrida: infraestrutura de nuvem composta por duas ou mais infraestruturas distintas (privadas, comunitárias ou públicas), que permanecem com suas próprias características, mas agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações;

XXXI - Nuvem privada ou interna: infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos usuários, e sua propriedade pode ser do próprio órgão ou de empresas públicas com finalidade específica relacionada à tecnologia da informação, conforme ISO/IEC 22123-1:2023. O modelo de nuvem privada admite o uso de recursos computacionais de provedores de nuvem pública somente se assegurado o isolamento lógico e físico desses recursos, no ambiente do próprio órgão ou de empresas públicas, e não se configurando como uso de Nuvem Pública;

XXXII - Nuvem pública ou externa: infraestrutura de nuvem dedicada para uso aberto de qualquer organização, e sua propriedade e seu gerenciamento podem ser de órgãos públicos, empresas privadas ou de ambos;

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

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

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

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

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

XXXVIII - Serviços agregados: são serviços adicionais providos pelo fornecedor da solução que oferecem aos usuários acesso a recursos adicionais relacionados ao objeto principal. Esses serviços podem incluir suporte técnico, treinamento, atualizações, implementação e outros serviços;

XXXIX - Sistemas estruturantes: são sistemas de informação desenvolvidos e mantidos para operacionalizar e sustentar as atividades de pessoal, orçamento, estatística, administração financeira, contabilidade e auditoria, e serviços gerais, além de outras

atividades auxiliares comuns a todos os órgãos da Administração que, a critério do Poder Executivo, necessitem de coordenação central;

XL - Software livre: tipo de software de código aberto que pode ser usado, estudado, modificado e redistribuído gratuitamente. O software livre é publicado sob uma licença que permite aos usuários acessar os códigos-fonte e modificá-los para atender às suas necessidades;

XLI - Software open source (ou de código aberto): tipo de software de código aberto que pode ser usado, estudado, modificado e redistribuído gratuitamente. O software open source é publicado sob uma licença que permite aos usuários acessar o código-fonte, mas impõe certas limitações quanto a sua modificação ou personalização;

XLII - Software pronto para uso: software disponibilizado (pago ou não) com um conjunto de funcionalidades pré-concebidas, também conhecido como Ready to Use Software Product (RUSP) ou mais comumente como “software de prateleira”;

XLIII - Suporte técnico: serviço provido pelo fornecedor para auxiliar os usuários com problemas relacionados ao serviço contratado. O suporte técnico pode incluir resolução de problemas, treinamento, atualizações, implementação e instalação;

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

XLV - Recursos reservados: são aqueles recursos tecnológicos que possuem planos predefinidos de consumo por determinado período mediante a aplicação de desconto, seja por meio de antecipação de pagamento, seja mediante pagamento mensal durante o período predefinido;

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

XLVII - Banco de Dados como Serviço (DBaaS): ambiente no qual o recurso usado pelo órgão ou entidade é um banco de dados disponibilizado e operado pelo provedor de serviços em nuvem, e suas funções são acessadas por APIs ou meios equivalentes, conforme ISO 22123-2:2023.

CAPÍTULO III

DAS REFERÊNCIAS

Art. 6º Para o desenvolvimento da Estratégia de Uso de Software e de Serviços de Computação em Nuvem, cabe à Anvisa 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 - Portaria SGD/MGI nº 852, de 28 de março de 2023, que dispõe sobre o Programa de Privacidade e Segurança da Informação;

III - Decreto nº 12.572, de 4 de agosto de 2025, que institui a Política Nacional de Segurança da Informação;

IV - Decreto nº 12.573, de 4 de agosto de 2025, que aprova a Estratégia Nacional de Cibersegurança;

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

VI - 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;

VII - 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;

VIII - 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;

IX - Instrução Normativa GSI/PR nº 8/2025, de 6 de outubro de 2025, que dispõe sobre os requisitos mínimos de segurança da informação para tratamento de informação classificada em computação em nuvem;

X - Portaria PT nº 60, de 24 de janeiro de 2022, que institui a Política de Governança Organizacional da Anvisa, e o Modelo de Governança de Tecnologia da Informação e Comunicação (MGT) dela decorrente, aprovado por meio da Portaria nº 943, de 4 de agosto de 2025;

XI - Lei nº 9.782, de 26 de janeiro de 1999, que define o Sistema Nacional de Vigilância Sanitária e cria a Agência Nacional de Vigilância Sanitária; e

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

TÍTULO II

DAS DIRETRIZES E NORMAS INTERNAS DE SEGURANÇA DA INFORMAÇÃO

CAPÍTULO I

DAS DIRETRIZES GERAIS

Art. 7º A Estratégia de Uso de Software e de Serviços de Computação em Nuvem da Anvisa será norteadada pelas diretrizes estabelecidas abaixo:

I - A adoção de softwares corporativos deverá observar os padrões arquiteturais definidos pela Gerência-Geral de Tecnologia da Informação (GGTIN), cabendo a essa unidade analisar e autorizar a sua utilização no âmbito da Anvisa;

II - Para a contratação de softwares e serviços em nuvem, deve-se prever e tratar o risco de dependência tecnológica a um fornecedor (risco de lock-in); e

III - A GGTIN deve manter atualizado o inventário de softwares da instituição.

CAPÍTULO II

DA IDENTIFICAÇÃO DAS NECESSIDADES DO NEGÓCIO

Art. 8º A Anvisa deve identificar e avaliar as necessidades de negócio antes da contratação de software e de serviços de computação em nuvem.

§ 1º Deve-se determinar quais sistemas, aplicações, dados e serviços — incluindo os sistemas de registro, cadastro, monitoramento e fiscalização sanitária — precisam ser movidos para a nuvem, como eles serão acessados e quais recursos computacionais e de armazenamento serão necessários.

§ 2º Deve-se avaliar, quando da concepção de novos serviços e sistemas, quanto à viabilidade de que os serviços sejam desenvolvidos para utilização em ambientes de nuvem ou não.

CAPÍTULO III

DA SELEÇÃO DOS MODELOS ADEQUADOS

Art. 9º Os serviços de computação em nuvem pública, de governo ou híbrida, poderão ser empregados:

I - nos casos em que a nuvem privada não consiga promover a escalabilidade, a flexibilidade, a agilidade, a segurança cibernética ou a inovação tecnológica necessárias para atender aos requisitos técnicos e de negócio; ou

II - para promover a eficiência de custos e facilidade de gestão e sustentação.

§ 1º Nas hipóteses em que os serviços de computação em nuvem sejam necessários apenas como parte de uma solução, poderá ser adotada a abordagem de nuvem híbrida, mantendo parte dos recursos em nuvem privada, sobretudo nos casos de uso de recursos tecnológicos em nuvem por meio de APIs.

§ 2º Quando houver estudos que apontem que a demanda prevista pode ser melhor atendida integralmente por meio de serviços em nuvem, uma abordagem completa, incluindo as demandas de migração do ambiente on-premises para a nuvem, poderá ser adotada.

§ 3º Quando houver a previsão de implementação de soluções totalmente em nuvem, deverá ser inserido no processo de contratação um plano de recuperação dos serviços em caso de descontinuidade do instrumento contratual por fatores externos ao controle da Anvisa.

§ 4º A adoção de soluções em nuvem constitui diretriz preferencial para novas soluções de tecnologia da informação e comunicação, desde que demonstrada sua viabilidade técnica, econômica, operacional e de segurança da informação.

CAPÍTULO IV

DA AVALIAÇÃO DOS POSSÍVEIS FORNECEDORES

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.

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

CAPÍTULO V

DA DEFINIÇÃO DE REQUISITOS DE SEGURANÇA

Art. 11. Deve-se 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.

Parágrafo único. As contratações de software e serviços de computação em nuvem deverão contemplar requisitos de segurança da informação compatíveis com a classificação das informações tratadas, observando a Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, e demais normas aplicáveis.

CAPÍTULO VI

QUANTO AO USO SEGURO DE SOFTWARE E DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM

Art. 12. A Anvisa deve observar os normativos 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 — inclusive dados de processos regulatórios, sanitários e de fiscalização — que eventualmente serão tratadas em ambiente de nuvem.

CAPÍTULO VII

CONDIÇÕES MÍNIMAS DE INFRAESTRUTURA DE TIC PARA UTILIZAR SERVIÇOS DE COMPUTAÇÃO EM NUVEM

Art. 13. A Anvisa deve efetuar a avaliação quanto às condições mínimas de infraestrutura de TIC do órgão para utilizar serviços de computação em nuvem, a exemplo de conexão estável com a Internet e com banda suficiente, inclusive link dedicado entre a Anvisa e a nuvem pública quando necessário para garantia de menor latência exigida pelas soluções na comunicação entre os ambientes privados e públicos de nuvem.

CAPÍTULO VIII

DEFINIÇÃO DE DIRETRIZES DE GOVERNANÇA PARA O USO DA NUVEM

Art. 14. A Anvisa deve garantir que as contratações apresentem claramente as diretrizes e os papéis e responsabilidades dos atores organizacionais (da TI, das áreas de negócio e da nuvem).

Parágrafo único. Devem ser observadas as práticas e orientações fornecidas pela Secretaria de Governo Digital - SGD em seus manuais e normativos relacionados a contratações de softwares e serviços em nuvem.

CAPÍTULO IX

DEFINIÇÃO DOS PRINCÍPIOS NORTEADORES DA ESTRATÉGIA

Art. 15. São princípios norteadores desta estratégia:

I - otimização do uso dos recursos disponíveis no Datacenter com foco na perenidade e padronização das soluções;

II - utilização integrada da infraestrutura própria e dos serviços de computação em nuvem, observadas as necessidades de negócio, os requisitos técnicos, de segurança e de continuidade dos serviços;

III - priorização das contratações de softwares por meio de licenças como serviço, evitando a aquisição de soluções com licenciamento perpétuo;

IV - lift-and-shift como último recurso, devendo ser evitada a migração de aplicativos do Datacenter para a nuvem sem primeiramente adaptar tais recursos para o ambiente de nuvem;

V - priorização, sempre que tecnicamente e economicamente viável, da adoção de soluções concebidas para execução em ambientes de computação em nuvem (cloud-native), em detrimento da simples migração de aplicações legadas;

VI - utilização dos serviços de computação em nuvem de forma racional, observando critérios de eficiência operacional, otimização de custos, escalabilidade e sustentabilidade tecnológica;

VII - promoção da interoperabilidade, da portabilidade e da adoção de padrões abertos, sempre que possível, de forma a reduzir riscos de dependência tecnológica entre fornecedores;

VIII - utilização da computação em nuvem como instrumento para fomentar a inovação, a transformação digital e a melhoria contínua dos serviços prestados pela Anvisa.

CAPÍTULO X

QUANTO AO ALINHAMENTO COM OUTROS PLANOS ESTRATÉGICOS

Art. 16. Esta estratégia possui alinhamento com os seguintes planos estratégicos:

- I - Planejamento Estratégico Institucional da Anvisa;
- II - Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC da Anvisa;
- III - Plano de Contratações Anual (PCA); e
- IV - Plano de Gestão de Segurança da Informação da Anvisa.

CAPÍTULO XI

CAPACITAÇÃO DA EQUIPE DO ÓRGÃO QUE GERENCIARÁ AS AÇÕES DESTA ESTRATÉGIA

Art. 17. A Anvisa 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.

CAPÍTULO XII

PORTABILIDADE E INTEROPERABILIDADE ENTRE SISTEMAS, DADOS E SERVIÇOS

Art. 18. A Anvisa deve considerar a viabilidade de adoção de medidas para mitigar a dependência tecnológica ou aprisionamento ao provedor.

CAPÍTULO XIII

DOS REQUISITOS REGULATÓRIOS E DE CONFORMIDADE

Art. 19. A Anvisa deve considerar os requisitos regulatórios e de conformidade para o uso seguro de software e serviços de computação em nuvem no âmbito da administração pública federal, inclusive, quando aplicável, os requisitos de proteção de dados pessoais previstos na Lei Geral de Proteção de Dados Pessoais (LGPD).

§ 1º Devem ser incluídos, nos instrumentos contratuais com os provedores de nuvem, cláusulas e mecanismos que garantam, ao menos, o sigilo dos dados no armazenamento e em trânsito, a não transferência dos dados a terceiros, a remoção incondicional dos dados após o término do contrato e a não utilização dos dados, para quaisquer fins, pelo provedor ou por terceiros.

§ 2º As contratações que envolvam tratamento de dados pessoais deverão observar a Lei Geral de Proteção de Dados Pessoais, os normativos da Autoridade Nacional de Proteção de Dados e as normas internas da Anvisa aplicáveis à privacidade e proteção de dados

CAPÍTULO XIV

ESTRATÉGIA DE SAÍDA

Art. 20. A Anvisa deverá considerar, nas contratações de software e serviços de computação em nuvem, a estratégia de saída da solução, contemplando, quando aplicável:

- I - A portabilidade de dados, aplicações e configurações;
- II - A reversibilidade da solução, permitindo a migração para outro provedor ou para infraestrutura própria, quando necessária;
- III - A continuidade dos serviços durante o processo de transição;
- IV - A mitigação da dependência tecnológica de fornecedores; e
- V - A preservação da integridade e da disponibilidade das informações durante o processo de migração ou encerramento da contratação.

TÍTULO III

DEFINIÇÃO DOS REQUISITOS PARA O USO SEGURO DE COMPUTAÇÃO EM NUVEM

Art. 21. A Anvisa 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, na Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, ou em documentos equivalentes publicados posteriormente.

TÍTULO IV

DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

CAPÍTULO I

DO COMITÊ DE GOVERNANÇA DIGITAL (CGD)

Art. 22. As competências do Comitê de Governança Digital (CGD), no âmbito das ações de Segurança da Informação, estão previstas na Política de Governança Organizacional da Anvisa, instituída pela Portaria PT nº 60, de 24 de janeiro de 2022.

CAPÍTULO II

DO GESTOR DE SEGURANÇA DA INFORMAÇÃO

Art. 23. As competências do Gestor de Segurança da Informação da Anvisa estão dispostas no art. 19 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, sendo essa função atualmente exercida pelo Gerente-Geral da Gerência-Geral de Conhecimento, Informação e Pesquisa, conforme a Portaria nº 257/GGPES/Anvisa, de 4 de março de 2024.

CAPÍTULO III

QUANTO À ÁREA DE TECNOLOGIA DA INFORMAÇÃO DA ANVISA

Art. 24. Compete à Gerência-Geral de Tecnologia da Informação (GGTIN) implementar os procedimentos relativos ao uso de tecnologias de computação em nuvem, em conformidade com as orientações contidas neste documento e na legislação pertinente.

TÍTULO V

DAS DISPOSIÇÕES FINAIS

Art. 25. A Estratégia de Uso de Software e de Serviços de Computação em Nuvem deverá ser divulgada amplamente no âmbito da Anvisa.

Parágrafo único. A Estratégia de Uso de Software e de Serviços de Computação em Nuvem, bem como todas as normas dela decorrentes, deverão ser revisadas e atualizadas sempre que se fizer necessário, não excedendo o período máximo de 4 (quatro) anos.

Art. 26. As novas contratações de software e serviços de computação em nuvem devem observar as diretrizes apresentadas neste documento, bem como o modelo de contratação de software e de serviços de computação em nuvem, no âmbito dos órgãos e das entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISF do Poder Executivo Federal.

Art. 27. Os casos omissos não abordados neste documento serão analisados pelo Comitê de Governança Digital (CGD).

Art. 28. Esta de Portaria entra em vigor na data de sua publicação.

LEANDRO PINHEIRO SAFATLE

Diretor-Presidente